Open Sourcing Normative Assumptions on Privacy and Other Moral Values in Blockchain Applications

Ishmaev, Georgy

DOI
10.4233/uuid:ae329b13-9def-478e-8a92-300b21560981

Publication date
2019

Document Version
Final published version

Citation (APA)
Ishmaev, G. (2019). *Open Sourcing Normative Assumptions on Privacy and Other Moral Values in Blockchain Applications*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:ae329b13-9def-478e-8a92-300b21560981

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Open Sourcing Normative Assumptions on Privacy and Other Moral Values in Blockchain Applications

Open Sourcing Normative Assumptions on Privacy and Other Moral Values in Blockchain Applications

Dissertation

for the purpose of obtaining the degree of doctor
at Delft University of Technology
by the authority of the Rector Magnificus, prof.dr.ir T.H.J.J van der Hagen,
Chair of the Board for Doctorates
to be defended publicly on
Wednesday 10 July 2019 at 10:00

by

Georgy Shamilyevich ISHMAEV

Master of Arts by Research in Philosophy, University of Hertfordshire, UK
born in Chelyabinsk, Russia

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus, chairperson	
Prof.dr. M.J. van den Hoven	Delft University of Technology, promotor
Dr. U. Pesch	Delft University of Technology, copromotor

Independent members:

Dr. S. Roos	Delft University of Technology
Dr. B. Bodo	University of Amsterdam
Prof.dr. A. J. Zwitter	University of Groningen
Prof.dr.ir. M.F.W.H.A. Janssen	Delft University of Technology
Prof.dr.mr.ir. N. Doorn	Delft University of Technology (reserve)

Keywords: data ethics, data protection, privacy, norms, blockchain

Printed by: Ipskamp Printing, Enschede

ISBN: 978-94-028-1595-5

Contents

1. Introduction

1.1. Privacy, power and cryptography

The disruptive potential of the blockchain technologies is difficult to predict accurately. Still, there is a definite demand for this kind of assessment evident from the amount of research growing around the blockchain applications. Certainly, some of these predictions can be considered as too far-fetched, but it is fair to say that only a while ago the very idea of Bitcoin was considered highly improbable for practical implementation. Yet we are now witnessing an unprecedented pace of development going far beyond cryptocurrencies, towards smart contracts and now identity management systems. It also needs to be said that, no technology appears in a vacuum no matter how novel or disruptive it is. It is alway defined by the previous developments in one way or the other, sometimes in the enabling sense, but sometimes also defining the ends and purposes of a new technology.

On the technological level, this development can be considered as the process of optimization - a range of developments that aims to overcome constraints of previous solutions. However, taken in the broader context, each generation of technological developments can be seen as a playing field between different actors trying to further their aims and goals with the adoption of new solutions. So, for instance, we can consider commercial enterprises competing on the market trying to achieve advantage over competitors via technological developments. Or we can consider an arms race between geopolitical adversaries trying to further their agendas and achieve goals, whatever these may be. Seen as such, technological development always carries a wide range of goals, much broader then mere optimization or overcoming of constraints brought by the previous generations of applications.

This model, however, should not be oversimplified, since every technology carries an element of unpredictability, bringing results opposite of those intended by the creators and thus serving interests of actors with opposite interests. This thesis should be taken as descriptive and neutral; on one hand, history has plenty of examples when technology created from the best of intentions serves nefarious purposes, and on the other technological tools aimed to promote harmful effects turn out to be in-

strumental for morally desirable means. Classic examples for the latter case can be found in the history of the cryptography, where a wide range of tools developed by government secret agencies became instrumental for the protection of privacy for individuals, simultaneously being developed in public domain (e.g. asymmetric encryption or TOR network). The choice of these examples is not accidental, since the development of blockchain technologies and goals of (some) of their creators cannot be understood without knowing the history of network protocols and cryptographic tools.

After all, blockchain technology and its first successful implementation, Bitcoin, is essentially an ingenious combination of tools that were known to cryptographers before. Hash function, asymmetric key encryption, merkle trees - all these tools precede blockchain implementation. In fact, the very idea of digital currencies can very much be credited to the community of 'Cypherpunk' thinkers. Inspired by the advancements in cryptography that made public-key or asymmetric encryption tools available for general public, this loosely associated group of computer scientists, cryptographers and technology enthusiasts, came up with a set of rather novel ideas based on one radical assumption: that cryptographic tools can and should change our society. Not only did these ideas become precursors for the development of blockchain technology, some of the predictions expressed by 'Cypherpunk' thinkers turned out to be surprisingly accurate.

In his seminal paper, David Chaum (1985) articulated and predicted key concerns associated with the development of communication technologies based on principle of hierarchical organisations. Loss of privacy, autonomy, and disempowerment of individuals faced with the increasing concentration of data resting in hands of centralized governmental and commercial entities. Chaum's biggest concern was that the logic of hierarchical computer systems inevitably would lead to situations where legitimate needs of computer security exaggerate information asymmetries and power imbalances in wider social contexts. More than 30 years ago, with prophetic accuracy, he pointed out that foundations were being laid for a 'dossier society' – one where computers and digital means of communications will enable governments and companies to accumulate unprecedented amounts of data on individuals.

The major flaw, as Chaum argued, was coming from the fact that as long as communication systems allow system providers, organizations or eavesdroppers to collect traces of information, these systems constitute a major threat to individual's ability to determine how information about them is used. Considering the state of individual privacy in the contemporary age, his predictions seem to be surprisingly accurate. There is no need to review all major incidents of the past years to appreciate Chaum's predictions.

The Snowden revelation alone would suffice to justify all apprehensions about the abysmal state of privacy, brought upon by the weaponized surveillance technologies employed without exception by all state governments. Not only state actors, but all kinds of commercial companies, from technological behemoths to small startups, compete in the race to create better and more comprehensive dossiers on Internet users. The most recent incident involving Facebook and Cambridge Analytica provided but a glimpse at the size of the abyss. This should be seen as a logical development considering how Chaum already observed that: "sophisticated marketing techniques that rely on profiles of individuals are already being used to manipulate public opinion and elections" (p. 1030).

These developments are also largely consistent with the main technological culprits highlighted by Chaum: centralized architectures enabling accumulation of data in silos controlled by corporate or government entities. These actors, placed as intermediaries in a variety of everyday online transactions and services, use their positions to harvest as much data as possible from the users of Internet. In fact, private data collection practices already transcend this obsolete distinction between Internet as online world and physical offline world. Sensor devices, which are becoming truly ubiquitous with the propagation of Internet of Things (IoT) technologies, present new vectors of surveillance in physical spaces that were not considered possible before (Christl et al., 2017).

Business models enabling extraction of a commercial value from the collected private data brought these practices to a new scale. Manufacturers and suppliers of all types of internet connected devices invent ingenious and bizzare ways to collect more and more data. Your TV eavesdropping on conversations in one's living room, an automated vacuum recording map of your house, your wardrobe mirror videotap-

ing how you dress every morning – all of these examples do not come from the dystopian science fiction, but are real commercial products. These developments bring profound moral apprehensions regarding degradation of privacy as Chapter 2 of this thesis shows. In that respect, Chaum's predictions were really an underestimation to say the least.

The accuracy of Chaum's predictions does not end with the identification of centralized client-server architectures as the main culprits of power asymmetries between the users and providers of technology in a digitalized society. Chaum also identified three key types of online interactions where individuals and their privacy would be most vulnerable in such society: communications, payments and presentations of credentials. Furthermore, he also proposed the concepts of cryptographic solutions corresponding to these types of transactions, which would help individuals to regain control of their data and shift the balance of power away from the centralized entities in the world of ubiquitous private data collection. Three key components could be considered as central elements of this paradigm shift, components enabling unconditional privacy of communications, payments and presentations of credentials.

Before looking into proposed solutions, it would be helpful to consider whether the specific problems highlighted by Chaum accurately correspond to these three domains today. After all, proponents of blockchain technology are often blamed for attempts to try and solve nonexistent problems. Narayanan (2013) went as far as to suggest that the crypto dream was effectively dead, from the very beginning built on misguided assumptions that individuals "seek technological privacy protection from governments and service providers". Can it be true that, as Narayanan argues, a 'feudal model' built on the user's trust (as seen in Google and Amazon services) provides better data security, and such companies as Facebook are good examples of privacy intermediaries? The short answer is, as we know now, that Narayanan turned out to be dead wrong, and the reality could not be further from these assumptions. Governments surveillance agencies and aforementioned service providers monetising private data are the main locomotives driving contemporary society into a dystopia of total surveillance, under the gloss of 'digital economy' hailed by Narayanan. To be fair, Naraynan himself later refuted these assumptions, becoming a supporter of the blockchain technology, and strong critic of the Facebook privacy policies. But the short rebuttal of criticisms targeted at 'Cypherpunk' predictions

would not suffice to appreciate their accuracy and relevance, so let us take a look in details at problems that were highlighted by Chaum, and correlate them to the actual state of affairs.

The first component enabling privacy-preserving communications between peers in Chaum's vision would be comprised of untraceable messages and anonymous identification of communicating parties. Untraceability here means that not only are the messages' contents encrypted, but also any traceable data that could reveal the identity of the sender or recipient. The relevance of this concern, these days, is apparent in the problem of meta data collection, aptly expressed by a former NSA employee: "If you have enough metadata, you don't really need content" (Rusbridger, 2013). Indeed, the ever increasing power of algorithmic tools for data processing allows for astonishingly accurate identification of individuals, even from metadata (Barocas & Nissenbaum, 2014). Current end-encryption systems do allow for pseudonymous communication and privacy of messages' content, but protection of meta-data is still an open question even in the most privacy-focused applications.[1] This issue is even more exaggerated by the abundance of meta data available from IoT enabled devices (Gasser et al., 2016), as also discussed in Chapter 2 and Chapter 3 of the thesis.

On the positive side, it can be said that end-to-end encryption is indeed getting wider adoption, and is now available to users of messengers and voiceover IP telephony without any requirements of technical expertise. However, the problem of secure peer communication is far from being solved - not only the issue of metadata collection, but attempts of governments to undermine individual rights for the personal use of encryption are still as persistent as in the days of short-lived 'Clipper chip' proposals (Dam, 1996).[2] One may experience strong dejavu comparing current proposals to undermine strong encryption with the 'crypto war' debates from 1980s and 90s. It may seem bizarre that proposals to create backdoored encryption that were refuted numerous times by academic researchers and experts as technically impossible and dangerous are still being peddled with astonishing persistence by the gov-

[1] Signal messenger, for instance together with many other privacy focused messengers does not completely solve problem of meta data. See https://github.com/signalapp/Signal-iOS/wiki/FAQ

[2] Clipper chip - a cryptographic device supposedly combing capacity to encrypt communications for end users (voice and data), with the escrow keys capability enabling government agencies to decrypt these communication.

ernment officials around the globe (Green 2018; Karp 2018; Sharwood 2018; Pearce 2019). And it would be tempting to discard these comments as comical technical inaptitude of certain officials - as statements alike - "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia." (Evershed, 2017). But the actual state of affairs is much grimmer, and this persistence, in fact, demonstrates over and over again that certain actors and institutions will not flinch in the face of blatant intellectual dishonesty in their efforts to create a surveillance society. Indeed, it seems that Orwell's "two plus two equals five" is uncomfortably close to reality.

With this background as a foundation, we may also consider a second set of issues and solutions suggested by Chaum, as they have immediate relevance to blockchain applications. Financial transactions performed by centralized intermediaries, argued Chaum, carry inherent risks for the privacy of individuals. Providers of such systems, whether banks or other payment services, have an unprecedented ability not only to collect private data about purchases but also to aggregate those data in profiles linked to real individuals. This is very much true today, as different payment providers not only aggregate such profiles, but also share and sell them as source of revenue. Paypal, one of the pioneering systems of online commerce, revealed that it shares customers data with as many as 600 third parties.[3] Other payment providers such as Visa and MasterCard also engage in such practices, sharing consumer data with data brokers and even offering their own marketing products built on these data (Christl et al., 2017). Some more exotic applications of the financial surveillance tools even include proposals to equip cash notes with nano-chips that could be tracked by government organizations (Chung, 2017).

These trends are also reflected in the developments of mobile payment systems, which use near field communication chips embedded in smartphones. As Hoofnagle et al. (2017) point out, not only do such systems allow greater collection of a consumer's data, they are often specifically designed for these purposes. Unlike plastic cards, which provide at least some separation of data between transacting parties, mobile payments allow merchants and payments providers to collect a lot of personal data unbeknownst to the smartphone owner. These privacy risks are only going to

[3] See Paypal privacy statement: https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list

become more extreme if the idea of 'cashless society' is realized on the basis of centralized technical architectures where few key entities could achieve complete control not only over financial data, but essentially eliminate individual monetary ownership (Agarwal & Krogstrup, 2019). All these issues strongly suggest necessity to radically reconsider the alternatives to existing digital financial infrastructures - alternatives which can be provided by blockchain based cryptocurrencies as demonstrated in the Chapter 1 of the thesis. At the moment blockchain based cryptocurrencies do not provide strong privacy to the users, given satisfactory scalable solutions for the protocol level privacy, network privacy and privacy of exchanges, have not been found yet. However, they provide some truly novel building blocks for the implementation of anonymous and fungible digital currencies.[4]

A third component - suggested by Chaum as necessary for the protection of individual privacy in computerized environments - is the privacy preserving system of credential management. As he argued, credentials, in the form of statements about individuals based on their relationships with organizations, play a crucial role in depersonalized online interactions. However, in centralized architectures, monitorability and control are completely taken away from individuals, since all credential data resides in repositories belonging to organizations. Glimpses of these credential repositories are periodically revealed these days with hacks of data bases belonging to credit reporting agencies and other companies engaged in the profiling of individuals. The most recent breach of Equifax, potentially compromising the data of 145 million individuals, revealed a staggering silo of data including tax identification numbers, driver's licenses, birthdays, home addresses, and other personal data (Matthews 2017).

True to Chaum's concerns, such data brokers collect and use these data against the interests of profiled individuals. These apprehension are true not only in regards to shadow profiles of individuals, those very existence is unknown to individuals themselves, such as credit reports controlled by data brokers (Ramirez 2014). Often, individuals even have no controls over the online credentials that they create themselves,

[4] Some developments in this area include protocol level privacy solutions in anonymous currencies such as Monero https://web.getmonero.org/ and Zcash https://z.cash/, that respectively implement ring signatures and zero-knowledge proofs to obfuscate identities of the transacting parties. Network level anonymity solutions include Kovri https://kovri.io/ developed for Monero and Dandelion for Bitcoin (Fanti et al. 2018).

as in the case of the disputes over Linkedin profiles (Mooney, 2013). In fact, with the propagation of online data scrapping tools and methods, combined with the legal ambiguities, create situations when profile owners have zero legal or technical guarantees of their data ownership.[5] These issues of identity and identity management systems create profound moral challenges and outline a focal point of concerns regarding informational privacy as Chapter 4 shows.

To sum up, we can say that the predictions of 'crypto dreamers' expressed more than 30 years ago turned out to be far more accurate than the more recent assessments of their critics (Narayanan, 2013). This observation, on one hand, signifies that the privacy issues we experience now are more serious and disturbing than we could have anticipated. If the dichotomy pointed out by Chaum is correct, and computerization can lead to two types of society – one based on strong guarantees of individual privacy and another where centralized data collection destroys basic liberties – then it seems that we already went very far in the wrong direction. But on the other hand, solutions suggested by Chaum have also turned out to be quite prophetic, with Bitcoin being the most vivid example. Indeed, despite consistent criticism from all range of skeptics, this technical solution turned out to be astonishingly successful as the first step towards creating a global decentralized infrastructure that should help to protect privacy, security, autonomy, and other human rights against total surveillance. These are distinctive moral concerns, and they compel us to look deeper into the moral significance of blockchain technology considered in the context of the broader family of cryptographic tools.

1.2. The Moral significance of cryptographic tools

It is safe to say that at the moment, the ethics of cryptography as a distinctive academic discipline has not fully formed yet, being a subset of wider debates and studies on the ethics of cybersecurity. This is not surprising considering the historical origins of research on practical cryptography, which until recently was associated primarily with military and security purposes, thus carrying a certain tradition of opacity. One historical case is particularly interesting in that respect, presenting a hallmark case when a cryptographer driven by moral convictions made the decision to

[5] See for instance legal case of HiQ vs Linkedin, as a rather revealing illustration of data-mining practices in the field of online professional identities (Bennet, 2017).

share his research with the general public. This action triggered a spectrum of debates and government actions. In 1991, Philip Zimmerman decided to make PGP (Pretty Good Privacy), an encryption tool which he had developed, available to all Internet users, uploading source code on a public server. In the accompanying user's guide, Zimmerman expressed his strong discontent with the attempts of the US government to prohibit the development and dissemination of encryption tools (Zimmerman, 1991). Developments in computer technology, he wrote, can dramatically undermine the privacy of individuals, creating surveillance capabilities that "Stalin could never have dreamed of".

Zimmerman argued that strong cryptography in the information age remains the only way to hold the line of privacy, to empower people, to take privacy in their own hands. He was also worried that the attempts of the US government to introduce the surveillance friendly Escrowed Encryption Standard (EES) and its most well-known implementation, the 'Clipper' chip, were an attempt to undermine individual rights for secure communication (Dam, 1996). Making cryptographic tools such as PGP publicly available, as he argued, was an act of resistance to the attempts of the government to outlaw cryptography and privacy. His decision triggered a criminal investigation from US customs service for alleged violation of arms export controls, which was cancelled without any proceeding after three years. The dismissal of this case marked the beginning of a dismantling process for legal restrictions on the export of cryptographic tools in US, but more importantly, made clear that the dissemination of such tools is an issue having social impact far beyond the community of researchers in this field (Lauzon, 1998).

Zimmerman's PGP case was not an isolated incident, but rather one of the most illustrative ones in what became known as the first 'crypto war'. Attempts of the US government to introduce and standardize the 'Clipper' chip were met with strong resistance within cryptographic community. Many of the most influential cryptographers started taking a public stance against this initiative, notably including co-creator of the public-key encryption Whitfield Diffie. His motives, as well, were very much based on ethical commitments, and strong views on the privacy, power and individual rights. As Diffie stated in his objection to the 'Clipper' chip: "If the only telecommunications products available allow the government to spy on your conversations, then there'll be no privacy left for anybody except fat cats" (Bass, 1995). A

good deal of the criticism from the cryptographic community was based on the technical side of escrow encryption, focusing on the fundamental security flaws of these solutions (Abelson et al. 1997). However, these discussions also helped to spark a new strand of thinking on the social role of cryptographic tools - coming from the informal 'Cypherpunk' community of cryptographers and also from technology enthusiasts.

Largely based on the peculiar mixture of libertarian ideals and techno-optimism, their ideas framed development of cryptographic tools as an inherently moral exercise. Eric Hughes (2001, [1992]), author of 'A Cypherpunk's Manifesto,' expressed these normative commitments as the strong belief in value of privacy and necessity of privacy guarantees provided by the publicly available cryptography. Very much in the vein of Chaum's reasoning, Hughes argued that a new type of open and free society, built on the principle of respect to individual privacy, would be enabled by communication networks, guaranteeing anonymous everyday transactions to individuals. May (2001) elaborated more on Chaum's three fundamental types of anonymous transactions, suggesting that developments in publicly available cryptography would have profound implications for personal liberty leading to state of 'Crypto Anarchy'. Undermining the power of centralized powers such as nation states, new communities based on the aforementioned principles would provide the only viable alternative to a surveillance society, he argued. In a consequentialist vein, May suggested that all possible downsides of such state of affairs would be outweighed by the guarantees of personal privacy, freedom of speech, and freedom of access of information. In essence, 'Cypherpunk' ideas explicated morally desirable values of privacy and individual freedom in socio-technical systems that could be protected or preserved with the help of cryptographic technologies, even if doing it in the somewhat one-sided fashion of a naive technological determinism.[6]

These ideas, in turn, were confronted by the supporters of the government initiatives on the regulation of cryptography, who tried to justify the need for state surveillance powers on moral grounds as well. These types of public arguments by academic

[6] Technological determinism is label that can be attached to a broad spectrum of views on the deterministic nature of technological developments. Ranging from assumptions that technology is a self-contained phenomenon developing autonomously, to views that technology is single dominant factor of social changes.

authors signified a new shift in the 'crypto wars' - expanding into the new dimension of 'narrative wars'. Denning (1993), being one of the most active academic lobbyists for the government restrictions on cryptography, provided a view on encryption tools that became the default set of arguments for state surveillance proponents for years to come. Countering the view that publicly available, unconditional security of communication and data is univocally morally desirable, she presents encryption as a dual purpose tool that not only protects privacy but also can assist criminals and terrorists.

This very view on the dual purpose of cryptography was, of course, not invented by Denning or other academic supporters of escrow encryptions schemes. This narrative, together with 'Clipper' chip project itself, was bred and nurtured within two US agencies – the NSA and the FBI – as a package used to convince the Presidential administration of that time of the necessity of this initiative (Levy, 2002). The idea that the spread of secure encryption for personal use will bring apocalyptic consequences of unstoppable global crime and terrorism – invoking the metaphor of a 'double edged sword'. These moralised metaphors in turn got deeply intertwined with the interpretation of privacy as an individual right, somehow standing in the opposition to the public good of security.

To understand the core foundation of this narrative, however, one has to deconstruct the logical structure of the argument. Froomkin (1995) reflecting on the ongoing court cases around the escrowed encryption standard and export controls of the cryptographic software, offered a criticism of this paricular use of moralised arguments. As he points out, in the debates on the role of cryptography, moral arguments were often not a reflection on the potential of technology, but rather metaphors chosen as an instrument to steer the development of technology in the direction of the social effects desired by the authors of these metaphors, such as preservation of power distribution in society. In essence, the whole juxtaposition of the public-key encryption to the escrowed encryption schemes was not about the strength of the encryption itself, but rather, about controls of the critical elements of communication infrastructures.

Froomkin's considerations are very much derived from the legal scholar perspective, yet he made a compelling moral argument as well. As he aptly pointed out, it "is

unsettling to think that one's [fundamental] right may turn on the extent of which people are able to find technological means". Fundamental human rights, he argued, lie in the foundation of a democratic legal framework, defining its very purpose - to guarantee and protect these rights, regardless of the goodwill of power holder in the state. Similarly, choosing between cryptographic solutions that can guarantee privacy in themselves and those solutions where these guarantees depend on the goodwill of escrow (key holders) we should consider the former as more desirable from a moral standpoint. It would be wrong to interpret his arguments in the purely deontic fashion, however, as he also offered consequentialist considerations. Acknowledging the possible morally undesirable side effects of anonymous transactions enabled by unconditional privacy, Froomkin argued that the complete absence of such refuge of anonymity is much worse. Fundamentally, the value of such refuge has to be appreciated against the wider background of the technological advances that create more and more possibilities for surveillance and identification of individuals.

The metaphor of a 'double edged sword,' from that perspective, would seem to fall into the category of guiding narratives, having little to do with moral concerns but serving rather as mean to promote subjective power interests of certain government agencies in the development of technology. And yet, there are good reasons to consider more carefully the dual character of crytographic research and its ethical significance. From the consequentialist perspective, any arguments on the restriction of personal use of cryptography indeed hold no weight. For one, the juxtaposition of privacy and security is misguided to say the least, since publicly available secure cryptography delivers both of these values in a society where critical communication infrastructures handle all types of everyday transactions (Kenneth et al. 1997).

Deliberate introduction of technologically inferior cryptography on a mass scale, on the other hand, undermines both of these values, depriving individuals of their rights (Moore, 2000). In fact, any consequentialist justification of the restriction on the personal use of tools enhancing privacy and security such as public key encryption runs into a major obstacle. An obstacle, which is essentially a radical claim that everyone's right to privacy should be taken away in order to prevent the possibility that some individuals in the future may abuse this right for the ill ends. Or, as Schneier (2016) suggests in a vivid thought experiment, it is akin to secretly poison-

ing all the food in the restaurant in the hope that one of the poisoned customers is a terrorist.

Yet an attempt to completely discard the idea of the double-edged moral significance of cryptographic tools runs into the problem of naive technological determinism. In that sense, cryptography is not necessarily a one way function, as early 'Cypherpunks' has hoped. Rather, choices of different cryptographic solutions can enable both centralization and decentralization of controls over telecommunication infrastructures (Diffie & Landau, 2007). Furthermore, as communication infrastructures become more and more dependent on cryptographic products, even nuanced and seemingly isolated choices tend to have potential for profound effects. These days propagation of new communication technologies such as Internet of Things (IoT) create new channels for surveillance, with connected sensor devices infiltrating all areas of everyday life (Gasser et al. 2016). In this context, even the introduction of a single element may have far-reaching consequences, such as a random number generator with a deliberate flaw (Schneier, 2007; Menn, 2013) or ISO standardisation of untrustworthy block cipher for IoT (McCarthy, 2018). And choices of normative assumptions underlying research in cryptography and implementation of solutions can also define these effects.

As Rogaway (2015; 2016) argues, far from being confined in the linear model of technological development, cryptography is rather an exercise in the socially determined construction of artefacts. These artefacts are never developed in isolation, but rather in a continuous feedback loop, both embedding certain moral assumptions in their design and reshaping societal norms in return. The history of the 'Clipper' chip vividly shows how the development of these products can, in turn, be affected not just by moral concerns but even by the choice of moralized concepualizations (Froomkin, 1995). Rogaway (2015) offers some more recent examples of developments of cryptography in proof of this point. Bringing examples of current areas of research such as Fully Homomorphic Encryption (FHE) and Differential Privacy (DP), Rogaway shows that the actual impact of technology may drastically differ from the claimed intentions if social, political and economic factors are not accounted for. In the case of FHE, over-exaggeration of the potential of technology creates vast space for misinterpretations, misleading the general public about the real state

of affairs, and providing useful cover for the political actions aimed to justify surveillance practices.

Rogaway (2015) highlights example of such misinterpretation, citing DARPA program director D. Kaufman, according to whom FHE can enable identification of 'bad guys' by the court order 'in a sea of encrypted data'. Not only is this interpretation is an utter nonsense, but it immediately brings to mind narratives on the 'magic' qualities of escrow encryption schemes, supposedly combining individual privacy and mass surveillance.[7] Other misinterpretations presenting FHE as a silver bullet that would combine commercial data mining with individual privacy, argues Rogaway, in turn lead to the misplaced assumptions regarding the safety of cloud storage and computing. The problem here is not in the lack of scientific value of the research in the field of FHE. It is, rather, an attempt to justify morally questionable data mining practices, which already take place, on the grounds of future promises of technology that may or may not materialize.

In a similar criticism, Rogaway (2015) points in the direction of another field in cryptographic research - Differential Privacy. Which is also often represented as a solution capable of addressing the privacy concerns of government and corporate databases. Yet, argues Rogaway, differential privacy implicitly presupposes that increase in data collection always serves the public good, not even considering possibilities of data collection minimization.[8] Combined with considerations of familiarity, economics, and the fundamental desire of authorities to have and hold data, these presuppositions make it easy to predict further propagation of a centrally controlled computer network designs. Providing this criticism, Rogaway is more cautious than 'Cypherpunk' thinkers, suggesting that while conventional encryption does foster individual empowerment, it can also be developed in different directions that tend to benefit either the weak or the powerful. Thus, it is important not to forget about the

[7] Fully Homomorphic Encryptions technique is a computation technique which allows a party to perform general computations on a cyphertext data without having an access to decryption keys, and without the leakage of a plaintext data. And as Rogaway (2015) explains in details, the idea of 'exceptional legal access' to the plaintext content of encrypted data, has no relevance to the core principles and promises of FHE whatsoever.

[8] Differential privacy is in essence a statistical technique which aims to ensure privacy of records, separating raw database contents from data analysis output, introducing distortions that do not affect the quality of outputs significantly. Of course significance of distortions for the quality of analysis and and level of privacy protection are variable parameters here, and DP by no means is a universal solutions. For critical high level overview on the tradeoffs of DP also see Green (2016).

core value of cryptography: the capacity to make surveillance more expensive, to serve as a counterbalance to the ever-expanding data collection enabled by the Internet. In that capacity, argues Rogaway, cryptography is important not only for individual privacy but for human rights and society in general. Here, he follows Chaum's predictions that in the absence of cryptography enabled countermeasures, telecommunication technologies propel us towards a world of a total surveillance "where no man belongs".

This moral issue is not only the question of professional ethics or values of individual researchers, but even more so an issue of values embedded in institutions that cryptographers help to create. Actual mechanisms of this process, argues Rogaway, are not understood yet, and the explication of moral assumptions which become embedded in cryptographic tools is necessary to understand how practical application can shape our society. This is not to suggest that the morally undesirable effects of cryptography necessarily fall into the category of unexpected 'function creep'. After all one, has to keep in mind that the heritage of research in cryptography is deeply rooted in the traditions of secrecy, and for some actors, this is very much true to this day. Very often, research and implementations of cryptography are driven by malicious motivations, which are obfuscated by design. Moral reprehensibility here is akin to the development of fake medicine that does nothing to alleviate disease which it claims to cure. After all, an intentionally flawed cryptographic product such as 'clipper chip' delivers the opposite of what it is supposed to provide - violation of privacy and security.

This analogy is even more striking if we consider that the same actors responsible for the spread of the "disease" are also trying to suppress medicine that might help with their flawed products. The real moral duality of the cryptography lies here, in the capacity to remedy or exacerbate many moral issues brought by the development and adoption of communication and information technologies. Similarly, normative assumptions on moral values and responsibilities of researchers, implicitly or explicitly present in the development of cryptographic tools can steer research and implementation in both directions. And the adoption of these assumptions can be morally problematic in itself, such as belief in the alleged 'going dark' problem - an idea that the wide availability of encryption primarily serves interests of malicious actors in the society (Etzioni, 2017). Apart from being factually incorrect, these assumptions

enable poor or flawed technology choices, creating corrupting effects for the security of global infrastructures and leading to the further dissolution of privacy and individual autonomy in the society (Gasser et al. 2016; Green, 2018).

1.3. Philosophy and ethics of blockchain technologies

If research in the cryptography and development of cryptographic tools are inherently moral activities, we can ask ourselves, "where do blockchain technologies stand in this respect?" A good starting point here is to clarify whether it can be said at all that blockchain technologies share their moral significance with the broader family of cryptographic applications. After all, the ever increasing range of applications has seemingly shifted the locus of many discussions on blockchains far away from the topics of privacy. To answer that, we need to keep in mind that the main novelty of blockchain in respect to previous cryptographic implementations is that cryptographic primitives such as hashes or asymmetric encryption are not just used to enable certain desirable features in the system such as confidentiality of communication or authenticity of data. Nakamoto (2008) solving the question of how to synchronise records in a distributed database without reliance on a trusted authority, needed to prevent forgery of those records, has made one step further in the use of cryptographic tools. In Bitcoin protocol, cryptographic primitives are used not just as enabling components for the technical system (network protocol) but also as socio-technical building blocks - instruments of constraint and affordances, prescribing certain behaviour to the human actors within the system (economic incentives), effectively emulating traditional normative structures, as explored in the Chapter 1 of the thesis. Thus, in blockchain implementations cryptographic products are essentially building blocks of a social structure in a very direct sense.

This uncanny resemblance to Chaum's ideas, suggesting that cryptographic tools can be used as a building blocks for the social structures, is not accidental, of course. Bitcoin did not occur in a vacuum, but was very much influenced by previous proposals for electronic currency systems, which emerged within cypherpunk community (e.g. Wei Dai's 'b-money' and Nick Szabo's 'Bitgold'). Szabo, in fact, was one of the contributors to David Chaum's project, Digicash – an early implementation of electronic currency that did not gain sufficient traction. Certain parallels can also be drawn with the way in which PGP was made public by its creator, Zimmerman, and

Nakamoto's intention to make the Bitcoin protocol openly available. There is also a crucial difference, though, as for one, Nakamoto was cautious to avoid public attention to the project before it reached mature stages of development. Another difference of course is the scale of adoption. Where PGP popularity was limited mainly within the community of Internet users with a certain level of technological expertise, who could appreciate novelty of the tool, very tangible economic incentives brought by the Bitcoin and other cryptocurrencies fascinated minds of a much wider audience. This public fascination with economic incentives obscured, to a degree, the origins of blockchain technologies, currently first and foremost associated with the speculative nature of cryptocurrency markets. Furthermore, this fascination not only dramatically expanded the number of interested parties, but also introduced incredible amount of noise in public discussions, making any obfuscations in the debates on 'clipper chip' to seem like a transparent film in comparison.

Indeed, even at the first glance, responses to blockchain technologies are astonishingly polarized, ranging from borderline bizzare accusations that cryptocurrencies are tools of the far-right extremism (Golumbia, 2016), to the assessment of blockchain technology as an enabler for revolutionary positive social transformations of all kinds (Tapscott & Tapscott, 2016). One indeed can find the full spectrum of responses characterizing this truly novel technology: neo-luddite rejection, exalted techno-optimism, and self-contradictory responses from regulators who simultaneously threaten to ban blockchain technologies and embrace them as drivers of the new economy.

Judging by the attitudes of the general public, blockchain implementations have far surpassed their predecessors - cryptographic solutions for the confidentiality of communications and data storage in the scope of public attention. A good part of this polarization in opinions can be attributed to the unique economic success of the first implementations of cryptocurrencies, which enabled highly speculative markets of immense volatility. And, of course, judgments accompanying market speculations can hardly serve as rational sources of moral assessments or even intuitions. Yet these responses, in themselves, can be helpful in the identifications of some morally significant patterns of technology effects, just like metadata of communications can reveal interesting patterns regardless of message content.

Building on Rogaway's (2015) hypothesis on the social character of research in cryptography, it would be correct to assume that blockchain technologies are not transcendental in respect to social responses. Rather, very much like the cryptographic tools before them, blockchains develop in a constant feedback loop, driven by the values, normative assumptions, and personal commitments of researchers, which shape moral effects delivered by the technology in return. From this perspective, responses to the technology often can be seen as an effort to shape normative assumptions inherent to it, and to change its effects and purpose in favor of the interests of competing actors.

Reijers and Coeckelberg (2018) support this view, as well, in their assessment of the role that narratives play in the development of blockchain technology. Providing a theoretical framework aimed to show how our social world can be actively shaped by these technologies, they argue against the instrumental view that humans merely use blockchain technologies for predefined purposes. Reijers and Coecklberg (2018)'s approach, though, is primarily ontological in its scope. Acknowledging that certain narratives have distinctive moral components, they rather deliberately focus on the descriptive aspects of the development of blockchain technology, as defined by the narrative framing. Still, their framework provides an outline for the moral assessment of the social effects of blockchain technology, defined as a capacity in to shape and redefine social narratives, creating the feedback loops of socio-technical narratives.

In their view, the main novelty and moral significance of blockchain technologies is rooted in the capacity to introduce new types of human relations, which may or may not follow core narrative structures presented in earlier developments. On one hand cryptocurrencies may have emancipating and empowering effects, providing inclusion in the realm of economic exchange for the anyone regardless of their background or status. Decentralisation of currency can also entail decentralization of power, making it difficult for human agents to subject others to their will within the system. However, blockchain technologies can also have negative effects, extending rigid, technologically determined interactions from domains where it is appropriate (financial sphere) to social contexts where this is undesirable (human care, education). The main risk of technology, in their view, comes from uncertainty about

whether the decentralised features of the technology would also result in the decentralisation of institutional power.

This view is shared by the Velasco (2017), who argues that blockchain applications in their ledger functions are, in theory, compatible both with centralised and distributed social and political relationships. That is, they can enable both types of relations in society without strong dependance on any particular type of political relations for the functioning of these application. This, in Velasco's view, is explained by the unique capability of blockchains - capability to control distribution of trust. This can be seen as a direct continuation of the enabling properties of the public-key cryptography, as noted by Diffie and Lanadu (2007). Eliminating the necessity to trust a communication provider, or escrow key providers, such tools effectively enable different types of direct private relations between individuals. The important difference is that for Diffie and Landau, these peer to peer relations are anything but new. They see it rather as a return to norm, a translation of normal peer relations, which do not require intermediaries, from the offline world to the digital environment. From that point of view, blockchain technologies can also be seen as a 'return to norm', rather than the introduction of radically new relations, at least in regard to cryptocurrencies. This view is certainly shared by Berentsen and Schar (2018), who argue that the main value proposition of cryptocurrencies lies in their capacity to emulate all desirable properties of a physical cash - inclusiveness, anonymity, and decentralized payment – in a digital form.

But this does not mean, of course, that blockchain applications cannot shape social structures and human interactions in novel ways. One particular blockchain enabled application called smart contracts does strongly suggest such a possibility. De Filippi and Hassan (2018) argue that smart contracts - computer programs implemented on the blockchain that can facilitate negotiations, verifications, and enforcements of the contract – in a way emulating traditional legal agreements. This capacity to replace legal intermediaries with the code implemented and executed in the decentralized network does bring novel possibilities but also novel moral concerns. This is problematic, argue De Filippi and Hassan, since particular architectures of blockchain systems can facilitate certain actions and behaviour more than others, inevitably bringing political and social implications. Considering that such blockchain systems can be implemented at the transnational scale, with relatively low entry barriers, this

means that certain norms can be implemented at speed and at scale, often bypassing existing legal regulations completely. A main concern for De Filippi and Hassan is that norms present in blockchain applications often can be hidden or opaque, often in the absence of scrutiny, as compared to scrutiny surrounding implementation of key legal norms in democratic societies.

But smart contracts have also another dimension of moral significance that can be better understood against the backdrop of current technological trends. One such trend presenting special significance is a family of technologies unified under the label of the Internet of Things (IoT). Developments of these internet connected sensor devices has accelerated deployment of new communication infrastructures with the vast potential for surveillance (Guerr et al. 2016). Against that backdrop, promises of developers to implement blockchain enabled smart contracts to mitigate IoT privacy risks does seem to fall in line with Chaum's paradigm.

It would seem that blockchain technologies can have an important moral role in the mitigation of these risks, creating new systems and architectures for the control of private data in the interest of individual IoT users (Zyskind et al., 2015). These developments could be interpreted as another key building block for decentralized global communication infrastructures. And even more fascinating prospects are brought by the blockchain project developing systems for the so called self-sovereign identity (SSI). These systems leverage the capability of blockchain based data structures to serve as a decentralized public key infrastructures in order to emulate traditional identification documents in the online interactions (Tobin and Reed, 2016).

Thus it can be said that blockchain implementations such as cryptocurrencies do have a strong connection with moral concerns shared by the wider family of cryptographic tools, but arguably raise the stakes even higher than before. On one hand, Blockchain technologies may provide much needed building modules for the development of decentralised future ICT infrastructures. This is probably the single most important moral aspect of blockchain technologies: a capacity to mitigate erosion of privacy brought by the centralised architectures. In that quality, they share their significance with other cryptographic technologies such as public-key encryption. But this also suggests that just like with other cryptographic application, non-linear models of technological development warrant closer scrutiny of expectations and

actual effects. As Rogaway (2015) suggests, the actual mechanism explaining what role normative assumptions and moral values play in the development of cryptography is not clear yet. At the same time, considering what is at stake, we have all good reasons to try to understand these mechanisms better.

The profound capacity to shape and reshape social structures inevitably attracts attention of actors tempted to use this feature of blockchain technologies in their interests. It is also expected that these interests may spawn a new generation of 'crypto wars' on a vastly different scale, involving all kinds of battles for metaphors, definitions, and normative framings of technology. Unlike juxtapositions of legal metaphors highlighted by Froomkin (1995), collisions between these 'encoded' norms can happen in a much faster dynamic and even invisibly to general public. We can already see dawn of this in conflicts over concepts which may seem obscure and esoteric to external observers of the blockchain development field. 'Bitcoin cash' vs 'Bcasch', 'Blockchain' vs 'Distributed ledger', 'Permissioned' vs 'Private-public', and truly esoteric 'Turing completeness' vs 'Rich statefulness' are just few immediate examples, of naming battles with very real economic and political content.

Repeating patterns of the 'clipper' chip era, attempts to define and redefine meaning of technology reflect efforts to steer its development. We are only starting to comprehend what effects full scale adoption of blockchain technologies may have on the society, but from what we already know from 'crypto wars,' even seemingly minor developments can have a 'butterfly effect'. And just like the introduction of one flawed element in the cryptographic application can have mass scale effects, the introduction of flawed normative assumptions can have far reaching consequences. If these apprehensions are correct, then norms hidden in the blockchain code like undocumented features or vulnerability will have effects at scale and speed unseen before. These concerns highlight the moral duality of the blockchain technologies, defining the main research hypothesis of this thesis.

Blockchain technologies are often presented as a great disrupting factor that will change the shape of our society, but this vision is not quite accurate. With or without blockchain technologies, our society is being transformed in the most radical fashion by the propagation of new ICT technologies, propelling us towards the dystopian future of a non-existent privacy. We hardly can put brakes on these developments,

but we can steer them in the different direction with the help of cryptographic tools. From that perspective, it is rather naive to view blockchain technologies juxtaposed against a status quo, if only for the reason that no such status quo exists. It is suggested that blockchain technologies can serve as key building blocks for decentralised architectures, providing alternative to the surveillance society in line with David Chaum's predictions.

It is also suggested that through the explication of normative assumptions present in the current blockchain projects, we can try to determine vectors of these developments, which may be bringing us closer to this goal, or take us further away from it. But it is also argued that we should not take these normative assumptions present in blockchain technologies as a given. Just like open-source code is developed through the public revision and scrutiny, we should aim to make our normative assumptions transparent and be ready to revise them in case we find some errors. This thesis itself, in a way, can be seen as a very humble attempt to map some of the key normative assumptions present in the blockchain projects, as a contribution to the open source project of the future society where privacy is one of the core values of a global technological infrastructure.

1.4. Research questions and chapters

This section offers an overview of thesis chapters and frames them in accordance with the research issues suggested by the previous sections. **The second chapter, 'Blockchain technology as an institution of property,'** looks into the main theoretical hypothesis and argues, using Bitcoin as an example, that blockchain technology implementation can, indeed, provide alternatives to some existing social institutions such as property. From that perspective, blockchain technology applications do have the potential to replace key elements in the digital infrastructures on an unprecedented scale. However, such observation on the capacity of blockchain technology in itself does not provide normative arguments *per se* about whether we should replace other existing institutions and infrastructures with such solutions.

Chapter three 'Rethinking trust in the Internet of Things' elaborates on the philosophical conception of trust in private data protection. It argues that current devel-

opments in digital infrastructures, defined by the propagation IoT, exploits users' trust in the providers of technology, and is ethically unacceptable. Centralized architectures based on the client-server model simply cannot justify trust in the guarantees of data privacy offered by the data-collectors in such infrastructures. These findings strongly support at least one normative assumption present in current blockchain applications – namely, prima facie distrust as a key design component of infrastructures, capable of providing real data protection guarantees. Blockchain solutions embedding this principle can take away the need for individual users to rely on trust. It is also argued that we should be careful not to assume that Blockchain itself is a 'trustless' technology. Allowing for trustless interactions between peers in certain contexts, it does not eliminate completely the necessity to trust in the developers and the technology itself.

Chapter four 'The Ethical limits of Blockchain Enabled Markets for Private IoT Data' looks closer into blockchain solutions that promise to enhance privacy of consumers using IoT. It is argued that current proposals in this area are inseparable from the ideas of 'private data markets', and stem from the normative assumptions that private data propertization can enhance individual privacy. In line with the arguments from technological determinism, it treats propertization of private data as an inevitable process and focuses on the development of techno-economic solutions that would help to make private data markets more fair and transparent. However, as this study shows, there is a significant risk that in the long term such approach could lead to an effect opposite of intended. With this apprehension, it is worth taking a cautiously critical stance towards other normative assumptions embedded in other blockchain based solutions.

Chapter five 'Sovereignty, privacy, and ethics in blockchain based identity management systems' explores Self-sovereign identity (SSI) solutions implemented on the basis of blockchain technology. These solutions are often seen as alternatives to existing digital identification systems, or even as a foundation of standards for the new global infrastructures for identity management systems. This chapter aims to highlight a broader range of ethical issues surrounding the changing nature of human identity in the context of ubiquitous private data collection, in order to qualify promises and challenges of SSI systems. It is argued that in their current implemen-

tations these solutions operationalize the concept of 'self-sovereignty' in a narrow technical sense, rather removed from the wider set of moral issues inherent to this concept. This chapter argues against the suggestions that such depreciation of moral semantics can facilitate wider adoption of SSI solutions. On the opposite to ensure moral desirability of these implementations it is necessary to bridge the gap between normative and technical meanings of 'self-sovereignty'. Furthermore, this connection provides a valid moral grounding for the arguments on the desirability of SSI solutions over centralized identity management systems, where ethical issues are glossed over and disguised under the cover of moralized legitimizing claims.

2. Blockchain Technology as an Institution of Property

2.1. Introduction

Blockchain technology conceived and implemented in the form of digital currencies such as Bitcoin, from its very beginning has been a puzzling development for regulatory bodies and legislators. Being essentially an alternative to fiat currencies, Bitcoin gave rise to new markets and financial instruments functioning largely out of the scope of legal frameworks. This became possible due to the decentralized nature of blockchain technology, enabling creation of currencies independently of any central regulator (Vardi 2016). Initial reaction to propagation of Bitcoin from legal scholars and legislators was a question if and how Bitcoin should be regulated (Schcherbak 2014, De Filippi 2014). The push to address this issue was stimulated by the apprehensions (mostly justified) that Bitcoin may contribute to the growth of contraband markets and tax evasion schemes (Hendrickson et al. 2014).

At the moment of writing of this article, efforts to implement these regulations have been largely unsuccessful, as so called 'dark markets' demonstrate continuous growth (Kruithof et al. 2016) and consistent policy on the taxation of cryptocurrencies does not seem feasible (Campbell 2016), even more so in the future, due to the pseudonymous (Bitcoin) or anonymous (Monero, Zcash) nature of these financial instruments. The only meaningful regulation now in practice concerns exchanges that offer cryptocurrency-fiat trade pairs, thus falling into the scope of money laundering laws and regulations. At the same time, alternative services facilitating bitcoin-to-fiat trades such as 'LocalBitcoins' largely operate out of legal regulations (Melendez 2016).

The most interesting feature of Bitcoin and other cryptocurrencies, however, is not just resilience to regulation enforcement but rather successful functioning outside any meaningful legal frameworks, even in the light of numerous financial crashes such as bankruptcy of the Mt.Gox exchange responsible for about 70% of bitcoin exchange transactions, amounting for losses of $470 million for its clients (McMil-

lan 2014). Mt.Gox being the biggest case is not an isolated incident, as similar hacks took place most recently of Bitfinex in August 2016, resulting in losses of roughly $70 million (Reuters 2016). Interestingly, Bitfinex compliance with legal regulation was named as reason for this security breach, as in order to comply with US Commodity Futures Trading Commission requirements from June 2016, (CFTC Docket No. 16-19) Bitfinex kept customer funds in an online accessible form ('hot wallet') rather than in more secure offline storage ('cold wallet'). These examples make it possible to say not only the bitcoin economy is functioning in the absence of meaningful regulations but sometimes do so even in spite of regulations.

Cryptocurrencies are a flagship example of blockchain implementations but present only one possible application of this technology. Another application of blockchain are so called 'smart contracts' which gained traction rather recently (at least in terms of investments attraction). The idea behind 'smart contracts' is the extension of bitcoin code beyond simple monetary transaction to more complex operations which can be carried out within a similar decentralized network (Buterin 2014). This, for instance, can mean that if two parties engage in a contractual agreement using a 'smart contract' application, performance of contractual terms is guaranteed not by the goodwill of parties or third-party arbitrage but rather by the encoded algorithm. The scope of 'smart contracts' applications is wide-ranging, from simple contractual agreements to self-governing organizations. Self-governance here essentially means that such organizations can function without external regulation, purely on the basis of encoded algorithms executed on a decentralized network and fuelled by cryptocurrencies.

The promise of such powerful and complex systems has prompted the expression 'code is the law' conveying the assumption that legal frameworks in many instances can be successfully replaced by computer code (Swan 2015, p. 16). The first large and ambitious enterprise the 'DAO' project aiming to create self-governing organization on the basis of Ethereum smart-contracts, created by the motto 'code is the law' did not live up to expectations, both in financial and ideological senses. Conceived and advertised as an innovative self-governing investment fund, 'DAO' attracted over $150 million in crowdfunding, a record sum, only to fall victim of hack, causing annulment of the project (Greenspan, 2016).

To amend results of the hack and return stolen funds 'Ehtereum' foundation, developers of blockchain on which 'DAO' was based, made a decision to change protocol (implement a hard-fork), effectively annulling all transactions on Ehtereum blockchain past a certain date (Hertig 2016). This decision caused split opinions, with critiques saying that such a decision violated principles of self-governance. This somewhat ideological split lead to the creation of an alternative blockchain 'Ethereum Classic' based on protocol prior to DAO hack.[9] And again similar to the Mt.Gox hack failure of DAO hardly curbed or slowed down development of other 'smart contract' applications such as 'Expanse', 'Counterparty' and 'Lisk,' along with two 'Ethereum' blockchains and possibly many others.

The idea that computer code implemented on the decentralized blockchain can replace legal institutions seems captivating not only to developers and investors but also to some academic researchers. Swan (2015) points out that many systems of governance, such as property registry, provision of identification documents, and even registration of marriages, can be replaced by the decentralized blockchain services. Fairfield (2015) suggests that blockchain technology has a potential to disrupt and reshape existing legal norms regarding digital property rights. He argues that the law of intellectual property does a poor job safeguarding intangible digital property rights, and suggests a replacement in a form of a new law of information property that can also provide governance for distributed ledgers. Fairfield thus does not suggest a replacement of legal structures but rather a hybrid solution of 'Bitproperty'.

Wright and De Filippi (2015) comprehensively review existing and prospective blockchain technology implementations and come up with a prognosis that legal frameworks in the future might be radically transformed by the rise of cryptocurrencies, smart contracts and self-governed organizations. They suggest that a new type of techno-legal framework – *Lex-cryptographia* should be recognized and accommodated by existing legal institutions, in the form of a new body of law. Wright and De Filippi argue that implementation of complex systems of smart contracts and decentralized organizations may rewrite the basic tenets of property rights, constitutional rights and even judicial enforcement of law.

---

9 Although from the technical point of view creation is incorrect term, since 'Ethereum classic' is simply an existing blockchain, and rather forked version is strictly speaking a new one.

Each of these claims deserves a special consideration, but one of the most radical claims is that in the future property rights may vanish, becoming a subset of contract law. This can happen when physical devices such as cars, locks, guns and anything else with internet connectivity ('smart devices') will be managed on the basis of blockchain technology, in the form of lease, rent and etc. Wrigtht and De Filippi highlight this possibility along with other developments, but I will argue that this claim is in fact the most crucial point of argumentation on the nature of contradictions between existing legal institutions and blockchain technology.

Arguments on the nature of property and property rights are central to many issues on the nature of individual rights and government power to interfere with individual freedom, highlighting the number of descriptive and normative questions. This centrality of the property issue can be traced back to Aristotle's 'Politics' where he argues the necessity and limits of property for a good life (1257b) and justice in the polis regarding distribution of property (1266b). Arguments on the nature of property were central for such thinkers as Locke (1993), who argued that the very idea of government is justified by the institution of property. One, however does not have to subscribe to Aristotelean or Lockean views on the nature of society and state in order to suggest that the question of the nature of property precedes other considerations of the wider impact of blockchain technology on the shape and role of normative social structures.

Looking at the historical timeline of blockchain technology development, it is possible to say that the core idea behind it was an attempt to develop cryptographic certificates in the form of an immutable public ledger (Haber and Stornetta 1990), which later was developed to function as a ledger of monetary transactions and the Bitcoin protocol (Nakomoto 2008), effectively implementing the idea of basic monetary property. Granted Szabo (1997) theorised the possibility of smart contracts and smart property earlier, but practical implementation of blockchain started as digital currency first, followed by smart contracts, which in turn made possible blockchain enabled management of physical 'smart property' (Naraynan et al. 2016).

Bitcoin is not only the first successful application but genealogically also the most basic successful implementation of blockchain technology being focused on deliver-

ing functionality limited to monetary transactions. In technical terms, this means that the scripting language used in the bitcoin protocol is not Turing complete, basically having intentionally limited functionality, while the protocols used for 'smart-contracts' are essentially extensions of currency protocol with added functionality (Buterin 2014). Thus from the technical perspective as well, it might be fruitful to focus first on the most basic function of blockchain technology (monetary property) to assess its potential impact on the legal frameworks and other normative structures in society. It is also reasonable to engage first in the descriptive analysis of blockchain technology to see what functions it might have in the social context, before moving on the normative assessment of its role.

As an illustrative case Bitcoin and other cryptocurrencies present a flagship example of new normative structures of property that can function independently of legal institutions. The ground-breaking novelty of this approach to monetary transactions was suggested in the first paper by pseudonymous author Satoshi Nakomoto (2008), as a mechanism that essentially replaces third-party authority with the decentralized ledger. In practice it means that the copies the of ledger holding information about monetary transactions are held on different computers on the peer to peer network. In itself decentralized network holding information on monetary transaction is nothing new, the uniqueness here is in the fact that all functions traditionally executed by third parties such as currency emission, authorization of account holders, etc. are built in the network protocol. In that sense bitcoin network is indeed a complete institution of monetary property functioning alongside traditional institutions.

To understand the scale of such a claim it is necessary to clarify the concept of institution itself since it can refer to a number of social phenomena. In the most general sense institutions can be defined as normative entities, as kinds of social structures embodied by human agents, governed by rules, conventions and predefined ends. Miller (2001) points out that institutions can take different forms such as organizations, systems of organizations or even systems without organizations such as language, depending upon the scale of institution and its purpose. I argue that true novelty of the blockchain technology lies in the capacity not just to create new types of property but to create social institutions, that can be either complementary or competitive in regards to existing institutions.

Bitcoin protocol as an instance of blockchain technology provides an example of such an institution, namely an institution of property of the transnational scale. In that sense it can be characterized as a meta-institution, a system governing relations between individuals, organizations and other institutions. In that capacity it may not only reshape or enhance existing legal institutions of digital property as suggested by Fairfiled (2015), but rather meet all criteria of a parallel normative structure. Furthermore rights and duties constituted by such an institution of property can operate in a different modality compared to legal rights and duties, thus providing a qualitatively new system of property relations.

2.2. Normative and descriptive theories of property

What is possible to draw from the conceptual scheme of Bitcoin protocol, at a first glance, is a peculiar analogy between the chronological structure of bitcoin ledger, and both the property theory of first occupancy and Locke's labour justification for the property rights. The very first record in Bitcoin ledger called 'genesis block' is essentially a starting point from which all the following transactions take their legitimacy. In the particular sense this conceptual scheme is reminiscent of the idea that all property rights can be traced back to the very first property owner (Pufendorf, 1653/1993). In the other sense there is also reminiscence of Lockean (1993) argument that property rights are granted first to those who mix their labour with raw material.

With some stretch of imagination it is also possible to say that Bitcoin miners consuming electricity and applying computer power gain some new property titles, effectively justifying their property rights over newly emitted coins. In all fairness though this observations as entertaining as they may be hardly provide any insights on the philosophical aspects of blockchain technology. The most helpful observation that can be carried from this analogy is that system of property rights in Bitcoin has a bottom-up normative justification, similarly to theories of Pufendorf and Locke. Such justification stands in contrast with top-down approaches to property such as Humean one where the state grants its citizens property rights purely in virtue of its authority, and thus the very institution of property is seen as derivative from the state power (Waldron 2013). This, however, does not constitute a qualitatively new observation since from the early history of bitcoin development it was largely seen as a

libertarian enterprise, aiming to promote ideals of free markets and individual freedom (Karlstrom 2014). Thus it might be helpful to take a look at theories of property providing more substantial analysis on the necessary and sufficient criteria of property.

Despite being a straightforward idea in everyday life, the concept of property in academic research is anything but simple. This is hardly surprising taking into consideration the interdisciplinary nature of the property concept, but conceptual disparity also persists within the field of legal philosophy (Merrill and Smith, 2001). Waldron (1990) looking on the possibility of the general idea of property suggested broad definition of property as the concept of rules governing access to and control of material resource. Waldron focusing on the issues of moral justification of property however does not look deeper in the definition of property in most abstract sense, arguing that locating family resemblance of concepts is sufficient for his goals.

Same can be said about other theories focusing on the normative aspects of property institutions. Nozick (1974) in the vein of Lockean approach to property defines property rights as the right of owner to determine what should be done with property *X*, as bilateral permission between individuals to the use of things. Arguably this definition does not provide us with sufficient and necessary set of criteria that can be applied to determine whether *X* is property or not. Penner (1997) analysing Waldron's definition of property suggests that subtle evasions of thinking about why some things are objects of property and others are not, in fact are quite common for many normative philosophical treatises on property. Thus if one has to address the question whether blockchain technology applications fall into the categories of property, it might be helpful to focus first on the descriptive theories of property.

Broadly speaking two main descriptive approaches to the theory of property stemming from different motivations can be found in the contemporary philosophy of property. On one hand there is a bundle theory of property suggested by some legal scholar that aims to address the issue how property should be conceptualized within the legal framework, and on the other there is an essentialist approach which arguably aims to address the more abstract issue of the philosophical definition of property. Munzer (1990), one of the most prominent theorists of the bundle approach, distinguishes between a popular, simple conception of property as things

and a sophisticated conception as relations of persons in relation to things, latter defining legal understanding of property. Idea of property according to Munzer involves a catalogue of tangible or intangible things and catalogue of various relations that the owner has in regards to these things such as claim-rights, liberties, duties and liabilities and other basic legal concepts borrowed from the legal works of Hohfeld (1917) and Honore (1961). These relations as 'sticks' constitute a bundle that is called a property, giving a name to the bundle approach.

Penner (1997) suggests an alternative approach to the conceptualization of property aiming to distinguish an essential characteristic of property which he derives from the core right to exclude. In the broad conceptual sense property according to Penner can be considered as a system of moral standards institutionalized in the legal system. Penner as well as Munzer traces legal theory of property back to Hohfeld-Honore legal vocabulary, drawing from the Honore's distinction between norms *in personam* and norms *in rem*. Norms *in personam* capture rights of behaviour of some particular person, binding thus specific individuals, as in contractual obligations. Norms *in rem* on the other hand bind 'all the world', that is all subjects of legal system, such as preventing all except the landowner 'A' from trespassing the land. In Penner's interpretation norm *in rem* is a rule which applies to owners of property simply by virtue of their ownership. Furthermore everyone's relation to A (in regards to property) is *through* her property, when identity of A is irrelevant to the imposition of negative duty on non-owners, as opposed to norms *in personam*. This approach is also sometimes characterised as an exclusion theory of property (Merrill and Smith, 2001), as it captures the essential idea of property as right to exclude non-owners from the use of resources.

It may be argued that both bundle and essentialist approaches can be helpful to clarify the role and impact of the blockchain technology on the social norms and legal institutions. Bundle approach as argued by Munzer aims to grasp a variety of rights beyond exclusion, such as rights to use and alienate but also liabilities of property owners, thus better grasping the complexities of legal property systems, unlike essentialist exclusion approach. Furthermore, argues Munzer it is difficult to derive the complexity of these rights from single exclusion right as suggested by Penner. Application of bundle theory in this respect may be an interesting attempt to see whether property rights might be reduced to contractual obligations with the implementation

of blockchain technology as, Wright and De Filippi (2015) suggest. However this step would require first an analysis of blockchain as a form of property and this requires more abstract conceptualization of property above the practical understanding of the legal system. Whether one or another approach is better at grasping complexities of legal systems, is arguably not relevant to the scope of the current chapter, however above arguments suggest that application of Penner's essentialist theory of property might be a preferable preliminary step for the analysis of blockchain technology for two reasons.

First any attempt to grasp a new normative structure (blockchain) within the conceptual framework of an old normative structure (law) may fail to highlight some significant qualitatively new aspects. Indeed if we want to examine Wright and De Filippi's claims that legal property rights can be replaced by 'technological ownership', it might be helpful to go up from the legal level of abstraction and look at the philosophical conceptions of property, in order to avoid dead end metaphorical reasoning. As Van Hoecke (2011) argues legal research has rather narrow explanatory power as explanation taking place is largely an internal enterprise when nothing is 'explained' in analytic sense, rather values or principles are postulated, or some interpretation of a higher rule is posited, in order to legitimate the rule one derives from them. The same critique can be applied to Fairfield's (2014) theory of 'Bitproperty', which highlights some novel epistemic aspects of public ledger but largely sees blockchain technology as a mean to reinforce existing legal frameworks of digital property rights.

The second argument stems from the technical analysis of the blockchain technology, which is built on the cryptographic primitives. The very basic primitive of blockchain (and cryptocurrencies) is the digital signature, essentially a message encryption method that excludes everybody except the owner of private key from modifying the content of a message (Nakamoto 2008). In general sense all the added functionality is built on top of this principle in the logic of blockchain. And as in Penner's approach, the actual identity of a Bitcoin owner is irrelevant as long as the digital signature serving as a proof of ownership is valid. However before we can apply Penner's theory of property to blockchain, it is necessary to have a brief look at the basic concepts and the principles of blockchain technology illustrated with Bitcoin blockchain.

2.3. Short technical explanation of blockchain

Bitcoin is a good example of practical implementation of blockchain technology, being the most basic successful application and the most researched one. At its core are basic principles called cryptographic primitives, which can be considered as a conceptual building blocks of the blockchain functionality. Two such principles are 'hash function' and 'digital signature', some of the basic technical elements that need to explained for the proper understanding of bitcoin technology (Nakomoto 2008, Koblitz and Menezes 2016).

First primitive - hash function is essentially a mathematical function on the data input of any size that produces an output of a fixed length, which is efficiently computable (in a reasonable amount of time). Cryptographic hash function, has several important properties (Paar and Pelzl, 2009) but the following three are particularly useful for the implementations of cryptocurrencies such as bitcoin. First, hash function is *collision resistant*, which means that it is computationally infeasible to find two distinctive inputs producing a single output.[10] In practice this means that hash function can be used as a message digest, a tool to verify that a copy of a message is identical to the original. The second property is *preimage resistance*, which means that given just the output it is computationally infeasible to infer the value of input. This property translates into the application of binding commitment, similar to putting message in envelope and committing to its content. Once the message is put in envelope I cannot change my mind and alter its content. Thirdly if the hash function output is required to have a certain properties, for example first x bits should be zeroes, the task of finding such output given predetermined string and a variable integer (nonce) for inputs, becomes a puzzle which is difficult (computationally costly) to solve.

The first and second properties of hash functions are employed to build complex data structures using simple data structures – hash pointers as building blocks. Pointer in computer science in general and in data structures in particular is essentially a reference pointing out where information is stored, similar to the code in a

[10] This does not mean that two distinctive inputs producing a single output do not exist; rather, we believe that finding such a collision is not possible in practice, and the hash function is good enough.

library catalogue. Hash pointer in turn is a reference complemented with the short digest of the information it refers to, helpful for verification. Using hash pointers, it is possible to build a data structure in the form of blockchain giving the name to technology itself (Narayanan et al. 2016). Note that having puzzle is not a necessary requirement for data structures itself but is necessary for cryptocurrency to ensure that new data blocks are difficult to produce but easy to verify.

Real blockchain structures implemented in the bitcoin protocol are more complex than this scheme, but for the task of this chapter the given scheme can be considered sufficient.[11] It gives a general idea of a so called public ledger, a tamper evident (sometimes called immutable) data structure which may exist in the number of copies and there exist a reasonable (from the computational perspective) method to verify that all these copies and their respective elements are consistent. Note that any given moment of times copies of the ledger are not identical given that the last block of the chain always differs due to the network latency. These copies, however, have what can be called e*ventual consistency*, which means that the nodes will eventually agree on the block *x*. This concept of a ledger is crucial for the general understanding of bitcoin functioning.

The second cryptographic primitive used in the logic of blockchain architecture is a digital signature. As follows from the name, it is functionally a cryptographic method to sign a message digitally. In order to do that digital signature method uses asymmetric/two-key encryption. To draw an analogy, two-key encryption is essentially a lock with the pair of keys of which one only opens and another only locks. Now in digital form the opening key can be made public, and the locking key is kept private. Thus if someone encrypts a message with a private key and provides resulted output 'signature' together with a copy of original message, anybody with a public key can decrypt the signature to verify that indeed the message was signed by the private key holder (Paar and Pelzl 2009, Hoffstein et al. 2008). Considering that there might be only one private key, which only one person knows, this signature method provides a verifiable identity. Using a key pair and hash function it is possible to generate bitcoin 'addresses', which are essentially hashes of public part of key pair.

[11] Comprehensive study of the bitcoin architecture can be found in the excellent Princeton handbook "Bitcoin and Cryptocurrency Technologies" by Narayanan et al. 2016.

Combination of these two rather simple cryptographic methods allows for the essential construction of digital currency or cryptocurrency. To illustrate in a simplified way how this tools can be used for digital monetary transactions, let's consider monetary transaction between Alice and Bob. First Alice using generated key pair can create a digital message saying that she owns ten coins, and sign it with a private key. Next in order to make a transaction to Bob she adds another message to the existing one, which says that Alice sends ten coins to Bob, using Bob's public key as a name for transaction recipient. This however hardly counts as money yet, since all this holds merely on the convention between Alice and Bob, who agree to treat it as a transaction. What is necessary here is a guarantee of some sort that this digital cheque signed by Alice will be good once Bob wants to give it to somebody else (Koblitz and Menezes 2016).

In a traditional monetary system, guarantor of check validity is a third-party – Bank, holding record of all transactions, and guaranteeing their validity, essentially co-signing Alice's cheque. Crucial function of Bank is to prevent double spend, that is prevent Alice from giving copy of same cheque to multiple people. To ensure this Bank holds a record that first of all Alice has only 10 coins, and that she gave this coins away to Bob. Bank (if it is a central bank) also acts as an issuer of new money, this means that Alice cannot write a message 'Alice has 10 bitcoins' out of nowhere, but she has to write it on top of the verified message 'Bank gave Alice 10 coins'. This is in fact rather similar to how online banking works, as the bank computer holds records of all transaction. Of course in reality Alice might use other types of verification and bank might have multiple servers holding copies of ledger but the principle of single authority here holds.

Bitcoin replaces third-party authority with the distributed ledger built on the blockchain. Novelty of this approach to monetary system is that in practice the ledger holding information about monetary transactions is held on different computers on the peer to peer network. Blockchain data structure guarantees that all this copies are consistent across that network and the validity of any new transaction has to be guaranteed by the multiple nodes (computers running bitcoin client software) on the network. Ledger holding records of all transactions that ever took place guarantees first that Alice indeed has money she wants to send. Validity of new transaction is

verified not only on the basis of previous records about Alice's money, but it also has to be signed by her private key (Narayanan et al. 2016). This is very simplistic depiction of how new transactions are accepted on the ledger but it sketches a general conceptual framework of bitcoin.

Another ingenious aspect of bitcoin is the mechanism for the emission of new coins, which is tied to the process of how new transactions get recorded in ledger. This can be explained with the earlier mentioned puzzle like properties of hash function. Bitcoin protocol requires that all records on new transactions has to be combined in data blocks of fixed sizes and properties, such as that hash of this block has some predetermined certain properties. Search for such output crudely speaking is a puzzle, of how to achieve this output with using existing inputs (transaction data). Some nodes of the bitcoin network may try to solve this puzzle by trying different solutions to achieve desired output, and propose this block for the whole network to be accepted as a newest record on ledger. In order for a block to be accepted by network participants, the participants trying to find such block (solve a puzzle) must complete a proof of work which covers all of the data in the block. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block.

Node that succeeds thirst in solving puzzle gets a reward of fixed size according to rules of protocol, essentially creating new coins. Size of a reward is a value decreasing in time while difficulty of puzzles is increasing progressively, thus by design the supply of bitcoins is limited, and emission of new coins will eventually stop. Some other technical aspects left behind the scope of current chapter present interesting points of philosophical and ethical enquiry, such as fairness of mining capacity distribution, whether bitcoin network can be truly decentralized,[12] or whether identity based on digital signature is truly anonymous.[13] However this short schematic illus-

[12] In theory concentration of 51% of hashrate power in hands of a single agent can allow him to control which blocks are accepted first creating a possibility of double spend. Though in practice this scenario is considered largely economically unviable, since such agent would have to carry significant costs accumulating hashrate power, that would not be covered by such double spend attack.

[13] Bitcoin users are in fact can be deanonymized at the moment, but this can be seen as temporary state of affairs, since greater obfuscation of user identity can be built on top of Bitcoin protocol. Significant research efforts in this area also bring new cryptocurrency protocols, providing greater anonymity such as Monero (https://getmonero.org/) and Zerocash (https://z.cash/).

tration of Bitcoin mechanics is sufficient to answer whether blockchain protocol can provide a functionality of property institutions.

2.4. Applying theory of property to blockchain

Realisation of property idea according to Penner (1997) is a legal structure of property laws serving as individuation of duties, powers, rights and permissions relating to fundamental interests or interactions of fundamental interests. While Penner does not elaborate on the underlying theory of interests, it is possible to say that by interest he means, a function of legal right to further right holder's interests. Thus in order to grasp the idea of property one has to understand the interest behind property ownership to highlight its conceptual essence. Such interest argues Penner is the interest in exclusively determining use of things. Following from this the essence of property is exclusion of non-owners from the determination of property use. Penner also highlights that it is a negative liberty that serves only to the extent that freedom of the interference of other does.

This essential idea of property allows Penner to derive the answer to the question what 'things' are property – sufficient and necessary criteria. First criterion for property is characterized by Penner as an exclusion thesis, which states that the right to property is a right to exclude others from things which is grounded by the interest we have in the use of things. Here use and exclusion are two sides of the same coin, as on one hand exclusion is not a goal to itself but rather it reflects owner's purposeful dealing with things, on the other owner excludes non-owners from the use of these things. As such property rights, according to Penner are *in rem* rights, creating negative duties for all non-owners even if they have no contractual relations with the property holder.

Application of this criterion to the concept of the coin ownership on the Bitcoin blockchain is rather straightforward. Indeed the core idea behind basic cryptographic tools is to exclude non authorized individuals from the use of encrypted data, be it a message, data base or bitcoin wallet. Significant distinction here is in the modality of property rights. While legal framework creates duty for non-owners not to interfere in the sense of permissibility (Penner 1997, Ripstein 2013), property rights implemented in the blockchain protocol operate in the sense of possibility. Two-key

asymmetric encryption used in bitcoin digital signatures, essentially guarantees a right to the holder of private key to exclude others from using coins. Exclusive use here means that owner of bitcoins can have sole disposition of them, transfer them using blockchain, sell them for other currency, or gift away as paper wallet (key pair printed on the physical media).

This corresponds with Penner's analysis of the mechanistic aspect of social use of property, which he compares with a gate rather than a wall. Penner also notes that right to exclude others in real legal practice is not necessarily full liberal ownership, i.e. it is not absolute and can be overridden by legitimate state power. This observation highlights an interesting aspect here since cryptographic ownership is certainly much closer to this ideal liberal ownership than any legal ownership, as modalities of permissibility and possibility rights conflate on the blockchain. Of course precedents of bitcoin confiscations from infamous 'Silkroad' dark market owners by US government show that bitcoin in practice is also not necessarily constitute absolute ownership (Kharif 2014). However it is necessary to point out that this example is rather a case of security breach and in theory bitcoin owner who keeps his real life identity separate from his bitcoin addresses kept offline can enjoy pretty almost absolute ownership (insofar as necessary infrastructure exists).

Second key criterion for the property Penner calls a 'separability thesis', that is ownership of things that count as property is contingent or conditional. Ownership of a property does not presuppose any special immutable relationship with it unlike say ownership of a talent. This argues Penner makes property rights transferrable, as when property rights are transferred from one person to another this does not alter the nature of property and duty of all other non-owners to be excluded from it. Indeed one can exclude others from enjoying her singing talent, but it is hardly means that given talent itself is her property. Thus separability in Penner's view constitutes a necessary supplement criterion to the exclusion thesis. 'Thing' here is a conceptual criterion which restricts the application of property rights to those things in the world which are contingently related to us and which contingency may change given the changing personal, cultural or technological circumstances. Bitcoin fully satisfies separability criterion, offering multiple modes of ownership change, not only in form of transaction on the blockchain, but also in form of physical transfer of key pair (on external hard drive or even paper).

It is possible to say that from the Penner's point of view coins on the Bitcoin blockchain do count as a property in all senses of that word, since bitcoins both satisfy exclusivity and separability criteria. This however does not fully explain all aspects of blockchain property for one important reason. As aforementioned, in theory cryptographic ownership can be an absolute ownership, which excludes anybody from interference in ownership rights. This is nicely illustrated by the ongoing debate over privacy, smartphone encryption and rights of government institutions to interfere with it. Apple iPhone encryption which recently became a centre of government lawsuits and media attention, uses cryptographic key built into physical architecture of the device, which makes it (key) unique (Zetter 2016). Thus only owner of the device with the knowledge of password can use it, effectively excluding anybody, even manufacturer and government agencies from interference.

Here cryptographic ownership effectively trumps some of the legal ownership rights. Nevertheless government agency such as police can take physical possession of device thus effectively excluding the person with password from its use. Bitcoins owner in contrast may enjoy (if she upholds necessary security measures) absolute non-interference from anybody else. To get a better idea of the absolute possession of property it might be helpful to turn to a historical conception of property developed by Hegel (1991). Unlike other historical philosophical conceptions of property such as Lockean theory which is largely normative, Hegel's account of property developed in 'Philsosophy of right' can be considered as much a descriptive theory as it is normative (Waldron 1988). From a general point of view Hegel's theory of property is also a bottom-up justification of property, where property rights occur when will of an individual is placed in the 'thing', being derived from an individual freedom and not from the government authority, thus the starting point in Hegel's reasoning is to define the idea of property in its absolute form (Waldron 1988, Penner 1997). It is important to notice that Hegel does not suggest on this basis that property rights are absolute, and can overrule state interest (Brudner 2013), but it can be argued that his normative considerations on the structure of law do not constrict explanatory value of his descriptive analysis.

The key interest for us presents a nature of property ownership as suggested by Hegel. He distinguishes three modes of possession for things. Physical seizure is

the immediate mode of possession, but subjective temporary and limited in scope, followed by the second mode which is giving something a form which extends will presence from immediate time and space. Third mode of possession is an indication, marking of a thing with one's will, and according to Hegel this is the most complete mode of all (Hegel 1991, § 58). Completeness means that marking a thing is an ultimate sign to others in order to exclude others and show them that I have put a will in the thing. This mode turns mere possession into property. It is an elaboration on the statement that for thing to count as a property it has to be recognized by others as such (Hegel 1991, § 51). In 'Philosophy of Mind' Hegel (2007) draws this conclusion from the idea that person's freedom and independence comes into existence as being of other persons, relation to them and recognition by them. Property for Hegel is another externalization of person's will and freedom coming in the existence through recognition by others (Brudner 2013).

This thesis highlights probably the most significant aspect of blockchain ownership, as in addition to the exclusion and separability, bitcoins have this third important aspect – universal recognition by the other users of blockchain as property. This seemingly trivial observation unpacks not only similarity of bitcoins to other types of property but also its uniqueness. In the simple sense all kinds of property indeed can be regarded as a social convention, recognition of property rights of owner and negative duties of non-owners (Waldron 1988). Implementation of such convention in complex society requires some kind of universal access to the knowledge about property rights of each individual. Government and other legal institutes providing access to this knowledge perform such function of epistemic access for citizens within the apparatus of property institution.

The uniqueness of blockchains are two-fold: not only do they eliminate a need in third-party authority for the enforcement of exclusion rights, but they also provide a system of universal access to the knowledge about property rights of all bitcoin owners.[14] Together with the exclusion and separability, this in fact makes blockchain technology a self-sufficient alternative institution of property existing independently

[14] Access to ledger records does not have to be completely open for functioning cryptocurrency. Unlike Bitcoin ledger which is fully transparent, privacy focused Monero blockchain works differently. It uses different protocol 'Cryptonote' where nodes check only group identities of addresses, which helps to obfuscate individual users, nevertheless principle of public ledger holds, see Van Saberhagen (2013).

of any legal institutions. In that sense all the collusions and contradictions of bitcoin with legal systems are rather understandable, since they can be seen as competing normative structures. The true scope of such blockchain institution of property is yet to be seen, but it can already compete with global intermediaries serving as a trusted third parties guaranteeing international monetary transactions such as SWIFT (Skinner, 2016). This also explains why most attempts on the national scale to regulate blockchain technology targeting miners and exchanges are likely to be unsuccessful, since such organizations are only elements of a larger normative structure.

For future analysis it is also crucial to clearly disentangle norms and ideas present in specific implementations of blockchain technology from the very capacity of a technology to deliver these norms as an institution. Indeed, as any other institution embodied by human agents, it can also incorporate the norms and beliefs of individual members or organizations constituting it. But in its design capacity blockchain protocol is essentially agnostic towards social or moral norms that can be delivered or ignored by the implemented system.

2.5. Conclusion

Looking at the blockchain as an institution of property helps to grasp the uniqueness and novelty of this technology in the social context. Of course it is still very early to conclude that some of the blockchain applications will be able to replaces legal norms and property rights. Yet it is already possible to see how some aspects of property relations in society are being replaced with blockchain. One example of such hybrid institution of property is a distributed ledger that can hold information about intellectual property of right holders instead of centralized government database (Ha 2016). One next possible step is the implementation of property rights for physical objects such as Internet of Things applications, that can eliminate some functions of third-party authorities for the enforcement of property rights (Brody and Pureswaram, 2014).

In that respect some of the forecasts by Wright and De Filippi look more and more plausible. My only point of disagreement with them is their hypothesis that wider blockchain implementation, can lead to the disappearance of property rights. Whether wide adoption of share economy will affect distribution of property in soci-

ety is of course an open question, answer to which is yet to be seen. But the blockchain technology in itself does not necessarily lead to the dissolution of property rights in society. On the contrary blockchain may help to extend and enforce individual property rights in new domains, such as ownership of private data (Zyskind et al. 2015). Of course there is no denying that blockchain may carry a significant threat to the existence of some legal institutions of property in the future, but in the bigger picture blockchain technology among other things should be regarded as a new type of property institution, as another implementation of the philosophical idea of property rights.

3. Rethinking trust in the Internet of Things

3.1. Introduction

Trust is often hailed as the key component of successful Internet of Things (IoT) developments, from technological research papers to policy recommendations and corporate business strategies. Needless to say, different conceptions of trust in technology have had a fair share of use in practical studies on the social acceptance of new technologies such as Genetically Modified Organisms, Nanotechnology and others. Indeed, as Am (2011) suggests, trust as a conceptual tool can be used for the purposes of social studies such as enquiries into whether the general public possesses sufficient understanding of new technologies. It can also be incorporated to assess future perspectives of technology adoption in society, or as a crucial element of risk perception assessment by the various stakeholders. Many studies on public trust in the IoT operationalise trust in more or less a similar fashion.

Some of the key considerations of the EU commission staff working document 'Advancing the Internet of Things in Europe' (EC, 2016) are informed by the IERC position paper 'IoT governance, privacy and security issues' (IERC, 2015). This study points out that in order to make a positive impact on people's life, technology has to be trusted and accepted. Thus, citizens' distrust in IoT technology-based systems and services can be a serious obstacle in the reaping of technological benefits. The report 'Europe's policy options for a dynamic and trustworthy developments of the Internet of Things' suggests that a proper implementation of ethical tools such as informed consent can ensure trust in the systems and thus social acceptance of the technology (Schindler et al. 2013, Tragos). 'Alliance for the Internet of Things innovation' (AIOTI, 2016) in the opinion report 'Digitisation of Industry Policy Recommendations' suggests that public trust in the IoT is a key factor determining speed of adoption, and refers to a number of surveys highlighting trust and a perception of risks by the users.

Indeed, trust can be said to be a crucial element of a functioning modern society. Interpersonal and institutional types of trust are essential as they provide the possibility of cooperation and enable the functioning of many mundane aspects of everyday life (Govier 1997, Hardin 2002). Furthermore, one of the key aspects of trust is a

capacity to reduce complexity, to represent social reality with simplified symbols and provide generalised expectations for actions (Luhmann 1979). However, such simplifications can also be irrational or unwarranted. Trust, therefore, is not something that is univocally good, or something that should be universally desired in all contexts (Baier 1986, Gambetta 2000). As Govier (1997) points out, while it is tempting to think that we can improve our social world by introducing 'more trust', it is not necessarily always the case. The other side of trust is represented by the vulnerabilities and risks that a trustor embraces when he or she acts on trust (Hardin 2002, Govier 1997, Baier 1986). Thus, even outright distrust can be morally justified in specific contexts, and this observation invites us to consider the real value of trust in the IoT.

Arguably, such an investigation is not a task for a single research paper, since the multitude of meanings and concepts involving trust in the IoT technology are further extended in turn by the broad definition of IoT. Still, it is possible to highlight the most pressing ethical concerns by looking at the key regulatory proposals in this area. A number of expert opinions, research papers and policy advisory reports (Miorandi et al. 2012, Aggarwal et al. 2013, Sicari et al. 2015, Ziegeldorf et al. 2014, Pagallo et al. 2017) highlight risks of IoT applications for the privacy of their users as a key issue in the future developments and implementations of these technologies. This narrows down the research scope to user's trust regarding private data protection in consumer IoT applications. Consumer applications here refer to the systems falling into the categories of specific IoT developments aimed at individual consumers: Wearable Computing, Quantified Self and domotics, in contrast to business-to-business applications and infrastructure solutions (WP29, 2014).

While ambiguity of the IoT definition is understandable in the context of emerging technology, vagueness of the 'trust' concept itself may come as surprise to some. Yet within a range of disciplines, trust remains a 'fuzzy' concept, in stark contrast to the everyday intuitive understanding of this word (McKnight & Chervany, 2001). Furthermore, as McKnight & Chervany argue, measurements of trust often outstrip meaningful conceptualisations, which seems to be the case in the context of IoT trust as well. This is not merely a matter of scholarly debate, considering that the choice of trust conceptualisation in policy proposals and technological designs can have very direct ethical consequences, as demonstrated for instance by the example

of 'Trusted Computing' (Anderson 2004, Monti 2010). As a starting point of investigation this chapter considers the widely adopted analytic definition of trust as a tripartite relation between trustor A trusting B (human or system) in regard to C. (Luhmann 1980, Govier 1997, Baier 1986, Taddeo 2010, Hardin 2002). This formulation can be used to define a user's (A) trust in the family of technical systems, unified by the consumer IoT label (B) to keep the user's private data protected (C).

More specific conceptualisations can highlight different aspects of this multifaceted phenomenon, and the choice of an appropriate definition may either put associated moral issues in the spotlight or gloss over them. To address the question of trust value, section 2 of this chapter considers different definitions of trust such as *psychological trust, rational trust* and *trust in technology*. Addressing these distinctions highlights shortcomings of trust conceptualisations used in opinion surveys and policy recommendations which operationalise trust in the narrow instrumental fashion as a mere precondition for cooperation. It is argued that such conceptualisations tend to neglect the distinction between justified trust and trust as mere psychological disposition, ignoring the issue of trustor's vulnerability highlighted in moral philosophy (Baier 1986, Govier 1997). A shortcoming which is exaggerated by the observed malleability of dispositional attitudes of trust in the context of privacy related behaviour (Acquisti et al. 2015, Adjerid et al. 2016). These findings urge us to consider rather *trustworthiness* of IoT systems as a focal point of concerns, which is a foundation of rational trust.

Section 3 defines objects of trust in IoT using reference models and highlights distinctive issues apparent from this analysis. Rational trust can be valuable insofar as it helps individuals choose optimal strategies of interaction with complex systems (Luhmann 1979, Taddeo 2010). However, IoT systems represent a case of trust in hybrid (part technical and part social system, where establishment of *system trustworthiness* is a non-trivial task (Nickel et al. 2010). This task can become almost impossible for the individual users considering information asymmetries and power disparities between suppliers and consumers of IoT systems (Stajano 2003, Andrejevic 2014, Christl and Spiekerman 2016).

Analysis of current IoT reference models also shows a tendency to conflate issues of data security and private data protection. While both these issues are closely intertwined, they refer to distinctive concerns both in empirical and conceptual senses (Stajano 2003), pointing to the difference between trust in data protection and trust in the security of data. I argue that these concerns compel us to embrace a Human appreciation of distrust as a starting premise for the design of social institutions. Inspired by this approach, Section 4 considers technological and regulatory solutions that can be used to enhance trustworthiness of IoT systems and at least partially remove the burden of trust justification from the users of the technology.

3.2. Conceptualizations of trust

3.2.1. Trust as an instrumental value

The concept of trust can have a crucial role in measurements of public attitudes towards a new technology. Expressions of trusting attitude or lack of it can serve as indicators of the social acceptance for a new technology. However, we should be wary not to slip into descriptive reductionism, conflating acceptance with moral acceptability of technology, as happens too often with private data collection tools. I argue that while existing policy proposals highlight some of the ethical concerns regarding unwarranted trust in consumer IoT systems, our understanding of trust in this context should be significantly extended to include other crucial issues. Granted, interpretations of 'trust' can vary dramatically throughout different areas of discourse and such descriptive pluralism, of course, is not itself problematic, as other contested concepts demonstrate.

The issue here lies rather with the fact that the concept of trust in policy proposals and opinion reports is often treated in a rather particular, normatively laden sense. More specifically, the value of trust in the IoT is usually interpreted in a narrow instrumental fashion, where users' trust is considered a pathway to acceptance that can enable all positive developments of the technology (Yan et al. 2014, Sicari et al. 2015, AIOTI 2016), and even as a remedy to the moral dilemma of choice between privacy risks and technological benefits (Schindler et al. 2013). There is a concern that such studies using methods of focus groups and surveys may lack explanatory depth when applied in the context of emerging technologies (Am, 2011). Indeed, apprehensions about surveys aimed to reveal public attitudes towards the IoT, are

reminiscent of earlier concerns towards the validity of such methods in assessments of public perception of nanotechnologies highlighted by Am.

Some limitations of such surveys come from misplaced assumptions that it is possible to have unified responses or attitudes towards early technologies that are actually not yet fully presented at the markets (Davies et al. 2010, Am 2011). This point of critique may well be justified in the context of IoT technology surveys. While some applications classified as the IoT can already be found on the market, they are fragmented in separate categories such as fitness wearables or smart home systems and thus are not necessarily perceived as a single technology (Uckelmann et al. 2011, Miorandi et al. 2012, Gubbi et al. 2013, Sicari et al. 2014). Furthermore, it is safe to say that full implementations of interconnected sensor systems utilising all aspects of envisioned IoT architectures are still not present in consumer markets in a meaningful sense (Pagallo et al. 2017). Thus, conceptualisation of generalised trust in some broad family of technological artefacts can at best serve as a reflection on attitudes of a general optimism towards the idea of technological advancement.

Another, arguably more problematic shortcoming of trust conceptualisations used in reports and opinion surveys is highlighted by Davies et al. (2010). When benefits of technology acceptance are framed in economic terms with little examination of the relation between promised benefits and wider social values, conceptualisations of trust tend to slip into the so called 'deficit model'. In such a model, trust in technology is treated as a scarce resource, and deficit of understanding/trust is seen as something that should be compensated to advance adoption of the technology. The main problem with such a conceptual approach where trust is treated as a scarce economic resource, is that it often fails to distinguish between cases of desirable and misplaced trust (Gambetta, 2000). The IoT public opinion surveys indeed are mainly framed in economic terms where trust is construed as an attitude of technology's users which should be elicited to guarantee successful developments of the IoT based business models.[15]

[15] Some interpretation of trust in more technical papers on IoT are also reminiscent of this model (Yan et al. 2014; Sicari et al. 2015). However, in this context it is crucial to be aware that interpretations of users' trust can be mixed up with technical problems of 'trust management' and 'trusted system', which have a very specific meaning in the context of cybersecurity. As Yan et al. (2014) acknowledge, little work in technical research on the IoT pays specific attention to the human-computer trust. Considering that the concept of trust in computer sciences should be seen as a motivating concept underlying many problems and contexts rather than a precise idea, some inevitable conceptual blurring should be expected (Artz and Gill, 2007). This issue is partially addressed in section 3 of this chapter.

3.2.2. Psychological attitude of trust

The shortcoming of the 'trust deficit' theoretical framework is even more pronounced in the context of trust in private data protection, as highlighted in empirical studies on privacy related behaviour of technology users. Acquisti et al. (2015) address the so called 'privacy paradox' - an observed discrepancy between privacy preferences reported by the technology users in surveys and actual decisions regarding protection of their privacy. The gap between expressed preferences and the actual behaviour can be quite significant as individuals' privacy decisions are not only highly contextually dependent, but can also be influenced by a number of external factors. In order to understand this phenomenon, it is helpful to introduce a conceptualisation of trust referring to *psychological attitude*, which can be defined as a generalised expectancy held by an individual that the word, promise or statement of another individual or group can be relied upon (Rotter, 1980).

Such an attitude or expectancy can be elicited by mere signalling – an *imitation of trustworthiness*, such as the presence of data collector's written privacy policy which has no real impact on the actual data sharing practice (Hoofnagle and Urban, 2014). Brandimarte et al. (2013) also find that mere increase in a perceived control over access to private data online, brings about an increased likelihood of sensitive, risky disclosures. These observations render base default assumptions present in the 'deficit model' highly problematic. Namely, the premise that the users of technology rationally justify their trust in providers on the basis of all available knowledge about benefits and costs of technology in the fashion of fair contractual relations. Empirical studies show this couldn't be farther from the truth, as privacy decisions and trust attitudes of technology users are subject to biases, habits and manipulations (Oulasvirta et al. 2012, Brandimarte et al. 2013, Acquisti et al. 2015, Kim 2016, Adjerid et al. 2017).

Of particular interest here is the experiment by Oulasvirta et al. (2012) on the privacy perception of in home surveillance by means of integrated multiple sensor systems. One of the key findings of the experiment was suppression of privacy-seeking behaviour when it came into a conflict with convenience associated with being at home. After three months, most participants of the experiments started tolerating home surveillance as a feature of everyday life. At the same time, Oulasvirta et al. found

that the acceptance of surveillance did not eliminate feelings of anxiety and discomfort associated with the invasive data collection, characterising new behaviour routines as fragile, and easily challenged by new events. This observation aptly demonstrates differences between rational behaviour and acceptance of technology, often misrepresented by data collectors, as a manifestation of a legitimate user's trust.

Such acceptance is closely intertwined with what Luhmann (1978) calls a routinised, thoughtless trust based on familiarity. Kim (2016) found in an experimental study that anthropomorphic features in IoT appliances such as individualised voice control interfaces, can elicit more positive attitudes towards appliances, including an increase in the perceived trustworthiness of the appliance. This, argues Kim, is explained by the fact that human responses to computers tend to be not only social, but also mindless, occurring because of reduced attention caused by the predominant reliance on the previously established social rules and categories. Such apprehensions about the malleability of users' trust cause significant concerns, as more IoT application such as 'Amazon Echo' and 'Google Home' use natural language processing and other technologies imitating human-like interactions.

These findings present special concerns with regards to Internet-connected children's toys that not only present a significant threat to privacy, but are also specifically designed to elicit trust attitudes from a child (Taylor and Michael 2016). As Luhmann (1978) points out, rational trust is a processing of experience that takes a lot of energy and attention and requires auxiliary mechanisms such as learning, symbolising, controlling, and sanctioning. As studies above demonstrate, even adult users of technology faced with the increasing complexity resort to less than optimal strategies of trusting behaviour, being unable to assess the actual *trustworthiness* of IoT systems on their own. This type of behaviour falls short of delivering the benefits of reduced complexity, whilst retaining all the risks of trust.

These observations suggest that the instrumental focus on trust in studies regarding acceptance of the IoT technology characterised by the 'deficit model', can present significant shortcomings. Such a narrow instrumental interpretation of trust stems from what Hardin (2002) calls a 'conceptual slippage', the reductionist notion of trust as a mere epistemological primitive, and not a subject of analysis. Indeed, if

trust is reduced to a univocally desirable attitude towards technology, and distrust as a mere obstacle to the realisation of benefits promised by technology, then the issue of users' trust in technology risks being reduced to the question of how to elicit such an attitude. These are worrisome prospects, considering that incorporation of perceptual cues eliciting psychological attitudes of trust in users is becoming an explicit subject of consumer technology design (Nickel, 2015).

3.2.3. Trustworthiness and moral aspects of trust

To appreciate these concerns, we can focus on the notion of *rational trust*, which tackles issues of trust and trustworthiness from rather different perspectives than psychological accounts. Taddeo (2010) suggests the following definition of trust based on a general relational account: trustor (A) chooses to rely on a certain party, or trustee (B), to perform a certain action (C); and this choice rests on the assessment of the trustee's trustworthiness. Trustworthiness here is understood as a measure (for the trustor) which indicates the likelihood of benefitting from the trustee's performance, and conversely, the risk that the trustee will not act as expected. This definition of trust focuses on one crucial aspect of such relation - reduction of complexity valuable to the trustor in Luhmann's (1978) sense.

Taddeo (2010) argues that such an interpretation of trust can also be extended to explain instances of depersonalised relations, mediated by the technology. Such *e-trust* can occur in the context of a digital environment where social and moral pressure effects, playing crucial role in physical environments, are perceived differently. However, considering the ever-blurring boundary between 'offline' and 'online', distinguishing e-trust from trust becomes a more difficult task. This is even more so the case in the context of IoT solutions that effectively blur this distinction to the point where it is no longer meaningful. Thus, speaking of trust involving communication technology such as IoT, we effectively consider e-trust as well. E-trust, argues Taddeo, has same valuable property of reducing complexity for the trustor, which makes it as fundamentally important as trust in persons and social systems, as highlighted by Luhmann (1978). This approach focusing on the value of trust for the trustor, is distinct from the interpretation of trust value found in the 'deficit model'.

There are moral reasons for this focus deriving from the fact that trustor (A), giving discretion to act on one's interest, is subject to the risk that trustee (B) will abuse this discretion (Hardin, 2002). Indeed, if that was not the case, we would speak of predictability or control, rather than trust (Nickel et al. 2010). Trust is also different from mere reliance, exposing the trustor to different types of vulnerabilities (Baier, 1986). There is a distinction between being disappointed by the poor performance of a trustee or being betrayed and harmed by the trustee's actions. It is also suggested that the presence of so called 'reactive attitudes', or availability of moral judgments on the trustee's actions as being praiseworthy or blameworthy, characterises such moral aspects of trust. Nickel (2015) suggests that same distinction is applicable as well in the situation where the object of trust is not a person, but a technological artefact or technological system. He defines *trust in technology* simply as the voluntary disposition towards reliance under condition of uncertainty, involving the attitude that technology should promote or protect the interests of a trustor.

The presence of such reactive attitudes in itself does not necessarily warrant moral concerns. After all, being angry with a TV does not necessarily make it an instance of betrayed trust. Tavani (2014) suggest an approach to the trust in technology which considers vulnerability of a trustor as a key factor of moral concerns. That is, if a human engages in a direct interaction with the technological system on the basis of expected functionality, and such interaction makes him vulnerable to risks, then this type of relation presupposes strong trust. Strong here means that such morally robust relations warrant a set of moral considerations similar (albeit not fully equivalent) to issues regarding trust between human agents. In the context of trust in private data protection, these vulnerabilities can be quite significant, involving information-based harm, informational inequality, informational injustice and undermined autonomy (van den Hoven, 2008). From that perspective smart TVs, which secretly share its owner's private data with different third parties, do seem to fall into the category of betrayed trust.

However, moral aspects of trust are not exhausted by the simple distinction between warranted and unwarranted trust. As Taddeo (2010) notices, emergence of rational trust in real life contexts involving human agents depends upon complex and shifting conditions, making it difficult to assess benefits of trust a priori. Indeed, if the distinction between morally acceptable and unacceptable instances of trust relations

could be reduced to the idealised notion of rational trust, then data collection practices based on the 'choice and notice' model would be rendered largely unproblematic. However, malleability of individual behaviour regarding disclosure of private information in the context of interactions with technology (Oulasvirta et al. 2012, Brandimarte et al. 2013, Acquisti et al. 2015), highlights two key moral issues: distribution of power and conflicting interests in trust relations.

The first is more than just an issue of power imbalance characterised by the uneven distribution of risk and benefits, which generally occurs in any trust relation.[16] Baier (1987) highlights a significant distinction between the cooperative trust occurring between equally distrusting peers standing in approximately balanced positions of power, and trust between parties who had uneven power distribution beforehand. If a trustor's standing beforehand was disadvantageous then it can be further undermined by the incurred risks of trust relations. Thus, in cases where the trustee has a significant advantage over the trustor, such an arrangement should at the very least be treated cautiously. Furthermore, if such an asymmetric trust relation takes place on the background of conflicting interests, we simply cannot speak of any rational trust at all.

It seems that both these concerns are present in the case of user trust in the IoT. The increasing complexity of data-collecting technology coupled with users' lack of technical expertise, prevent said users from properly assessing the risks and benefits (Stajano 2003, Andrejevic 2014). In this sense, power imbalance manifests as information asymmetry between suppliers of the technology and the individuals affected by it, whom are often oblivious to its true capacity, or even of its presence. What is arguably even more problematic is that economic incentives seem to drive interests of the consumer IoT suppliers further away from the interests of individual users in regard to private data protection, echoing the paradigm of moral failures which characterise the online advertising industry (Christl and Spiekerman, 2016).

Given this analysis of the value of trust, it becomes apparent that the problem of trust in the IoT is not a descriptive question of why the users do or do not trust in

[16] Indeed, generally, a trustor delegating certain actions to the trustee prior to the promised benefits thus carries immediate risks. A trustee, on the other hand, defaulting on the obligation, gets immediate benefits, while carrying only the probability of future risks such as sanctions, reputation damage, lack of future cooperation etc. (Hardin, 2002)

technology. Showing that people trust in technological design does not imply that it is trustworthy, nor the other way around (Nickel, 2015). It is first and foremost a normative question of whether individuals can rationally trust in IoT technology, which in turn hinges upon whether IoT technology can be made trustworthy in respect to private data protection. Only after an affirmative answer to that normative question it is possible to start addressing the issue of how the scrutiny of trustworthiness can be made available to the users of technology, the second condition necessary for the emergence of a rational trust. Trustworthiness of the IoT technology can be considered a viable concept insofar as we can speak of trustworthy technology at all (Nickel et al. 2010, Nickel 2015, Tavani 2014). It is not immediately clear though whether we should consider trustworthiness of smart devices, networks, technology suppliers or service providers. Thus, the next necessary step is to address the question of the objects of trust in the IoT.

3.3. Objects of trust in the IoT

3.3.1. Reference models and architectures

The term IoT is, firstly, an encompassing label which designates a technological model for a wide range of emerging products and services, thus making it hard to identify immediately specific objects of trust. This issue is apparent in light of the observation that 'IoT' being an umbrella term includes a great multitude of technologies such as various wireless communication protocols, sensor technologies, encryption protocols and many others. Neither is it possible at present to identify exemplary flagship products representative of the whole range of consumer IoT designs (Pagallo et al. 2017). One way to tackle this ambiguity is to define IoT as any system fitting into a certain design paradigm. The EU commission staff working document on 'Advancing the Internet of Things in Europe' characterises the first stage of IoT development as an ecosystem where all objects and people can be interconnected through communication networks in and across private, public and industrial spaces, and report their status and/or about the status of the surrounding environment (EC, 2016).

From the system-level perspective the IoT then can be defined as a highly dynamic and radically distributed networked system, composed of numerous smart objects that produce and consume information (Miorandi et al. 2012). Architectures of IoT

can have different levels of decentralisation (Ning 2013) depending upon the scale and complexity (Miroandi et al. 2012, Mashal et al. 2015). This also means that some entities in such a model may be comprised of networks including multiple actors, having various roles in distributions of data flows. The way to provide a more specific conceptualisation is to consider the IoT reference model with a particular architecture and system logic, present in most products and services employing smart objects. Gubbi et al. (2013) define key enabling components of the IoT: (1) Hardware - including sensors, actuators and embedded communication hardware; (2) Middle layer - on demand storage and computing tools for data analytics; and (3) Presentation - interfaces, easy to understand visualization and interpretation tools and applications.

Conceptual similarity to this tripartite scheme is also suggested in the three-layer model of IoT, which often serves as a generic reference model (Ning 2013, Yan et al. 2014, Mashal et al. 2015, Pagallo et al. 2017).[17] The first layer is the sensory layer (perception) which includes different sensors and actuators, the function of which is to identify objects, collect information and perform actions to exert control. This layer essentially comprises hardware, including RFIDs, MEMs, cameras, GPS, WI-FI modules, Bluetooth modules and so on. Second is the network layer which includes a variety of communication channels, interfaces, gateways and information management of the network. This layer is comprised naturally of the Internet itself but also of all other types of mobile networks, ad-hoc networks and closed-circuit networks. The network layer in this model also includes data coding, extraction, restructuring, mining and aggregation. Third is the application layer which provides applications and services to the IoT end users, and is essentially an interface offering diverse functionalities. These interfaces can be embedded in smart objects, be implemented in the form of smartphone apps or web-based applications.

Using the conceptualisation provided by the reference model, we can attempt to make sense of a notion of a trustworthy IoT system. Here it is helpful to reflect on the meaning of *trustworthiness* in a technological context. In the most general sense

[17] Some other layered models of IoT expand this conceptual structure to five or more layers, expanding data processing or data management into separate categories such as middleware layer comprised of a software (Ning 2013, Mashal et al. 2015). Here I agree with Pagallo et al. (2017) who argue that in the context of policy analysis, the three-layer model provides sufficient explanatory depth and has a further advantage of complementing the basic architectural levels of IoT.

in computer security, a trustworthy technical component or technical system is the one which performs according to a precise set of rules, and which will not deviate from these rules.[18] Artz and Gil (2007) characterise this interpretation as a 'hard security' approach which views trustworthiness as a status that should be established using traditional security techniques such as authentication, access control, encryption, etc. This view essentially equates trustworthiness with a threshold of predictability, classifying something as "trustworthy if its behaviour is predictable" (Proudler et al. 2014). In the context of purely technological artefacts, indeed there is little sense to speak of trustworthiness in the interpersonal sense. Still trustworthiness of a technological artefact is not necessarily is an absolute notion. Nickel et al. (2010) argue the concept of trustworthiness applied to technology can also be understood as a gradual notion in the sense of reliability. The more reliable artefact can be considered more trustworthy than an unreliable one.

Here it is also important to draw a distinction between trustworthiness in terms of data security and trustworthiness in terms of private data protection. It is helpful to keep in mind that in computer sciences, the problem of trust generally refers to the two main issues: securely exchanging data and securely identifying communication peers. Fundamentally, security requirements of confidentiality (preventing unauthorised reads), integrity (preventing unauthorised writes), and availability (ensuring access for authorised users), all rest on a distinction between authorised and unauthorised users (Stajano, 2003). Accordingly, satisfaction of trustworthiness requirements (usually shortened to 'trust requirements') is strictly related to identity management and access control issues. From the security perspective then, a trustworthy system is the one that reliably prevents unauthorised entities from accessing private data, satisfying the condition of confidentiality. On the other hand, a component or a

[18] Although 'Trustworthy' and 'trusted' can be used interchangeably, sometimes a distinction is drawn. In the information security a 'trusted' system or component is one whose failure can break the security policy, while a 'trustworthy' system or component is the one that will not fail (Anderson, 2004). A trusted entity here is taken in a narrow descriptive sense as being entrusted with information, without including reasons why the entity is entrusted with it. This chapter follows Anderson's distinction, treating 'trusted' as a descriptive term, and 'trustworthy' as a normative. To add to the confusion, the widely used term 'trusted computing' is more of a marketing term referring to a family of security solutions (Proudler et al. 2014).

system can be considered trustworthy in regard to privacy, if it reliably collects, stores and shares private data strictly in accordance with users' privacy preferences.[19]

As Fernandes et al. (2016) point out, most of the analysis of privacy issues in current consumer IoT such as 'smart home' appliances is centred around security of devices and protocols. Often, the issue of privacy in the context of IoT architectures is even conflated with the issue of data security (Ziegeldorf et al. 2014, De Fuentes et al. 2016, Malina et al 2016), and accordingly, the trust in data protection is sometimes considered as synonymous to the trust in the security of users' data (Sicari et al. 2014, Tragos et al 2016). There is little denying that the security of private data in consumer IoT systems is a cornerstone of data protection guarantees for users, especially considering how poorly designed some of such systems can be (Apthorpe et al. 2018). However, the confidence in the reliability of security protocols does not encompass the whole spectrum of trust in the protection of private data.

The distinction between trust in security of data and trust in data protection can be elaborated through the example borrowed from interpersonal trust. Baier (1986), arguing on the scope of trust, provides an illustration of a Greek mailman in a small village who is trusted to deliver the mail and not to tamper with it. However, in a certain scenario it may be appropriate for him to read the content of the mail in order to deliver it, e.g. when it has certain urgency and recipient's address has changed. The mailman is trusted to use his discretionary power competently, non-maliciously, and transparently, making intelligent decisions about the best interests of the mail owner. Analytically, trust in the safety of the mail, confidence that it will not be stolen from the mailman by a thief, does not encompass the full spectrum of the mailman's capacity to abuse trust. It does not matter if only authorised entity has access to private data, insofar as this entity has a capacity to undermine users' privacy. As Stajano (2003) points out it makes little sense to address questions of security and authorisation if we do not ask more fundamental questions: "authorised by whom?" and "for those benefits?"

[19] In fact, the security of a system can be completely divorced from the issue of users' privacy or even contradict it. For instance, if a trustworthy status for a user's endpoint is earned by revealing a certain number and type of credentials, and privacy of credential information is lost as the credentials are revealed, then there is a trade-off between privacy and earning of trust in the sense of security (Artz and Gill, 2007).

Achievement of trustworthiness even in the minimal sense of security of data is a non-trivial task in the context of IoT. Heterogeneity of components in any given IoT system means that achieving trustworthiness of a single component does not translate into trustworthiness of a system. Furthermore, as Yan et al. (2015) argue, even ensuring trustworthiness of the whole IoT layer does not imply that the justified trust in whole system can be achieved, and any satisfactory privacy-preserving solution should address private data flows through all layers of the IoT. Realisation of such a solution is a notoriously difficult task, even in the case of a system comprised only of technical artefacts. Achievement of trustworthiness in the sense of private data protection in a system which involves multiple human operators is a problem of a different scale. The more operators in such systems, the less coordinated their actions and considerations are in regards to users' interests (Nickel et al. 2010).

3.3.2. Data collectors and trustworthiness

Consumer IoT systems indeed fall into the category that Nickel et al. (2010) characterise as hybrid systems, partially technical and partially social. Data handling entities in IoT architectures include not only users of technology, device manufacturers, cloud service providers and platform providers, but also all entities that collect, store and process private data. Even in the case of single smart device data collection, processing and presentation can be performed by third parties which may lead to serious privacy issues, as in case of Samsung's 'Smart TV', which shared voice recordings of users with third parties (EPIC, 2015). These practices are partly explained by objective factors, since the development of data processing algorithms is a costly and time consuming task, and is hence often performed by specialised companies, separate from the hardware manufacturers (Andrejevic, 2014).

However very often, the presence of data collecting entities in the IoT architecture has nothing to do with the functionality of smart devices. Christl and Spiekerman (2016) reveal an intricate ecosystem of private data markets involving data brokers of different calibre ranging from Alphabet and Facebook to lesser known companies, actively engaging in the collection of user data from device manufacturers and suppliers of consumer IoT services. One such example is the sale of household interior map data to third parties by the manufacturer of the smart home-cleaning appliance 'Roomba' (Jones, 2017). Most recently, Samsung's 'smart TV' was again in the spot-

light when it was discovered that simply powering up the 'smart TV' initiates communication with Google Play, Double Click, Netflix, FandangoNOW, Spotify, CBS, MSNBC, NFL, Deezer, and Facebook, even if user does not have accounts with any of these parties (Apthorpe et al. 2018).

Thus, we must keep in mind that in the context of IoT architecture, these are not mere collections of interconnected technical artefacts. Rather, they should be seen as a complex and dynamic socio-technical system comprised of different entities, whose interests in regard to the collection of private data may be diametrically opposed to those of the technology consumers (Andrejevic 2014, Christl and Spiekerman 2016). Furthermore, the architectures of these systems can be highly dynamic, threatening reliability in terms of data protection.[20] Changes in the data flow architecture can happen almost instantly, as in the case of 'Amazon Echo' which was turned into a telephone-like device with a single software update from the manufacturer. 'Echo' users found that contact lists from connected smartphones were used to connect 'Echo' devices into a kind of social network, without regards to privacy preferences of the 'Echo' users (Hill, 2017). One more recent example of 'Echo' malfunctioning occurred when a conversation was recorded and shared with random person without the device owner's knowledge (Machkovech, 2018).

From the user's perspective, assessment of IoT device trustworthiness is a highly complicated task, inevitably requiring certain levels of technical knowledge, an issue that was already apparent some time ago (Stajano, 2003). There are even fewer reliable strategies that could help a user assess trustworthiness of an entire IoT system. It is essentially an issue of epistemic impairment for users, stemming from a very limited ability to acquire evidence about all aspects of the IoT system. As Pagallo et al. (2017) point out, identification of data-collecting entities is the first challenge for private data protection in the context of IoT architectures. To be trustworthy, an entity has to be known to the user, a requirement which is not easily satisfiable in the context of a complex IoT architecture.

To assess the reliability of a smart device in terms of private data sharing with other entities within current IoT systems, one would have to perform a network traffic

[20] A very basic notion of reliability in engineering implies performance of required functions in the given time interval.

analysis as in Arthorpe et al. (2018). However, such a tool is not necessarily available to an average consumer. Furthermore, this assessment may easily become obsolete in a short time as demonstrated by the example of the 'Echo'. It is sometimes suggested that from the user's perspective, trustworthiness of an IoT system can be guaranteed by the trustworthiness of a system manufacturer or service supplier (AIOTI, 2016). However, it is clear from the above-mentioned examples that this suggestion is not feasible with the current models. Even if we could conceive an IoT system where all data flows are fully controlled by one entity, such as the smart device manufacturer, rational trust in such an entity would be highly problematic for several reasons.

One reason is the issue of conflicting interests, which renders any trust relation inherently suspicious (Baier, 1978). Indeed, manufacturers of sensor-equipped smart devices very often have direct economic interests in private data collection. This is not a problem of isolated anecdotal examples like the 'Rumba', but already an industry-wide issue (Christl and Spiekerman, 2016). Contrary to the intuitive idea of consumer IoT in which end users are the paying customers generating revenue for the suppliers with payments for products and services, actual business models lean towards the information marketplaces (Nicolescu et al. 2018). In that respect, the Internet of Things is reproducing the successful business models of 'traditional' Internet, dominated by data brokers and revenues from private data monetisation.

Secondly, we see that the problem of skewed economic incentive is also closely intertwined with the implementation of proprietary software embedded in smart devices. Even when consumers purchase IoT hardware, they do not actually acquire property rights to the embedded proprietary software in any meaningful sense (Fairfiled, 2017). In fact, consumers merely rent such software, often without rights to alter it and without guarantees that it will retain same functionality. Not only does such approach make it difficult to scrutinise the actual private data collection protocols of sensory device, but it also provides much greater field of deliberation in regards to private data collection for the device manufacturers. The combination of skewed economic incentives and opaque embedded software creates situations when hardware products are shipped to the consumers with preinstalled malware, as in the infamous case of 'Lenovo' (Schneir, 2015). Furthermore, it becomes harder and harder to draw a line between privacy breaches happening because of poor imple-

mentation and malicious intent.[21] This reality, as Monti (2010) argues, creates a very distorted concept of trust in the hardware and service providers, where trust is degraded from ethical commitment to a marketing 'buzzword' used to obfuscate risks for the user.

Finally, even if we could consider a sensor hardware supplier as trustworthy, it does not provide much of an evidence about trustworthiness of third parties with whom data could be shared with. This issue becomes apparent from an observation that transitivity of trust is a highly demanding property dependent on the possibility of delegation – empowering someone to extend your trust indirectly (Hardin, 2002). Furthermore, if the scope of trust involves a trustee's capacity to harm a trustor's privacy, then distribution of justified trust is much more difficult to achieve (Monti, 2010). By definition, if Alice trusts Bob with private information, any of his attempts to share it with a third party undermines such trust. In order to justifiably trust the chain of entities to handle her message containing private information, Alice first has to identify all involved entities, and second to assess their trustworthiness independently from one another. This means assessing each entity's capacity to provide reliable information about its data handling practices and evidence that these practices will not be changed unilaterally.

The pessimistic conclusion here could be that from the moral perspective, IoT systems will never be trustworthy with regards to its users' private data protection. However, that would be a premature resolution. The main issue here is a need for the conceptual reconsideration of trust value. Understood as a deficit good that should be elicited from the users by all means, not only does 'trust' become a buzzword as Monti (2010) warns, but turns into a dangerous instrument of coercion. This overly exposes users to vulnerabilities which are exaggerated by the power imbalance between trustor and trustee in such relations. This does not suggest that we should abandon the benefits of IoT technology altogether. Rather, such concerns invite us to reconsider whether trust is the best instrument to reap these benefits.

[21] The recent finding that Android smartphones from well-known manufacturers were shipped to consumers with malware preinstalled at the firmware level, is both highly disturbing and unsurprising at the same time (Boocek and Crysaidos, 2018).

Luhmann (1978) somewhat paradoxically suggests that a system of a higher complexity requires more trust but at the same time also needs more distrust.[22] However, this is a valid point, once we consider that distrust can also be a rational strategy aimed at eliminating a range of possible scenarios. Furthermore, distrusting someone or something does not preclude development of trust in future, given new evidence (Govier, 1997). Counterintuitively then, acting on distrust to achieve justifiable trust can be a viable strategy, especially in the context of strong power imbalances or information asymmetry between trusting parties. Thus, distrust should also be considered with an end in mind, as a prima facie that can be discarded once a sufficient level of trustworthiness is demonstrably achieved. This is very much an approach in the spirit of Humean (1987) suggestion that with contriving institutional arrangements such as governments, we should start from the premise of distrust, an assumption that such institutions will be staffed by knaves.

3.4. Building on the distrust in the IoT

3.4.1. Minimising reliance on trust

Arguing from the Humean approach, Hardin (2002) points out that systems of checks and balances in the design of institutions in fact increase trustworthiness of the system as a whole. It is reasonable then to embrace this approach in the design of IoT applications as socio-technical systems, and try to derive some practical principles from it. One such principle is the minimisation of reliance on trust in the IoT systems. As Gambetta (2000) argues, trust is closely related to the agent's degree of freedom to disappoint a trustor's expectations. Thus, when the trustee's actions are heavily constrained, the role of trust in such a relation is proportionately smaller. The same can be said of the data collecting entities in IoT architecture. The lesser freedoms an entity has in regards to private data, the lesser amount of trust a user has to place in this entity.

Essentially every type of technological solution that can minimise users' reliance on trust in the system can be considered morally desirable. Edge computing as an approach might be one such solution, a technological design paradigm suggesting that as much data as possible should be aggregated and processed at the user's end (the

[22] Luhmannn, of course, refers to social systems, but this principle can be true in regards to social parts in socio-technical systems.

edge of a network). Another very promising solution to the protection of private data on the IoT systems might come with the development of blockchain technologies. The latter is of particular interest in the context of this paper since blockchain-based solutions are sometimes branded as 'trustless' (Christidis and Devetsikiotis, 2016) or even 'trust-free' (Beck et al. 2016).

To elaborate on this point, it might be helpful to consider very briefly some of the proposed blockchain-based IoT solutions. Considering that blockchain protocol is a general purpose technology, it has a wide transformative potential for many aspects of IoT which cannot be covered in a single study (Swan, 2015). Given this limitation, it makes sense to highlight some possibilities and potential limits of these technological solutions in the context of IoT consumer's trust, without going into details of particular projects. Blockchain in most general sense can be seen as a distributed transaction database, which solves the key problem for any distributed data base - that is, the issue of record synchronisation between the nodes of the network. A key novelty of blockchain comes from the fact that this problem is solved without the need for a centralised trusted authority.

Such transaction database or more specifically a distributed ledger, is implemented on the basis of cryptographic hashes which provides several interesting properties. Firstly, this is an append-only ledger which means that new records can only be added but not deleted (immutability). This also means that any new records must be generated in a specific 'block' format, containing the hash of the preceding one (resulting in a chain of blocks, and hence the name). The generation of such blocks is computationally demanding, and nodes taking part in it ('miners') are rewarded for successful generation of a valid block on a competitive basis.[23] Secondly, it is relatively easy to verify consistency of a new block with previous ones for any node holding a copy of the ledger (verifiability). This ingenious solution does solve the problem of trust in a very specific sense, guaranteeing that all nodes behave in a predictable way. It does not matter if a miner is trustworthy or not since malicious behaviour is costly in terms of time and computation, and easy to identify by the rest of the network.

[23] This approach is rather straightforward in cryptocurrencies, where nodes generating blocks get fees for the processing of transactions in the same currency.

This general scheme had found its first successful implementation in cryptocurrencies which use a relatively constrained set of rules in their protocols. Blockchain protocols, capable of encoding complex sets of rules, allow not only ledger keeping, but also distributed computation, prototypically implemented as 'Smart contracts' (Christidis and Devestikiodis, 2016). Smart contracts are general purpose, distributed applications that can be executed on the blockchain with code and state stored in the ledger. It is fair to say that most IoT related solutions using blockchain technology are built around smart contracts in one way or the other. Such proposed solutions can have numerous applications such as providing identity layers for network nodes, access control layers, providing secure track records of data flows, and many others (Dorri et al. 2016, Atzori 2016).[24] This is a radical departure from existing client-server models where all data streams from the consumer's end point are usually aggregated and stored in the cloud provided by the hardware manufacturer, or some other entity acting as a gatekeeper for private data.

Such solutions might not only increase transparency of data flows, but also provide users with better controls over their private data. For instance, providing management mechanisms for secure and transparent transfers of private data from consumer to services, such as health analytics, diagnostic services for personal car or any other remote applications, based on smart contracts. Christidis and Devetsikiotis (2016) characterise such layers as 'trustless environments', where entities on the network do not need to rely on trust in their interactions, since actions for entities are not only predictable but guaranteed by the network protocol. However, as Buterin (2015) points out, blockchain systems in themselves are not 'trustless', despite being sometimes labelled this way. First of all, only public (sometimes called 'permissionless') blockchains have the above-mentioned properties.[25] Second, trust solutions that work in the (relatively) narrow context of cryptocurrencies do not translate easily to other domains. Even the implementation of a single smart contract which can be considered 'trustless' in meaningful sense is contingent upon the set of a very specific conditions. Strictly speaking, a more appropriate term here is a 'trust-minim-

[24] It is necessary to point out that implementing blockchain solutions for the control-access layer is currently is the preferred solution for IoT applications since storage of private data on public blockchain itself is quite problematic from the privacy perspective.

[25] Decentralisation is arguably most interesting property of blockchain technology, which is absent in so called 'private' or 'permissioned ' blockchains, where instead one entity (company) decides who can become a node. This is not very different from a distributed database where trustworthiness of nodes is decided by centralised authority.

ised' system, since smart contracts can allow interaction between parties without reliance on trust only in a very specific context of a transaction enabled by it.

It would thus be very misleading to treat all blockchain-based solutions as 'trustless systems' and simply wrong to label them as 'trust free'. In this respect, it seems understanding of trust in blockchain implementation is not immune from Hardin's (2002) 'conceptual slip' as well.[26] Blockchain based solutions can minimise reliance on trust in private data protection for some components of IoT architecture, but not eliminate it completely. When systems involving human operators are made more reliable through automation, users' trust is not eliminated but rather shifted from operators to the designers of the system (Nickel et al. 2010). Consider an idealised example of a technological artefact with highly predictable functionality. Such a device, say a flash drive with built in hardware encryption, still relies on distributed trust. Apart from trusting the reliability of the artefact itself, at the very least a user has also to trust the manufacturer to properly implement the encryption, the authors of that encryption protocol, and the testers who did their best to find vulnerabilities in the protocol.

Even with the radical increase of predictability of IoT components, on the larger scale, information asymmetries persist, and we inevitably run into issues of trust in developers, trust in code reviewers/auditors and trust in institutional arrangements. These issues are partially mitigated in large cryptocurrency projects like Bitcoin, which greatly benefits from a transparent and decentralised developer community. This effect essentially amounts to the distribution of trust between independent entities. However, it is much less clear how the trust problem will be solved when IoT blockchain solutions are developed and offered by commercial companies. This is not necessarily an issue of trust in commercial entities but also a problem stemming from the variety of implementations allowed by blockchain technology and the different interpretations of transparency.[27] It would also be very disappointing and dis-

[26] Again, some of this confusion can be attributed to the overlap of concepts, since one can define a 'trustless' system in the same sense as the narrow interpretation of 'trustworthy', that is, the one that is fully predictable. Buterin (2015) even suggests that 'trustless' and 'trustful' systems refer essentially to the same resulting state of a predictable system, achieved through different means. Thus, the choice of the 'trustless' descriptor here highlights the point that predictability is achieved in the absence of trusted third parties.

[27] For instance IOTA, which brands its product as an alternative to IoT blockchain solutions, was found threatening researchers with legal action to prevent disclosure of vulnerabilities. See. http://blockchain.cs.ucl.ac.uk/2018/04/update-partnership-iota-foundation/

turbing to see the emergence of a new marketing buzzwords such as 'trust free', used to lure consumers into a false sense of security.

3.4.2. Mediating trust

Following our discussion, it can be argued that technological solutions aimed at the minimisation of trust in the IoT should be complemented with instruments that Hardin (2002) characterises as trust intermediaries. Existing solutions to the problem of impersonal trust extension via intermediaries are reputation systems (Taddeo). These essentially combine two functions of a trust intermediary: proof of identity for potential trustees and proof of goodwill and good sense in the form of reputational evidence. According to Simpson (2011), a reputation system is a truthful, comprehensive and accessible record about a person (or entity) that can be used to assess one's trustworthiness.

Such evidence should also be impossible or very difficult to fake and be subjectively available to trustor. A reputation system then may carry two functions of a trust intermediary – providing knowledge of data collecting entities and evidence of trustworthiness for identifiable entities. The question is whether such a system can provide sufficient incentives to data collectors not to default on trust obligations. I argue that a reputation system can act as this deterrent due to the peculiar nature of trust epistemology - that is a vulnerability of trust to a counter-evidence. While the evidence of past goodwill behaviour is crucial for the assessment of trustworthiness, it does not guarantee it, especially in the case of institutional trust.

As Gambetta (2002) notes, past evidence does not fully eliminate the risk of future deviance. In that respect, he argues trust predicates not only on the evidence of benevolent behaviour, but also on the absence of counter-evidence. This is a peculiar property of trust as an epistemic constraint: one cannot believe B to do P, if one possesses overwhelming evidence that B will not do P. The same kind of overwhelming counter-evidence can simplify an issue of an organisational reliability assessment, as highlighted by Hardin (2002). It is apparent that not any kind of counter-evidence is sufficient for such a role. As practice shows, data collecting companies often having an appalling record of privacy violations tainted by court decisions and public scandals, still stick to their malpractices (Christl and Spiekerman, 2016). This occurs

largely because media coverage is not a reputation system, but rather a playing field where PR efforts of companies can effectively mitigate reputational damage.

In Simpson's terms (2011), such information is neither comprehensive nor subjectively available to the trustor. Thus, an effective reputation system capable of fulfilling all three roles of trust intermediary must be a standardised system, providing necessary competence, quality reputational evidence and accessibility. Such systems can certainly be implemented using technological solutions, and blockchain technologies may present interesting opportunities in that respect (Powelse et al. 2017). Radical but intriguing solution could be an implementation of reputation scores for service providers processing private data, a reverse of consumer credit scores. It is however important to keep in mind that specific solutions are still far away from commercial implementation. Furthermore there is no guarantee that these solutions will disrupt current business models of private data monetisation in the consumer IoT sector, purely on the basis of free market mechanisms.

It is reasonable thus to consider possibilities of institutional arrangements, and avenues to remedy issues of trustworthiness for already existing consumer IoT products and services. Certain interest in that respect presents an idea of 'trust labels' or 'privacy seals' which has been suggested in different contexts as a tool to establish reputation of a service provider or a product (De Hert et al. 2014, Rodrigues et al. 2016). Some 'trust label' solutions applied specifically to the problem of privacy in the context of IoT can be found in the EU commission staff working document "Advancing the internet of things in Europe" (EC, 2016). One of the ideas proposed here is the 'Trusted IoT' label that would help consumers assess end products as being compliant with the aforementioned principles.

This suggestion is a part of the package together with the proposal on standardisation and liability clarifications which are considered crucial for future technological developments. Implementation of a 'Trusted IoT' label scheme is seen as a measure that would complement the upcoming GDPR regulation to help consumers with the problem of trust in the new technology. Existing proposals on a 'Trusted IoT' label largely focus on cybersecurity requirements, although promising applications of this scheme could also be extended to cover the wider issue of private data protection.

Granted, existing privacy seals developed as industry self-regulatory measures have been criticised before for the lack of standardisation and effective enforcement, and these are indeed valid concerns (Rodrigues et al. 2013). However, these concerns do not preclude development of institutional schemes that can offer a reputation system with truthful, comprehensive and accessible records about private data collectors (and processors) as suggested by Simpson (2011). In that respect, 'trust label' should be understood first and foremost not as a mere 'label' but as a certification scheme aimed at guaranteeing trustworthiness of a service or entity through the introduction of checks and balances (Hardin, 2002). To the large extent many failures of previous 'trust labels' stem from the fact that in the absence of underlying robust certification schemes, they are reduced to just another of marketing gimmick.[28] This again shifts the focus from the trustworthiness of services in terms of data protection, to consumers' attitudes of trust.

From that perspective any self-regulation certification are not going to deliver intended results. De Hert et al. (2014) suggest that credible certification can be achieved in the absence of conflicting interests between certifying bodies and service providers, arguing in favour of industry-independent expert bodies. Such institutional arrangements can effectively decrease power imbalances between consumers and providers of IoT services. Rodrigues et al. (2016) list a number of options for the implementation of data protection certification enabled by GDPR regime for certification and seals. The existence of independent certification bodies can provide consumers with the capacity to distribute trust among different institutional entities: experts, accreditation agencies and data protection authorities. Furthermore, an absence of such certification would indicate that neither the device nor the device provider could be considered trustworthy with regards to data protection standards, serving as counter-evidence to trust.

Another point of consideration here is an aspect of certification which should satisfy criteria of comprehensiveness (or sufficient scope). De Hert et al. (2014) provide several examples of certification schemes in different technological contexts, highlighting key points of consideration. They argue that in certain contexts (such as biometric systems), the main beneficiary of a certification scheme should be the par-

[28] It is quite telling that many 'privacy seals' emphasise marketing advantages granted by the certification (Rodrigues et al. 2013).

ty with the least effective power and influence over construction of the system. This principle is applicable in the context of consumer IoT as well. Of course, considering diversity of IoT products and services, as well as the dynamic nature of architectures, standardised certification is hardly feasible. Nonetheless it is reasonable to aim for a minimum standard of transparency for IoT services and processes, and not just hardware elements. It is also crucial that certification is performed on a dynamic basis, similar to vulnerability scans, rather than as a one time assessment.

At the very least, certified IoT solutions should by default conform to the principle of minimal data collection necessary for basic functionality, and strict opt-in for any extended data sharing. Granted, it may not always be trivial to define precisely basic functionality in many smart products and services. This problem however it not a technical issue, but the intentional design of products employing advertising revenue models. Key criteria here is that consumers should always have a choice between products and services which function with or without personal data monetisation. This brings about another requirement which is an availability of transparency tools in certified devices. This means that consumers should always be able to get truthful dynamic information about data which is collected in the process of service use, about all entities that have access to the data, and the tools that can be used to modify data flow in accordance with their preferences. These tools may either be integrated into a smart device itself or be available through the use of hub device (app on a smartphone).

Finally, such a certification scheme should satisfy criteria of accessibility to consumers, dealing specifically with the 'label' part itself. Given miniaturisation of sensor equipment and diversity of hardware formats, there is, once again, no 'silver bullet' solution in terms of label format. However given ever increasing connectivity of IoT components it is reasonable to assume that most flexibility can be achieved with the implementation of digital labels. Given that all smart devices by definition have extended connectivity it is reasonable to aim for the implementation of labels in digital format. Some interesting solutions which may serve as a basis for such labels can be found in the research on standards for digital identifiers.[29] Such identifier is essentially a cryptographically signed digital document, which allows for the reliable verification of its authenticity and contains references to additional information re-

[29] See. https://w3c-ccg.github.io/did-spec/

sources. Using standardised format it is possible to ensure that all necessary information (IoT certificate, links to certification body registry, links to transparency tools), even for most the most miniature device can be authenticated and accessed through a smartphone or any other smart device with connectivity module and graphic interface.

3.5. Conclusion

The complex nature of IoT architectures contributes significantly to privacy risks for users of such systems. In this context, the capacity of trust to reduce complexity, can indeed make the implementation of such systems more viable. However, it is crucial for policies and technological solutions to focus on the trustworthiness of systems and not just the psychological trust attitudes of users. If the latter becomes a goal framed in the model of 'trust deficit', instead of the promised benefits, consumer IoT systems can bring about the dystopian vision of a ubiquitous surveillance economy. Even in the absence of intentional nudging towards sharing of private data (malicious interface design) and psychological bias, the complexity of existing and future IoT systems simply does not provide technology consumers with much opportunity for balanced and rational decision making. The position of epistemic impairment significantly constrains the amount of available evidence to the users of technology which could be employed in order to justify trust in the system.

Another factor limiting such capacity is the non-transitive nature of trust in the protection of private data, which is particularly relevant in the context of structural data sharing. While it is possible to extend trust through the chains of data-collecting entities, in order to justify trustworthiness of the system as a whole, such extensions cannot be realistically achieved in the context of power imbalances. This means that justified trust in IoT systems and services can never be encompassed by trust in a single technological artefact or a single entity such as the provider of the system. To be trustworthy, the system as a whole should include both technical and institutional tools aimed at amending information asymmetries and power imbalances. Thus, based on a Humean vision of institutional design, the moral value of distrust could be used as a premise defining design requirement in IoT implementations, comprised of technical and social elements. Rephrasing Hume (1986 E.VI) - without this, we shall find, in the end, that we have no security for our liberties or data, ex-

cept the good-will of data collectors; that is, we shall have no security and privacy at all.

This approach gives rise to a key guiding principle of minimisation of trust with all means available. Too much reliance on trust can be a burden and a serious failure of the system design, especially when the burden of establishing evidence to justify trust is placed on the trustor – the user of technology. Even in the absence of other complications, it is difficult to provide moral justification for trust relations in the context of significant information asymmetry. Consumer IoT systems can make this task next to impossible, taking into consideration economic and power imbalances between consumers and providers of technology, where interests of the latter often align with interests of data collectors. Thus, minimisation of trust here should be considered a moral imperative, a means to reduce dependence of users on the benevolence of multiple data collecting entities.

This is followed by another guiding principle which suggests a necessity to distribute trust wherever it is impossible to avoid it completely. In the context of IoT architectures, this means that users should not be left to their own devices in the process of making privacy relevant decisions, dealing with a single entity such as hardware manufacturer or service provider. This can be achieved with the introduction of trust intermediaries, providing functions of expertise, tracking of data collecting entities and some means of redress in the cases of trust abuse. Such arrangements can take forms of independent certification bodies combined with technological solutions that can increase transparency of data-collecting practices. While these requirements are sometimes presented as excessively demanding, they are in fact necessary minimal measures that should be implemented to avoid paying the price of eroded privacy in exchange for the benefits of IoT.

4.The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data

4.1. Introduction

Centralized data collecting entities placed as intermediaries are often singled out as the main culprits responsible for the dissolution of online privacy: telecom providers, search engines, social networks, market platforms, and financial services are – due to market share or network lock-in – entities that are uniquely placed to claim their customers' private data (Christl & Spiekermann, 2016). The same apprehension applies to many current consumer IoT products that combine client-server models and the use of embedded proprietary software, enabling the opaque collection and aggregation of users' private data by hardware providers (Gasser et al., 2016). Furthermore, these solutions also enable the vertical integration of IoT services where hardware manufacturers provide cloud data storage, data processing and data-based services, retaining control and de-facto ownership through the data lifecycle. It is quite a disturbing trend, which threatens to expand morally problematic practices of commercial surveillance from social networks and search engines into physical spaces filled with connected sensor devices.

Proposed blockchain solutions for consumer IoT are particularly interesting in this context. Not only do they promise technological tools for enhanced private data controls, but also the reconfiguration of IoT architectures and even the radical disruption of existing business models based on private data monetization (Dorri et al., 2016; Novo 2018; Shafagh et al., 2017; Zyskind et al., 2015a; Zyskind et al., 2015b). It is argued that these solutions will eliminate privacy risks associated with the lack of users' control over their private data, and will rewrite the norms of data ownership. Instead of trusting a centrally controlled cloud service or sensor manufacturer with their private data, IoT users will rely on the predictable performance of decentralized blockchain-enabled networks. Leveraging 'smart contracts' functionality, these networks will serve as a layer for interactions between hardware, data collectors, and data processors that will be performed in accordance with users' preferences.

It should be noted that many of these proposals in some fashion reflect the ethos of the original blockchain implementation – Bitcoin – which was first proposed in a white paper by its anonymous creator Satoshi Nakamoto (2008). Emerging as a logical continuation of 'cypherpunk' ideas on digital currencies, Bitcoin was conceived as a tool that could provide individuals with anonymity and freedom of market interactions; unimpeded by any centralized intermediary or authority. (Karlstrom, 2014; Dierksmeier, 2018). However, the moral merits of 'cypherpunk' ideas are a topic worthy of a standalone investigation, and can be omitted here for several reasons.

For one, even in the (relatively) narrow space of 'cryptocurrencies' it is non-trivial to objectively characterize any given blockchain project as purely 'cypherpunk'. And this connection becomes even more remote once we move into the space of projects implementing solutions on the basis of blockchain technology other than digital currencies.[30] Furthermore, as Reijers and Coeckelbergh (2018) argue, the morally desirable properties of blockchain-enabled cryptocurrencies do not necessarily translate directly into other contexts of application. Rigidity of social interactions, mediated by the blockchain technology while desirable in the context of financial transactions, may become harmful in other contexts. Thus, it would be misleading to argue that the moral desirability of IoT blockchain solutions could be defined within the framework of 'cypherpunk' ethics.

Secondly, as this chapter aims to demonstrate, normative ideas underlying the aforementioned blockchain IoT applications are more strongly influenced by the liberal tradition of legal thinking on communication technologies famously represented by Lawrence Lessig (2006), rather than by the radical libertarian tradition of 'cypherpunk' and Satoshi Nakamoto. De Filippi and Hassan (2018), providing an evaluation on the possible adoption of the wider range of blockchain applications (such as 'smart contracts'), highlight the continuity of these applications with the ethos of Lessig's maxim – 'code is law'. These applications maintain key aspects of regulations by code where desirable or undesirable behavior is not regulated *ex-post* by third parties as in legal regulations, but rather are enforced with the help of technological tools *ex-ante*, eliminating the need for judicial arbitration and leaving no

[30] It is illustrative that the phrase 'Satoshi's vision', originally used to signify continuity with the 'cypherpunk' values of early Bitcoin implementations, became so overused by the promoters of Initial Coin Offerings (ICOs) and dubious Bitcoin clones ('hard forks') that now it is hardly ever used in any sense but ironic.

room for ambiguity. De Filippi and Hassan also highlight another important normative aspect of such applications, and associated moral apprehensions. Given low barriers for entry and the malleability of code, these new regimes of regulations in the digital environment open up doors to regulation by private actors who might try to impose their values on others by embedding them into a technological artefact.[31]

This latter point is of particular interest in the context of this chapter given that many of the proposed IoT blockchain solutions not only aim to reconfigure IoT architectures but also seek to implement rather particular assumptions on the value of privacy. In these proposals, the right to privacy is interpreted as a right to property in private data, and monetary compensations are suggested as a remedy for the loss of privacy (Zyskind et al., 2015a; Zyskind et al., 2015b; Streamr, 2017; Van Niekerk & van der Veer, 2017; Levine, 2018). On the basis of these normative assumptions, it is argued that blockchain-enabled tools for the control of private data will enable new data markets, where IoT users will be able to monetize the sensing capacity of their hardware and even sell private data directly if they choose to.

The rationale behind these components is a broadly utilitarian justification for the properatization of private data. A belief that new mechanisms of data monetization can bring a fairer and more diversified market for data-based services, resulting in transparent data collection and processing practices on the wider scale of the consumer IoT ecosystem (Pentland, 2009; Koutroumpis et al., 2017). Unlike technological components of blockchain solutions, these proposals are less novel and can be traced back to the debates on the merits of private data propertization, which took place as far back as early 1990s. Understood as a legally recognized ownership of private data, propertization was suggested as a market-centric solution to the problems of privacy brought by the new communication technologies (Laudon, 1993). The question of private data propertization – seen as a legal recognition of property rights – has been contested from the very coining of the term itself.

Opponents of propertization point out the key moral question of whether personal information should be commodified at all (Litman, 2000; Rossler, 2015; Samuelson, 2000). Samuelson (2000) aptly condensed this criticism in the maxim that proper-

[31] The barrier for entry for software builders is arguably lower if compared with the participation in the traditional lobbying mechanisms in legislation. Besides, code is inherently adaptable, which means it can be relatively easy repurposed and carries virtual zero costs for reproduction.

tization as the solution to privacy is highly misleading since personal data markets are 'the problem'.[32]

There are indeed valid moral reasons, as suggested by Sandel (2013), to take a critical stance on the diffusion of market relations into all spheres of human life. First, market modes of valuation do not always guarantee a fair distribution of market goods to those who value them the most. Secondly, there is a risk that good, activity, or social practice can be corrupted by commodification being reduced to a single mode of valuation. Thus, it can be argued that even within the constrains of utilitarian justification suggested by the proponents of propertization, their arguments are far from compelling. This criticism of propertization, however, is primarily expressed in the context of legal frameworks. Hence, given that blockchain-enabled application has already introduced qualitatively new types of property, and new types of regulation, reconsideration of these arguments may be warranted in a new technological context (Reijers & Coeckelbergh, 2018; De Filippi & Hassan, 2018).

And indeed, it has been argued that blockchain technology can reshape data markets in a truly radical fashion, warranting a reconsideration of criticisms (Koutroumpis et al., 2017). Such new multilateral markets, as argued, can provide transparent chains of provenance and enforceable usage restrictions, alleviating the majority of concerns associated with private data trading. Another argument presented by the proponents of propertization is the observation that whether we consider commodification of private data desirable or not, de facto such markets already exist, and they cannot be undone. Thus, as argues Pentland (2009), the pragmatic approach is to try and make these markets fairer with the help of tools that enhance individual data ownership.

From the perspective of moral philosophy, this later argument does not hold any ground on its own. The fact that some practice is ubiquitous in society does not make it necessarily acceptable or desirable. However, one can inquire if this practice can be altered in such a way that makes it acceptable or even desirable. Rossler

[32] Here it is helpful to make a distinction between 'commodification' and 'propertization' of private data. In the legal literature, the latter term can be understood as referring to the legitimized commodification. In the context of a moral-philosophical analysis, argues Rossler (2015), 'commodification' is preferable as a less loaded concept, which does not overlap with the more general questions on the moral justification of property. However, considering the argument that certain implementations of blockchain technology can be seen as alternative mechanisms to the traditional legal frameworks (De Filippi and Hassan 2018), the term 'propertization' seems more appropriate in the given context.

(2015) makes a case for the moral acceptability of 'incomplete commodification' of private data, arguing that private data can be treated as a market commodity within certain limits. The task for ethics, argues Rossler, is to criticize tradability if it becomes harmful or injurious in order to guide limitations of the market in personal data.[33] So the main question here is whether these new technologically enabled regimes of property in data could address the ethical issues of privacy for IoT users, and tackle negative aspects of data propertization.

While no wide scale blockchain IoT applications comparable to Bitcoin exist at the moment, different implementations ranging from proof-of-concept to small scale projects provide an opportunity to analyze the limits of this technology and some key normative assumptions that drive developments in this area (Dorri et al., 2016; Novo, 2018; Shafagh et al., 2017; Zyskind et al., 2015a; Zyskind et al., 2015b). Of particular interest in that respect is project 'Enigma', where novel technological solutions and the explicit ethical positioning of its developers make it particularly illustrative case (Zyskind et al., 2015a; Zyskind et al., 2015b).

Based on the analysis of the proposed solutions, the chapter argues that blockchain-enabled regimes of property in private data do not in fact solve the ethical issues associated with the legal propertization of private data. Furthermore, it is argued that the unique nature of blockchain applications introduces new ethical concerns regarding the privacy of IoT users. Unlike legal regimes of property, blockchain-based solutions are by their very design resilient to any attempts to undo them. Thus, morally undesirable aspects of private data propertization can be amplified by the irreversibility of these developments.

The chapter is structured as following: section 2 looks into ethical concerns associated with the privacy of IoT users, and highlights how technological developments force us to reconsider our understanding of informational privacy. Section 3 provides brief technical descriptions of the blockchain-based solutions and highlights its key components including decentralized access-control systems and data markets. Sec-

[33] We also should not underestimate the possibility that such data markets could have unexpected effects either supporting or effectively undermining existing legal measures aimed at guaranteeing privacy and private data protection of IoT users. This apprehension already stands sharp in the context of the General Data Protection Regulation (GDPR), as noted by Finck (2017). Furthermore, it has even been argued that blockchain technology can potentially provide superior mechanisms of private data protection and thus should be exempt from the GDPR, which will only hamper development of these tools (Brito, 2018).

tion 4 considers the technical limitations of the proposed solutions and limits of effective control over privacy for technology users within the framework of private data property. Section 5 concludes with an outline of the ethical limits for the proposed private data markets and argues that disregard for these limits can bring effects opposite to the intended ones by the developers of blockchain IoT solutions.

4.2. Privacy ethics in the context of IoT

IoT itself is not a specific technology but rather a unifying design paradigm describing a wide range of applications utilizing the growing accessibility of miniature sensors and connectivity solutions.[34] Indeed, first and foremost, all current IoT developments ranging from industrial applications to consumer electronics would probably be better characterized as an 'internet of sensors', providing an ever-increasing number of channels for the collection of data. It is easy to see that such IoT systems carry inherent privacy risks, especially in the context of consumer applications and services. Economic incentives for data collectors, combined with insufficient data security measures and a lack of regulatory oversight, has led to the point where consumer IoTs are seen as a vast 'attack surface' and a serious threat to the privacy of individuals (Apthorpe et al., 2017; Christin, 2016; Christl & Spiekermann, 2016; Gasser et al., 2016).

The IoT is also often characterized as a technology capable of blurring the threshold between the online and offline worlds (Gasser et al., 2016). One consequence of this is that the distinction between physical privacy as a right to be left alone in one's physical space and informational privacy is hard to distinguish meaningfully in the context of the IoT (Floridi, 2006). Ubiquitous connected sensors, present in home appliances, wearables, cars, and smartphones can create an eerily accurate representation of a physical persona in a digital format that is easily shareable with the whole world, phenomenon sometimes referred to as a '*datafication*'. This, however, is not the only threshold that can be blurred by the IoT. In fact, the very distinction be-

[34] Neither, strictly speaking, is there a single standard definition of a 'smart' technology. This chapter treats it as a label for any IoT device or environment with embedded sensors, actuators and connectivity modules designed to provide interactive services to the user.

tween private data and non-private data is rather difficult to address in the context of physical spaces inhabited by humans.[35]

Unsurprisingly then, the very definition of privacy and our understanding of its value is being constantly challenged and reshaped by the development of IoT technologies. With the propagation of ubiquitous computing, which can be considered an antecedent of IoT, the focus of privacy concerns extended from personal information itself to the technologies facilitating the generation and sharing of information. Van den Hoven and Vermaas (2007) provide a two-partite definition of informational privacy in the normative sense – a non absolute moral right of a person to have control over access to: 1) information about oneself; and 2) situations in which others could acquire information about oneself. However, as they argue, this definition is insufficient to include our moral concerns about the propagation of ubiquitous Internet connected devices without 3) a moral right of a person to have control over access to technology that can be used to generate, process or disseminate information about oneself.

And, unfortunately, it would be wrong to say that more than ten years of developments in the area of IoT has managed to address this point. Quite the opposite, centralized architectures of many IoT solutions, combined with opaque proprietary software, has led to the point where 'smart' things are effectively controlled by the manufacturers and providers rather than the users.[36] Amplified by the information asymmetries between users and providers, stemming from the ever-increasing technical complexity of IoT solutions, this situation effectively forces IoT users to trade their privacy in exchange for the benefits of IoT products and services (Christl & Spiekermann, 2016). These trade-offs become especially problematic when we consider the diffusion of IoT appliances in all spheres of everyday life, providing capacity to collect highly sensitive health data, or even data from children (Bruynseels & van den Hoven, 2015; Haynes et al., 2017).

---

[35] There is also a standalone issue of the distinction between 'private data' and 'personal information', which are, strictly speaking, different concepts. Purely philosophical conceptualization suggests that data generated by the person is still impersonal if it lacks contextual meaning, while information about a person is always meaningful and thus is always personal. On the other hand, legal approaches, including the GDPR framework, largely conflate these terms. Debate on the merits of this distinction in law is beyond the scope of this chapter, thus 'private data' is used here in the sense of meaningful data.

[36] The term centralized architecture is used here in the broad sense to include server-client IoT solutions where end-point devices provide 'smart' functionality using the connection to the remote centrally controlled server that collects and process data.

It can be argued though, that developments in data processing technologies can make even this extended definition incomplete. A patent from Google aptly illustrates this point. Unironically called 'Privacy-aware personalized content for the smart home', it suggests that the value of data collected from 'smart' households can be utilized by a remote data processing engine through the aggregation of statistics, use patterns, and inferential abstractions. These inferences from home data may provide information on: "when occupants are home, when are they sleeping, when are they cooking, when are they in the den watching television, and when do they shower" (US Patent, US 20160260135A1, 2016, p. 12). But probably the most striking illustration of processing capacity here is a suggestion that data can always be repurposed, in a way which is not immediately obvious: for instance, to infer "the sleep patterns of schoolchildren in a particular ZIP code" from house occupancy data collected for the purpose of fire safety (p. 13).

Given the progress in big data analytics, it is easy to see that this is not an isolated example but rather a reality of private data collection in consumer IoTs (Greveler et al., 2012; Apthorpe et al., 2017; Acar et al., 2018). Thus speaking of the informational privacy of IoT users, it is crucial to consider not only control over access to the private data and technological artefacts, but also privacy invasions based on the inferred information.[37] As Durante (2017) argues, this requires us to move beyond *reactive* conceptualziations of privacy, which are concerned with the status quo of a person and historical private data. He proposes the following extended definition of informational privacy: a) the protection of personal data; and b) the protection of our ability to turn data into information relevant to us.

Indeed, the moral right to protect the uses of data collected from individuals is rooted in the very same concerns that justify the right to have a say in the collection or dissemination of private data. On one hand, in the instrumentalist vein of privacy justification, it can be argued that as long as inferred data allows for same harms as directly collected private data, there is no difference between these data from the moral standpoint. On the other hand, it is argued that this right is grounded in even deeper moral and philosophical concerns, and inferred data warrants protection on

[37] It would of course be wrong to say that IoT sensor data are unique in that respect, since these inferences can be derived from communication metadata, social networks data, etc. The issue rather is that these technologies dramatically increase the volume of available data, thus increasing the efficiency of data processing techniques based on large data sets.

the basis of a special significance to the identity of an individual (or a group) as data constitutive of the identity in ontological sense (Floridi, 2006; Durante 2017), or data relevant to the construction of moral identity (Manders-Huits & van den Hoven; 2008).

From this perspective, the proponents of the merits of private data propertization seemingly aim to address the need to re-conceptualize the right to privacy in new terms allowing to grasp wider range of privacy scenarios (Pentland, 2009). This approach, however, does not align well with the proactive understanding of the moral right to privacy (b), given that there is no easy way to establish property rights when inferences are performed by third parties. Furthermore, ascribing to ownership based conceptualisations runs the risk of interpreting the value of privacy in a reductionist fashion in terms of market evaluation. Sandel (2013) illustrates this problem by discussing the difference between fines and fees that can be identical in their monetary representation. Unlike fines, which essentially register moral disapproval, fees are mostly devoid of moral judgment. This is not to say that replacing one with another is always wrong, but rather, that when doing so, we need to ask: what is the purpose of the social practice in question? And what norms should govern it? The problematic nature of such reductionism becomes particularly apparent in the context of sensitive data collection, such as health data or minors' private data (Bruynseels & van den Hoven, 2015; Haynes et al., 2017).

It seems, then, that this contradiction between privacy cast as a moral right versus privacy as data ownership in the sense of property, mirrors the central point of the criticisms about legal private data propertization (Litman, 2000; Samuelson, 2000; Rossler, 2015). Furthermore, in the context of IoT, this contradiction adds to the previous arguments against data propertization. New technological developments raise moral concerns regarding the question of how property regimes in data can address the problem of inferences detrimental to informational privacy. Thus, to claim successfully that the blockchain-enabled propertization of private data can solve the issues of privacy for the IoT users, one would have to demonstrate how this approach could address the aforementioned ethical concerns. To investigate these claims, the following section, examines key elements of the proposed blockchain based solutions enabling technological propertization.

4.3. Blockchain based IoT solutions

4.3.1. Key technical components

To understand how future IoT architectures and even ecosystems could benefit from the implementations of blockchain technologies, it might be helpful to take a brief look at the key technological elements of the proposed solutions. The starting key concept, crucial here, is the idea of the distributed ledger, and often implementations in this family of technologies are also labeled as a distributed ledger technology. Sometimes these two labels are used to differentiate alternative implementations, but strictly speaking the use of terminology often reflects marketing efforts of developers, rather than meaningful technological differences.[38] Thus, this chapter treats blockchain and distributed ledger terms more or less synonymously.

Blockchain, understood as an implementation of an append-only distributed database, solves a key problem for such databases: synchronization of records between the nodes of the network. Furthermore, it solves this issue without the need for a single verifying (trusted) authority, treating all nodes as untrusted. This is achieved with the combination of underlying cryptography and economic incentives for individual nodes to act non-maliciously, resulting in a tamper-proof (sometimes also labeled as immutable) distributed database – a distributed ledger. It needs to be noted that the original family of protocols (such as Bitcoin or Ethereum) are sometimes labeled as public or 'permissionless' blockchains, and distinguished from alternative, so-called private or 'permissioned' blockchains, where nodes are identified and authorized by the third party authority to read or write to the ledger.

Granted, specific implementations of such protocols can provide interesting distributed systems solutions for the enterprises. However, from an individual IoT user's perspective, these solutions do not necessarily present a radical departure from the existing corporate databases and associated issues, and thus are not considered here. Furthermore, it can be argued that since the unique characterizing

[38] Some notable exception in the field of IoT-related solutions is the IOTA project, which in theory employ network protocol 'Tangle' sufficiently differently from the blockchain. However, practical applicability of this approach is very questionable considering that the IOTA protocol might be flawed at the level of cryptographic primitives, specifically in the implementation of a nonstandard hash-function. See Colavita and Tanzer (2018) for details.

aspect of blockchain is an absence of trusted third parties, it is an open question whether permissioned distributed ledgers should be named as such.

The resulting data structure implemented on the basis of blockchain protocol can contain any type of data including scripts, thus providing a capacity for distributed computation applications called 'smart contracts'. These applications are executed on the virtual machine running on the blockchain – again without the need for a single authority to verify implementation of such a contract (Buterin, 2014). Using scripting language with sufficient expressive power, it is possible to encode arbitrarily complex logic in smart contracts, amounting to distributed applications. Key properties of such blockchains – public accessibility, immutability, and censorship resistance through redundancy (each node may have a full copy of a ledger, and a single copy is enough to reconstruct the blockchain) – make it quite obvious that no plaintext private data should ever be put on the blockchain itself.

Similarly, it is unacceptable to store simple hashes of private data – like emails – that can be easily reversed (Acar et al., 2018).[39] Even encrypted private data stored on a blockchain presents serious privacy issues, considering that with the key leakage privacy loss is irreversible since data cannot be modified or erased. For these use cases, blockchain, in fact, is a worse solution than any centrally controlled private data storage. The latter, at least hypothetically, can be subject to legal action, while any sufficiently decentralized blockchain is resilient to it.

Still, it is possible to leverage these peculiar properties of blockchain, using it as a component of private data management systems. Zyskind et al. (2015a) propose such a solution – 'Enigma' – where blockchain is implemented to provide access-control layer, together with off-chain (external to the ledger) storage for the private data. This approach can also be implemented in a consumer IoT architecture where a sensor device owner has an ability to grant and revoke access to sensor data for different services without reliance on a trusted third party. A similar approach proposed by Shafagh et al. (2017), which they describe as "agnostic of the storage layer", also implements access-control layer in the IoT architecture on the basis of a public

[39] These apprehensions unfortunately are not merely hypothetical. A rather disturbing example of how blockchain should never be used is provided by a patent on medical records system filed by Wal-mart. This implementation not only suggests storing private health data on-chain, but also introduces the capability of access to private data without the data subject's knowledge or consent through biometric identification including thumbprints and facial features (US patent No. 20180167200, 2018).

blockchain.[40] It is important to point out that in most of the solutions for the decentralized access-control management, blockchain ledger still stores some metadata such as hashes of encrypted private data used for referencing. This means there are still some privacy risks, as will be shown later.

This approach to the access control management in IoT networks is certainly a step forward from existing IoT architectures, where devices are identified, authenticated and connected through centralized servers. Another option, of course, is an implementation of a local access-control server physically controlled and managed by the user as suggested in Perera et al. (2017). Such localized solutions, however, cannot compete with a cloud-based access-control management which has significant advantages from an end user's perspective: usability, affordability, interoperability, and scalability.

Blockchain-based implementations can potentially deliver all these advantages without the privacy costs of a commercial cloud service. And compared to personal server implementation, hardware requirements for the dedicated device serving as a full or lightweight blockchain node are much lower (currently it does not seem viable to implement full node functionality in all IoT devices).[41] From a technical perspective, the only problem is an issue of scalability, since current smart contract implementations are severely limited by the transaction processing capacity of the networks. There are however, some promising developments in this area that warrant cautious optimism in relation to the resolution of scalability issues (Poon & Buterin, 2017).

---

[40] Zyskind et al. (2015a) and Shafagh et al. (2017), point out several options for off-chain private data storage, including local (user's edge), cloud, and decentralized storage based on Distributed Hash Tables (DHS). The latter's option is particularly interesting, since it combines high levels of data integrity and availability inherent to decentralized networks with privacy guarantees of the local storage. Some proposed DHS implementations leverage Interplanetary Files System protocol (IPFS) and blockchain technology in order to build a decentralized system for the shared storage resources (Benet, 2014). In these implementations, data storage layer is separate from the ledger, which is used to manage resource allocation. Furthermore, it should be possible to encrypt and fragment data in such a way that no single node has access to the content of stored data, and only the original uploader can read or modify data. These implementations in theory could provide significant privacy benefits in comparison to the existing centralized cloud storage solutions. See, for instance, projects such as 'Stroj' https://storj.io/, and 'Filecoin' https://filecoin.io/. These projects, however, are in the early stages of development and practical viability of these implementations in IoT architectures is a standalone research question outside the scope of this chapter.

[41] For the discussion on the implementation of dedicated blockchain nodes in IoT architectures, see Novo (2018).

What is even more interesting is that blockchain-based solutions are quickly evolving from proof-of-concept implementations to market-ready systems offered by existing IoT providers and a growing number of start-ups. Some of the biggest projects in this area include solutions from existing IoT suppliers such as IBM, one of the earlier entrants (Brody & Pureswaran, 2014). A number of other big companies active in the IoT market, such as Cisco, Bosch and Foxconn, are also participating in the development of blockchain-based solutions.[42]

However, as mentioned, these solutions – based on private DLs – do not necessarily present a radical departure from the existing database solutions built around trusted third parties. Furthermore, these corporate projects largely focus on the business-to-business (B2B) sector demands, providing products for supply chains, industrial IoT and infrastructural solutions. Thus, in the context of this chapter, probably the most interesting visions of blockchain applications aimed at tackling consumer IoT privacy issues are offered by start-ups. These visions include not only access-control solutions, but also (and a key point of interest for this chapter) the idea of a distributed marketplace for IoT-sourced sensor data.

4.3.2. Data marketplaces

The idea behind the creation of the ecosystem for IoT-sourced data markets is not new or exclusive to blockchain projects, of course, since the whole industrial IoT sector has been moving in this direction for a long time (Buyya et al., 2008). What makes these new projects particularly novel, however, is the promise to extend this vision to consumer IoT applications, enabling every individual user to sell his or her personal data or share access to IoT devices for revenue in a transparent and fair (from the market perspective) way. Projects working in this direction include not only 'Enigma', but also 'Databroker DAO', 'Streamr', 'Datum', 'Ocean Protocol', and others. These projects combine promises to bring privacy and control over private data through the implementation of blockchain-based decentralized IoT architectures and data marketplaces powered by cryptocurrency payments.

---

[42] See 'Trusted IoT Alliance'. Available at: https://www.prnewswire.com/news-releases/newly-launched-trusted-iot-alliance-unites-the-industry-to-further-a-blockchain-based-internet-of-things-300521935.html?tc=eml-cleartime

The 'Streamr' project whitepaper suggests that with the help of a secure blockchain-based platform, individuals could sell the heart rate data from their smartwatch on the data marketplace (Streamr, 2017). A whitepaper published by 'Databroker DAO' also suggests that while industry sector sensor owners will constitute the majority of data producers, consumers of IoT products – such as health and fitness or smart home applications – could also contribute to the data market (Van Niekerk & van der Veer, 2017). In fact, it is fair to say that most projects working in this direction include the development of decentralized data marketplaces, which may not necessarily target the consumer IoT sector, but nethertheless aim to disrupt existing ecosystems of data flows and data silos, currently dominated by the centralized data collectors and aggregators. Some even more radical suggestions include proposals on blockchain enabled marketplaces for health and genetic data (Levine, 2018)

'Enigma' project, which emerged from academic research, is particularly interesting in the context of this section. Not only it represents a number of working proof-of-concept solutions, but given its academic origins, it is possible to track some of the ideas central to its foundation (Zyskind et al., 2015b).[43] The idea behind the decentralized data marketplace offered by the Enigma project suggests that with the help of the blockchain layer, all sensor owners would be able not to only create listings for data products, but also to sell or share their data with the help of smart contracts. The project description suggests that the creation of such a marketplace would provide more data for research, make the value of data explicit, and enable more people to have the benefits that come with controlling their data and privacy (Enigma, 2017). The latter argument is of particular interest here as it illustrates the underlying normative assumptions on the nature of privacy and private data controls, serving to provide a broadly utilitarian justification for the propertization of private data as a privacy enhancing tool.

One of the 'Enigma' whitepaper co-authors, Alex Pentland, clearly formulates this idea as a privacy achievable through the ownership of private data. Pentland (2009) argues that our notions of privacy and data ownership need to evolve in order to adapt to the value of big data and suggests that market incentive mechanisms provided by the recognized ownership of private data can be sufficient to achieve such a

[43] Currently implemented as a Testnet (testing network). See: https://enigma.co/protocol/AboutThisRelease.html

balance. The idea itself, that the market-based ownership of private data presents a sufficient mechanism to guarantee privacy rights for individuals, in fact can be traced back to the work of Laudon (1996) who largely laid the foundations for these proposals. In the presence of a functioning data market where private data ownership is recognized and enforced, Laudon argues, data collectors will be forced by market incentives to respect the privacy of individuals, providing an effect that cannot be achieved with legal protection alone. These ideas were later developed by Lessig (2002; 2006), building on a key argument that legal measures – inevitably lagging behind ICT developments – are insufficient to guarantee privacy for individuals, and that adoption for privacy preserving technologies cannot be bootstrapped without market incentives.

Granted, at this moment it is rather hard to predict whether any of these projects will be able to garner significant market share, let alone disrupt the whole ecosystem of consumer IoT.[44] Still, there are good reasons to believe that if any of the blockchain-based IoT architectures get mainstream adoption, they will carry implementations for data marketplaces in one form or another. This becomes apparent from the observation that the idea of data marketplaces is closely intertwined with two key trends driving current development of IoT technologies: machine- to-machine (M2M) economy and Sensing as a Service (SenaaS).The M2M economy is a rather broad label, which encompasses a range of communication technologies underlying IoT solutions aimed at creating future economic models.

In these models, smart devices with autonomous or semi-autonomous capacity would be able to make their own decisions, participate in markets, buy and sell services, creating new class of market actors (Holler, 2014). SenaaS is another closely related vision of a business model where IoT services and products are offered on-demand, mostly focusing on sensing data in smart cities (Perera et al., 2014; Perera et al., 2017). It is also possible to say that the idea of technologically enabled ownership in IoT data, found in blockchain solutions, is conceptually (if not technologically) similar to those presented in SenaaS.

---

[44] The number of emerging startups and projects has been dramatically boosted by the availability of Initial Coin Offering (ICO) crowdfunding mechanisms. However, specific market characteristics of these mechanisms, which incentivize overinflated promises from the project founders, make proper assessment of projects somewhat problematic (Sehra et al. 2017).

Furthermore, these visions seem to align well with the cryptocurrency developments in blockchain technologies that enable financial micro transactions. Many cryptocurrency projects are moving towards providing cheap and almost instantaneous payments, serving as an enabling factor for both M2M and SenaaS models. In fact, it can be said that micro transactions were the driving force behind some of the earlier ideas for IoT-related blockchain applications (Worner & von Bomhard, 2014). Blockchain solutions providing an interaction layer – not just for various devices, but additionally for data providers, consumers and services – also address issues of interoperability and transparency highlighted in parallel proposals on the IoT data markets (Koutroumpis et al., 2017; Perrera et al., 2017; Spiekeramann & Novotny, 2015).

Thus, unsurprisingly, many current blockchain IoT solutions emphasize promises to realize these business models, effectively enabling some aspects of property in private data, for example, limited access (excludability), and alienability (tradability). At the same time, it is much less clear whether the arguments to re-conceptualize privacy as a property in data with the help of blockchain applications are rooted in valid moral considerations or rather merely serve to justify aforementioned business models. In order to answer this question we need to evaluate the qualitative novelty of such technologically enabled propertization, and outline its affordances and limits.

4.4. Limits of the technologically enabled data propertization

4.1. Anonymization and data markets

Proposed blockchain IoT implementations do promise to tackle one large core set of privacy issues associated with the concentration of private data in the hands of sensor providers and manufacturers. In that respect, decentralized access-control layer enabled by a blockchain application partially addresses the question of users' control and ownership for the hardware elements of the IoT architectures, raised by van den Hoven and Vermaas (2007). It is hard to underestimate the value of this proposition, considering that in centralized IoT architectures hardware and service providers defacto have full deliberation to choose what types of personal data will be commodified – and the default choice is all the data that they can get their hands on. Still, given the wider range of ethical issues regarding inferential data and consumer IoT

products, it is clear that the mere transfer of this choice to the owner of an IoT sensor hardly alleviates all privacy concerns.

It is fair to say that these issues are not addressed directly in the proposals for blockchain-enabled IoT data marketplaces. One possible explanation is that implicitly these solutions do mirror Laudon's (1996) and Lessig's (2006) normative assumptions that market-based incentives can promote technological solutions desirable from the privacy perspective, bootstrapping wider adoption of anonymization techniques. In the similar vein, in his arguments on private data ownership, Pentland (2009) suggests two broad avenues of approach towards privacy risks: enforced use of anonymous data, and monetary compensations. One of the elements in the 'Enigma' project aims to address the issue of anonymity with the proposal on integration of privacy-preserving data analytics. Services and data users in this scheme – using secure multi-party computation (sMPC) on the encrypted data – are only allowed to obtain the final results of the computation, but never get to observe raw data (Zyskind et al., 2015a; Zyskind et al., 2015b; Zyskind, 2016).

However, the practicality of this approach in the context of consumer IoT raises certain concerns. Secure MPC has been proved to be feasible for specific applications, such as anonymous online voting or bargaining negotiations. General purpose implementations for highly distributed cases involving large number of participants, however, can incur prohibitively high computation and communication costs for data holders (Cramer et al., 2015). There are also questions of incentives for data collectors and services, since sMPC adoption requires them to solve the problem of integration with existing data processing systems and analytics workflows, raising issues of economic feasibility. Furthermore, it can be argued that sMPC does not address wide range of private data uses cases such as marketing, lending, and fraud prevention, which are built around the aggregation of fine-grained individual profiles.

'Enigma' tries to overcome scalability issues through the introduction of a dedicated peer-to-peer layer for sMPC, which allows data owners to share a piece of data over a number of parties (nodes) for computation. Parties do not execute all computations as one large group, but rather they are divided into many groups of constant size (quorums) and execute each round of computations individually. The combination

of this layer with a blockchain layer used for settlements in theory provides scalable sMPC, amounting to secret smart contracts (Zyskind, 2016). At the moment, though, there is no practical implementation of this approach, and the latest implementation of 'Enigma' aims to emulate secret smart contracts functionality using the trusted execution environment in processor chips, which is a less secure approach than sMPC.[45] Practical implementations of the decentralized data marketplaces, on the other hand, are already available – including 'Catalyst' by 'Enigma'.

Not only are decentralized marketplaces technically easier to implement than scalable sMPC, they also fall into the class of blockchain implementations which De Filippi and Hassan (2018) characterize as fundamentally malleable. As such, these marketplaces do not face issues of compatibility with existing business models, and can be easily adopted for the various use cases.[46] Thus, a realistic yet undesirable development scenario would suggest a lag between the adoption of marketplaces supplementing existing practices of data monetization, and privacy preserving data analytics. Such a possibility is illustrated by the example of a fully homomorphic encryption, still largely a prospective technology which nevertheless is already used to justify existing data collection practices (Rogaway, 2015).

These observations raise a serious concern that blockchain-enabled data markets could follow the path of previous proposals, where privacy concerns are brushed away with superficial reliance on the wide adoption of anonymization techniques. Spiekermann and Novotny (2015) make such a contentious argument when they say that "good-enough" anonymization can mitigate most of the privacy concerns associated with data marketplaces, since "in many cases re-identification of data does not cause harm to people" (p. 193). Such an approach can be considered rather objectionable on moral grounds, given that re-identification can be very harmful in a range of scenarios, especially in the context of diverse IoT data sources, which enable trivial re-identification.[47]

---

[45] See 'Enigma' protocol documentation: https://enigma.co/protocol/AboutThisRelease.html

[46] See this non-exhaustive list of various marketplace implementations for tangible and non-tangible goods: https://github.com/john-light/decentralized-marketplaces

[47] A great practical illustration for possible re-identification attacks has been provided by the researchers who managed to identify military personnel and members of the intelligence services in different countries by combining supposedly anonymized data from fitness bracelets, and publicly available data from social network profiles and geo maps (Postma, 2018).

Granted, it would not be fair to paint with one wide brush all the different anonymization tools and characterize them univocally. Still, the examples show that it is safer to err on the side of caution when dealing with ubiquitous sensors. In such an environment, the task is not simply to obfuscate real-world identity but any unique patterns that can be attributed to an individual. In the case of wearables or any other sensor equipment capable of providing mobility patterns, cross analysis of those patterns enables re-identification based on their uniqueness (Christin, 2016). Furthermore, as Christin shows, even if a sensor owner reports coarse location data, his or her precise location can be revealed on the basis of comparison with other sensor owners who have chosen to share more fine-grained data. Considering that geo-spatial data is a crucial attribute in many scenarios, including weather, air quality, road traffic, as well as other sensor readings, this opens a range of re-identification possibilities.

The related privacy issue is a vulnerability for IoT sensor owners to adversarial profiling based only on metadata. It has been demonstrated that even encrypted traffic from smart home appliances can provide rich metadata sufficient to reveal device types, sensor use patterns, and even high order behavior of the smart home occupants (Acar et al. 2018; Apthorpe et al. 2017).[48] Furthermore, data sellers on the decentralized data marketplaces, where no single entity can censor transactions or participation, are vulnerable to what could be called a kind of a Sybil attack. A smart-home owner may try to protect themself from profiling through the segregation of anonymized data streams, i.e. never selling all available data to one buyer. However, it would be trivial for an attacker to create multiple identities for data purchases targeting sellers with repeating unique patterns in order to aggregate rich profiles. It is also an issue for future research to demonstrate whether inferences based on metadata accompanying data products listings on marketplaces can present similar privacy issues.

These, of course, are limited examples, but they represent the tip of an iceberg, which is a fundamental contradiction between anonymization tools and big data. As

[48] Apthorpe et al. (2018) conducted an experiment using devices built on the traditional 'client-server' architecture that allows passive eavesdropper such as an ISP to gather internet traffic metadata. Acar et al. (2018) use a similar approach to infer device types, and user activities from the monitoring of wireless traffic. Although it could be argued that their findings are specific to these types of IoT implementations, their attack methods based on laboratory replication of traffic metadata generation and pattern matching are not architecture specific.

Barocas and Nissenbaum (2014) duly point out, comprehensiveness of databases and robust inference techniques available to data collectors, drastically widen the space of privacy violation not covered by anonymization techniques. In the absence of a market-wide adoption for the new types of data analytics such as sMPC, mere obfuscation of collected private data hardly addresses IoT privacy issues of inferred data (Durante, 2017). Thus, from a moral perspective, the suggestion that it is acceptable to make private data streams available on marketplaces because sensor owners are equipped with anonymization tools becomes akin to the suggestion that it is acceptable to open Amsterdam's floodgates because inhabitants are equipped with Wellington boots.

4.4.2. Technical limitations of property in data

This leaves us with the examination of another broad avenue for the mitigation of privacy issues suggested by proponents of the blockchain-enabled private data markets. Namely, that transparent multi-sided markets can serve as a robust regulatory mechanism capable of establishing morally acceptable data collection practices. This argument is based on two key premises, which deserve closer scrutiny here. The first is the idea that with transparent marketplaces and the ability to exercise property rights in data during the several stages of its lifecycle, market mechanisms will be able to deliver privacy to those who value it (Koutroumpis et al., 2017). The second key assumption is that monetary evaluation can accurately grasp not only nuanced privacy preferences but also the costs of privacy harms (Pentland, 2009). If these conditions are met, the argument goes, users of data will be compelled by the market forces to adjust their business models accordingly, since data use practices are known to all market participants, thus satisfying the varying, and fine-grained privacy preferences of individuals acting as data suppliers.

Strictly speaking, the idea of complete property in data in general is rather problematic, both from conceptual and practical points of view. Data by nature are non-rival; are cheap to produce, to copy and to transmit. Thus in order to treat data as an object of property, legal and technological tools should be able to not only provide excludability and alienability, but also transparent asset ownership claims. And, just a brief overview of digital management rights (DRM) technologies shows there are serious limitations to technology that can successfully put restrictions on the use of data,

and more so to guarantee persistent asset ownership claims. Nevertheless, it has been proposed that at least some of these restrictions can be applied to private data with the use of 'sticky policies' that assure data provenance (Spiekerman & Novotny, 2015). Similarly, Koutroumpis et al. (2017) suggest that blockchain-enabled solutions could act as mechanisms of transparent chains of provenance and enforceable usage restrictions.

At the moment, blockchain solutions for private data provenance are arguably much less researched in comparison to access-control solutions. Still, some implementations can provide insights into the scope and feasibility of such data provenance. Neisse et al. (2017) propose a blockchain-based platform for private data provenance tracking and accountability, implemented on the basis of smart contracts as a proof-of-concept model. Neisse et al. leverage the capability of smart contract applications to implement what amounts to dynamic end-user agreements linked to specific off-chain private data assets. There is, however, an important caveat here since the key purpose of their solution is to provide a GDPR compliance tool rather than a market-oriented platform. Thus, the provision of provenance is delegated between the smart contract layer and data controllers that are assumed to be acting as trusted parties restricted by the legal framework.

The main role of a smart contract here is to provide a description of conditions for data access, usage and data transfers that can be modified on the basis of dynamic consent, as well as a means to demonstrate compliance with these policies. Using cryptographic hashes of private data as pointers to off-chain data, it is possible to ensure that all events associated with data transfers are logged in the blockchain ledger and guaranteed to be tamper-proof. This model, however, rests on the assumption that it is in the interests of the data collector to ensure accurate logging of these events, which are used as a proof of the lawful acquisition of the data. But more importantly, even if on-chain data is limited only by the hashes of private data this can also be very problematic from the privacy perspective. Finally restriction mechanisms available to the original owner of data here are limited by the withdrawal of consent, implemented as a unilateral power to deactivate the contract and so preventing its future use as a provenance mechanism. Thus, in itself such a solution does not prevent the unlawful holding or redistribution of private data.

Although at present, it is too early to predict the success of blockchain-based data provenance solutions, implementation by Neisse et al. (2017) highlights one key limitation of this approach. Smart contracts can be used to provide highly reliable provenance and even management for intangible assets that can be tokenized and stored on-chain, such as digital collectibles, utility tokens, etc. And as aforementioned, on-chain storage of private data is completely unacceptable from the privacy perspective. Linking off-chain assets to the smart contract layer, on the other hand, inevitably rests on security assumptions about the goodwill of trusted third parties. The cost of these assumptions can be relatively low in the case of tangible assets, which can be made uniquely identifiable and resistant to forgery, such as cryptographically signed IoT hardware.[49] However, there are no such mechanisms for intangible off-chain assets such as private data that could prevent misuse, duplication, and delinking from the provenance ledger.

4.5. Ethical limits of private data markets

As Floridi (2006) argues, digital information and communication technologies can alter the nature of informational privacy, and hence our understanding and appreciation of it. The same can be said of blockchain technologies which not only introduce new types of technological architectures but also provide strong incentives to re-consider and re-conceptualise our understanding of privacy and private data protection. This process, however, should be appreciated against the wider background of technological developments which as Durante (2017) points out require a shift away from the narrow, reactive understanding of privacy. Indeed developments in the IoT private data analytics urgently require us to reconsider the narrow conceptions of privacy which focuses only on the control of historical private data collection. These developments call both for practical privacy solutions and close critical scrutiny of privacy theoretical approaches.

From this perspective proposed blockhchain IoT solutions can be seen as an attempt to address this conceptual gap, not just as an introduction of new mechanisms for the private data controls, but also as a new re-conceptualiztion of the value of privacy understood and implemented as a property right. However, as this chapter demon-

[49] There are of course other assumptions here, such as absence of physical tampering and trust in the manufacturer of the equipment.

strates, technical limitations of the proposed solutions mean that blockchain enabled regimes of property in private data cannot overcome issues highlighted before by the critics of legal propertization. Namely, the tension between the multifaceted nature of the moral value of privacy and somewhat reductionist interpretations of privacy in 'property' discourse when marketed goods are being reduced to a single mode of valuation highlighted by Sandel (2013).

For one, proposed blockchain IoT applications only partially address issues of informational privacy regarding a moral right of a person to have control over access to technology that can be used to generate, process or disseminate information about oneself (van den Hoven & Vermaas, 2007). It does not seem plausible though that blockchain-based data provenance solutions can help data owners to exercise property rights, extending beyond initial collection of data. Secondly, these very technical elements enabling a wider range of developments including decentralized data markets, consequently open new avenues for an even more ubiquitous collection of private data. While some of the proposed solutions include novel tools such as sMPCs that aim to mitigate privacy risks associated with the widening scope of collected data, it is questionable whether these new types of data analytics can address all scenarios of consumer IoT applications.

And given the fundamental contradiction between the availability of big data sets which enable rich inferences, and the efficiency of data anonymization tools, proposed data marketplaces instead will only aggravate privacy concerns regarding secondary uses of data, highlighted in this chapter. Of course, the temptation to introduce a 'silver bullet' solution that could balance privacy issues and the wider benefits of IoT such as technologically enabled property in private data is understandable. Even more understandable is the temptation for developers to tap into new financing mechanisms that could provide bootstrapping and wider adoption of the new technology. Blindly proceeding in this direction without regard to the moral concerns, however, can bring one to the point of launching an ICO for the equivalent of a 'Clipper chip'.[50] And indeed technical limitations of the proposed solutions translate into profound ethical concerns amounting to the arguments against such blockchain enabled regime of property in private data.

[50] The infamous 'Clipper chip' was advertised by its proponents as a solution capable of reconciling issues of individual privacy with the practices of mass surveillance (Rogaway 2015).

The central issue here, often ignored or omitted by the proponents of data propertization, is the fact that even if we could conceive of a perfectly transparent private data market, capable of providing fine-grained compensation for diminished privacy to its participants, it does not address the core issue of whether such evaluation appropriately reflects underlying norms of privacy. Furthermore, in the context of blockchain-enabled decentralized data marketplaces, ethical contradictions of private data propertizaion are magnified by the very properties that enhance fairness and inclusiveness of these markets from an economic perspective. Censorship resistance, lack of a central authority, low barriers for participation and reduced transaction costs, can enable highly efficient mechanisms for the commodification of any private data. This leads to further blurring of the distinctions between fees and fines, further diminishing the moral component of privacy concerns.

One particular set of IoT consumer applications rather vividly illustrates this issue. Internet connected toys and other appliances targeted at minors, enable the collection of very sensitive data from children and their parents (Haynes et al. 2017). To suggest that these instances of privacy violations could be remedied with monetary compensations misses the point in the same way as a suggestion that the issues of child labor can be remedied with fair wages. And this specific set of moral concerns certainly does not exhaust the list of privacy norms ignored by the market approach. Consider proposals on blockchain enabled markets for health and genetic data (Levine, 2018).

The focus of privacy concerns in cases of sensitive health information collection, such as genomic data, is a prevention of wrongdoings including social sorting and discrimination on the basis of such data, among other harms (Bruynseels & van den Hoven, 2015). Monetary compensations as fees fail to address these concerns and others complex issues such as group privacy of genetic relatives. Not only genetic data, but also personal biodata in general, present a set of very specific privacy norms. In the case of medical data, the value of privacy, among other things, reflects the moral obligation of medical professionals to respect a patient's dignity. Violations of privacy that neglect these concerns can be appropriately addressed with fines but not with fees.

A market approach to the evaluation of privacy not only presents the risk of corruption for the existing norms, but it may also distort the perception of emerging moral issues. It has been argued that a crucial moral aspect of informational privacy is a matter of personal identity construction (Floridi, 2006; Durante, 2017), and autonomy of moral identity (Manders-Huits & van den Hoven; 2008). From this perspective, ownership of personal information should be seen as ownership in the sense of belonging, as a constitutive part of a person, rather than property or commodity.

This observation provokes questions that cannot be easily answered in the framework of market relations. What types of data should be seen as constitutive of a person then, or how should we define privacy violations when data are interpreted in ways that are detrimental to the construction of personal identity? The vision of the society where everyone's identity is assessed only by its market value not just paints a bleak future of human relations, but threatens to undermine the very foundational aspects of personhood and autonomy.[51] And it avidly demonstrates deficiency of the property based conceptualization of privacy not only from practical but also from moral-theoretical point of view. Indeed, the ethical limits of the proposed blockchain enabled markets for private data provide compelling arguments against the 'new deal on data' formulated and justified in the utilitarian vein as a universal solution to the issues of privacy (Pentaland 2009).

Furthermore, the tension between property-based and rights-based approaches to privacy in this context highlights the pitfall of technological determinism in the process of privacy re-conceptualization. While on the surface decentralized data markets seem to provide an avenue for libertarian economic peer-to-peer relations, at the core – and dressed in the veil of technological determinism – these solutions rather entrench a false perception that the total datafication of human lives is inevitable. Where privacy – understood as a moral right – questions the very desirability of ubiquitous data collection and processing, the concept of private data property paints dissolution of privacy as an inevitable process that can only be compensated for at best. Not only is this interpretation highly misleading, it also obfuscates the

[51] These issues present particular interest in the context of related blockchain developments known under the label of 'self-sovereign identity' solutions. Seen primarily as alternatives to the existing mechanisms of online and offline personal identification, some of these solutions also contain enabling elements for the commodification of personal data.

fact that we can and should choose which conceptions of privacy get implemented in the design of technical systems.

The significance of these choices becomes particularly evident in the context of blockchain technologies. Markets enabled by blockchain implementations, unlike legal regimes of property in data, do not leave much space for the luxury of post-factum deliberations, and if the history of cryptocurrencies can serve as an example here, once these technologies become sufficiently adopted there is no way to roll them back. This does not suggest of course that blockchain enabled solutions for consumer IoT products and services can not be morally desirable from the privacy perspective. Quite the opposite, some elements of the proposed blockchain applications, namely solutions for the decentralized access-control layer in IoT architectures, could help to alleviate many of the privacy issues inherent in current consumer products. However, this can be achieved only if technical elements are disentangled from the attempts to introduce the propertization of private data, as otherwise, these very elements will instead contribute to the further dissolution of privacy in the world of ubiquitous sensors.

5. Sovereignty, privacy, and ethics in blockchain-based identity management systems

5.1. Introduction

Any technical solution dealing with the issues of human identity management and private data, can carry with them a set of ethical challenges. This is especially so in the case of Self-Sovereign Identity solutions enabled by the blockchain technology developments. Much like cryptocurrency applications, these systems aim to reduce reliance on trusted authorities replacing them with distributed ledgers as sources of trust. Proponents of these solutions argue that SSI systems can bring enhanced privacy, data security and full controls over their digital identities to individuals (Tobin & Reed 2016; Allen 2017; Ma et al. 2018; Wagner et al. 2018). These claims are loaded with ethical assumptions seemingly targeting the very core set of concerns about the changing nature of privacy and identity in the emerging socio-technical structures of contemporary society. And as with many other similar claims, it is hard to disentangle actual technological implementations from promises, unsupported assumptions, and even misinterpretations, constituting the all too familiar retinue of blockchain technology applications.

The task to qualify these claims becomes even more complicated once we consider that SSI systems, like many other blockchain implementations, are still very much a bleeding-edge technology in the experimental stages. However, unlike other implementations, these experiments seem to deal with hypersensitive issues of individual identity and identification. And as Sen (2007) vividly demonstrates on the historical lessons from the 20th century, experiments on identity can have dramatic and undesirable consequences. Thus, disentangling the valid moral reasoning behind SSI technology from false assumptions and far-fetched promises is hardly an optional task. It is also clear that a proper moral evaluation of any technical implementations cannot be carried out in the vein of a naive technological determinism. The complexity of technology development cycles, does not always guarantee that even the noblest moral aspirations of its creators will necessarily translate into desired social

outcomes. With wider adoption, technologies become embedded into preexisting social, economic and political contexts and resulting socio-technical phenomena not only surpass the ambitions of its creators, but sometimes also bring outcomes completely opposite to the intended.

This is especially true for blockchain technologies: those key properties – malleability, low costs for entry, and potential for rapid adoption on a scale – make accurate predictions very problematic (De Filippi & Hassan 2018). This is even more so when such predictions involve reflections on a philosophically loaded phenomenon of 'identity' and 'sovereignty'. Unsurprisingly then, some critics in the field of SSI solutions developments are calling for the heavy baggage of philosophical reflections – which only distract the developers from bringing the practical benefits of technology for society – to be abandoned as they would rather focus their efforts on the rapid market adoption for these solutions (Ma et al. 2018). And arguing that the concept of 'sovereignty' in SSI solutions should be treated as completely unrelated to the traditional meaning of that term (Wagner et al. 2018).

The problem with this approach, of course, is that even if moral-philosophical considerations are explicitly postponed in the process of technological development, it does not mean that the resulting solution will be morally neutral. As Manders-Huits (2010) argue, any identity management system inevitably carries a special sets of moral concerns primary of which is a nominalization of identity – the reduction of personal identity to a set of forensic descriptions; a process that ignores fundamental moral considerations of respect for persons. Neither is it possible to narrow down our moral concerns to the set of issues regarding only the protection of private data in the context of identity management systems as suggested by Ma et al. (2018).

Identity related data does not need to be linked to specific natural persons worthy of protection – as a discourse concerning private data protection presupposes – making this category of data distinct from private data. Thus, even without direct linkage to individuals, such identity relevant data can structure interactions with them in a ways that invoke moral concerns (Mander-Huits & van den Hoven 2008). Similarly, Shoemaker (2010) argues that it is not possible to disentangle moral aspects of private data management from the issues of self-determination and identity formation,

given the changing nature of identity in the digitalized world defined by the ubiquitous collection of private data.

It can be said thus that the task to explicate the key moral concerns driving the development of SSI technologies regarding philosophical issues of sovereignty, identity and privacy is hardly an optional exercise. This chapter aims firstly to outline the context of the social and technological developments that define the moral concerns motivating the development of SSI technologies. Such investigation is impossible without first locating the common normative theoretical and technological roots of SSI systems and other blockchain implementations.

Not only is this necessary to clear up some basic misconceptions, but also to understand the rather special status of moral concerns surrounding the very idea of 'self-sovereignty' in a broader context of blockchain technologies. From its very first instantiation, blockchain technology – presented to the world as the Bitcoin application – has been deeply intertwined with issues of individual freedoms and rights in the world defined by information-communication technologies. Indeed, a quote attributed to Bitcoin's anonymous creator, Satoshi Nakamoto, explaining some motivations behind the project, is worth citing here: "we can win a major battle in the arms race and gain a new territory of freedom for several years."[52]

This statement, which may seem a colorful metaphor at a first glance, refers to the set of key moral concerns regarding issues of autonomy, self-determination and individual rights in the context of changing social structures that are more and more defined by the new technologies. In that sense the "arms race" refers to the fact that with the growing dependence of contemporary society on communication infrastructures, the adversarial thinking initially constrained to the fields of cybersecurity and cryptanalysis, spilled over into many other contexts of social relations on an unprecedented scale. In fact, this apprehension was highlighted much earlier by David Chaum (1985).

[52] The Cryptography Mailing List. Full context of citation is a response to a previous mail in the mailing list: "You will not find a solution to political problem in cryptography" - "Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years". Available at: https://nakamotostudies.org/emails/re-bitcoin-p2p-e-cash-paper-3/

Chaum argued that a society dependent on computer networks in all aspects of everyday life, risks extending the logic of computer security into many other realms of social relations. This, in turn opens up a Pandora's box of a dossier society, repeating rigid hierarchical structures of centrally controlled communication systems, built around mandatory identification, mandatory trust assessment, and scrupulous record keeping of past behavior for individuals. It can be said that Bitcoin emerged from this line of thinking; an attempt to change the balance of power between entities racing for control over key communication infrastructures, and individuals becoming more and more dependent of those infrastructures.[53]

Unsurprisingly then, the idea of self-sovereignty, not only in respect to financial sovereignty of cryptocurrency solutions, but in a broader politico-philosophical context takes prominent place in different implementations of blockchain protocols (Reijers et al. 2016). Thus, it may seem at a first glance that the idea of 'self-sovereign identity' implemented on the basis of blockchain is a direct manifestation of the same techno libertarian ideas, a tool that is capable to shift the balance of power in favor of individuals. Another prerequisite key element suggested by Chaum (1985), necessary to steer the technological developments away from the path of dossier society.

This chapter argues that the normative concept of 'self-sovereignty' is, in fact, distinctively different from the technical term of 'self-sovereign identity' used as a label for a rather broad family of technological standards and solutions. However, as this chapter aims to demonstrate, the gap between moral-philosophical and technical meaning of these concepts should not be ignored, and the moral desirability of SSI implementations directly depends upon our capacity to bridge this gap. It is argued that the normative ideas of 'self-sovereignty' can be better understood through the vein of critique on the moral foundations of sovereign powers, revealing certain commonality with the Lockean critique on the moral sources of authority in the society (Locke 2003).

The concept of functional sovereignty here provides an important analytic tool that helps to disentangle and highlight key moral concerns surrounding the development

[53] Bitcoin was influenced by a long line of successive projects, attempting to implement cryptographically based digital means of exchange including Chaum's 'Digicash'. For historical overview of these implementations see Narayanan et al. (2016)

of SSI technologies. This theoretical grounding helps us to appreciate moral significance of SSI technologies and provides a guiding framework for the moral evaluation of some of the practical technological implementations. Section 2 of this chapter looks into the moral issues caused by the asymmetric distributions of powers in the technological infrastructures for identity management, explained and defined by the empirical and normative aspects of functional sovereignty. Section 3 takes a high-level overview of the key technological components for SSI systems, in order to locate the moral significance of these systems in the broader socio-technical contexts. Section 4 provides a moral-theoretical grounding of the idea of 'self-sovereignty' combining insights from the Lockean classic liberal critique on individual rights and the more recent philosophical tradition of thinking on the moral foundations of informational privacy. Section 5 concludes with the arguments that the gap between the moral aspects of 'self-sovereignty' and technical label of 'self-sovereignty' needs to be bridged to avoid the risks of identity nominalization in SSI systems.

5.2. New domains of sovereignty

The concept of sovereignty has a long history and a variety of meanings in different discourses. Thus, for the first step of our investigation it is crucial to outline the peculiar and unique role that the concept of sovereignty enjoys in different fields. One key aspect of sovereignty is highlighted by Kalmo and Skinner (2010), who argued that the ambiguity of sovereignty has certain historical depth, being not a result of conceptual confusion, born out of misunderstanding, but rather a reflection of past efforts to give it content. As such, most of the time arguments about sovereignty are not merely scholarly debates on the meaning of terms, but rather arguments about allocation of power. It is also a liminal concept in the sense that it inhabits frontier, grey areas in between law, ethics and political sciences.

Furthermore, as Kalmo (2010) argues, the concept of sovereignty is a liminal concept in the sense that it is poised between facts and norms. In the field of international jurisprudence, for instance, it points to a paradoxical possibility that when illegality becomes extreme (such as formation of new state), it can convert itself into a new standard of legality. Similarly, Werner and De Wilde (2001), providing analysis of concept of sovereignty in the context of international law, point out that treating sovereignty as a purely normative concept is equally erroneous as trying to

define it as a purely descriptive one. First and foremost, sovereignty is a claim – not only a factual claim or merely a normative one, but also a legitimizing claim. What is meant by this, is that a successful claim to sovereignty aims to establish a link between a certain institutional fact and certain rights and duties following from this fact. Thus, it can be said that the unique liminal status of the concept of sovereignty means that ascription of sovereignty reflects a struggle over whom or what institution ought to posses it. It is never merely a description of empirical fact, but also an attempt to legitimize and justify a certain state of affairs.

To understand some empirical aspects of these transformations in the context of our investigation, it might be helpful to employ a concept of a *functional sovereignty*. This concept was first introduced by Riphagen (1975) in the context of international maritime law to describe a new phenomenon of legal rights occurring outside the scope of territorial rights traditionally defined and circumscribed by the context of national sovereignty. He suggested an application of a concept of functional sovereignty in those cases where there is said to be a *stateless domain*, yet where there seem to be some government in the absence of territory. It can be said that new information and communication technology (ICT) infrastructures, brought about by the creation of the Internet and other technological developments, effectively create new domains outside the scope of traditional territorial divisions.

This is, of course, a very multifaceted issue, covering numerous phenomena such as, for instance, 'Balkanization of the Internet' – attempts by state actors to translate national boundaries in the virtual spaces,[54] or the more recent generation of 'encryption wars' – manifesting as a struggle between various corporate and state actors to control vast amounts of persona data.[55] And interestingly enough, sometimes this struggle for functional sovereignty even spills over into, and overlaps with, the tradi-

[54] The term 'balkanization of the Internet' is used in different discourses, and can refer to a wide range of issues. Here, it refers to the increasing legislative and technological measure of national governments, aimed to ensure control over certain segments of the Internet. These measures include localisation of data in rest and in transit within physical boundaries of nationals state, censorships measures targeting national segments of the Internet, and measures aimed to ensure compliance of service providers with local regulations. For an extended critique of this issue see. Hon et al. (2016)

[55] Widely publicised legal battle between Apple and FBI, regarding access to data encrypted on Apple hardware, is just one of such examples (Zetter, 2016). Or concessions that Apple made to the Chinese government regarding the storage of Chinese Apple users' data.

tional domains of territorial sovereignty, with the developments of smart-city infrastructures.[56]

But of course, in the context of our investigation the greatest interest presents the emerging domain of new identity management systems. While it would be naive to expect a complete characterization of this domain in the scope of a single research chapter, it is possible to highlight some key trends defining developments in this area. And as strange is it may seem, it is possible to highlight just two major players in this field that could be credited with the spearheading of key developments and largely the formation of this domain itself. These major players are of course two companies that came to define the commercial Internet as we know it: Alphabet (formerly Google) and Facebook.

The latter, in a sense became an epitome for the very concept of online identity for the millions of Internet user. And what is more interesting is that Facebook not only introduced a new global identity layer for the Internet as a new domain, but explicitly engaged in attempts to legitimize its status in this domain on (even if dubious) moral grounds. As chief privacy officer of Facebook, Chris Kelly, expressed in relation to this claim: "We've been able to build what we think is a safer, more trusted version of the Internet by holding people to the consequences of their actions and requiring them to use their real identity" (Kirkpatrick 2011). Furthermore, these attempts to exercise such self-legitimizing functional sovereignty from the position of 'brute facts' went largely unchallenged by regulators and the public at large up until recent revelations around large-scale data abuses that came to light in the context of 'Cambridge Analytica' scandal (Adams 2018).

But the real scale of this domain is probably even better illustrated by the company Alphabet acting in this space as a main competitor of Facebook. Combining private data from its various surveillance platforms, the most well known of which is Google, it manages to aggregate incredibly fine-grained and full profiles, not just of Internet users, but increasingly extends its profiling practices in the physical spaces

[56] A recent controversy surrounding the development of a smart-city project in Toronto provides a glimpse of such future contradictions (Canon, 2018).

on a truly staggering scale (Schmidt 2018).[57] And even though these two companies are exemplars of self-proclaimed sovereigns in these new identity domains, they in fact represent just a tip of an iceberg, which is largely an opaque, global private data industry that includes corporate and state actors of various calibers and ambitions, trying to aggregate dossiers, consumer profiles and ultimately silos of identities (Ramirez 2014; Chrsitl & Spiekermann 2016).

Some further insights on the key trends taking place on the global scale provide two ambitious nation scale projects – 'Aadhaar' in India, and 'Citizen Social Score' in China. These projects can be seen as attempts by the respective national governments to extend the scope of national sovereignty in the new domains enabled by the developments in technological surveillance apparatus. And as with other claims for sovereign power, these are deeply entangled with moral claims aimed to legitimize these new extended powers.

Aadhaar – a centralized identity database for Indian citizens built around biometric identification – presents an interesting example of what Kalmo (2010) characterized as a paradox of sovereignty and illegality. Dixon (2017), providing a timeline for the implementation of Aadhaar, points out that the system was effectively put in place in the absence of any connected regulatory and policy guidance.[58] At the same time, the introduction of this system was justified to the general public, largely on the moral grounds, as a necessary implementation capable of preventing fraud in the distribution of state subsides. And just like in the case of corporate identity management systems, moral argumentation aimed at justifying Aadhaar implementation is overshadowed by numerous data breaches, instances of data abuse, and function creep that effectively undermine the validity of this justification (Dixon 2017).

---

[57] Both Facebook and Google should also be noted for their efforts to introduce end-user identity solutions, built on top of their massive private data silos - 'Facebook connect' and 'Google sign-up' respectively. These are sets of Application Programming Interfaces (API), that can be implemented by third party web-services (websites, apps, etc.) to let their visitors authenticate themselves using Facebook or Google identities.

[58] As Dixon observes, by the time Adhaar system passed the barrier of one billion enrolments in 2016, Indian government still has no passed national data protection and privacy legislation. And more astonishingly by the time of passing of 'Aadhaar act' regulation the system has been in place effectively for seven years.

But, an even more fascinating example of this trend in the development of identity management systems is presented by an ambitious project by the Chinese government – 'Social Credit System' (SCS). This system, envisioned as an integrated registry of Chinese citizens, is maintained on the basis of collaboration between various state agencies and commercial companies. But unlike other state identity management systems, SCS goes beyond mere forensic purposes and implements an explicit system of scores for profiled citizens designed to reflect their 'trustworthiness'. Furthermore, having a low or high score has very real material consequences for profiled individuals, formalised in the system of respective rewards and punishments (Ohlberg et al. 2017; Engelmann et al. 2019).

In that sense SCS presents an 'endgame' example of a complete system for surveillance and profiling, which in itself carries profound moral issues. However, it also serves as a fascinating example of an effort of the Chinese government to exercise its sovereign power in a completely new domain. In itself the claim for the sovereign right to define moral identities of its citizens is not new for Chinese or other governments, and can be traced back in history to probably as far back as the theocratic societies of the Bronze Age. Koskenniemi (2010) also draws a historic parallel, highlighting continuity between early Christian practices and manifestations of sovereign powers in some modern governments by subjecting its citizens to the 'controlled mechanisms of identity formation'.

What makes SCS implementation historically unique, however, is firstly its scale, and secondly, the modality of its normative components. It is not merely a system prescribing moral norms and identities, but effectively an integrated control apparatus that ensures adherence to prescribed norms through automated rewards and punishments. Thus, it is not merely a 'moral code of conduct', but a socio-technical engineering project aimed to eliminate, 'untrustworthy elements' and 'black sheep' in society (Ohlberg et al. 2017). Unsurprisingly, the system carries a distinct character, prioritizing the focus on behavior that can result in a lower scores and consequently emphasising punishments (Engelmann et al. 2019).

SCS thus, represents a highly peculiar (and disturbing) illustration of a trend characterized by Koskenniemi (2010) as a transformation of sovereignty from traditional *limiting* sovereign powers, to *enabling* powers. As such, sovereign power is not only

state power used to limit certain actions of its subjects, but rather power to define the very category of a subject. This is also a moral problem characterized by Sen (2007) as a denial of choice and responsibility for one's own identity, when individuals are prescribed with 'true' singular identities, stemming either from national or religious identification. And this shift also largely defines manifestations of *functional sovereignty* in the domains of identity management systems, not being limited to state entities but also found in actions and strategies of hybrid and corporate actors.

From that perspective, a widely cited statement by Facebook's founder Mark Zuckerberg takes on a new meaning: "Having two identities for yourself is an example of a lack of integrity" (Kirkpatrick 2010). Indeed, this statement is not merely an opinion, or expression of a moral view by a private person, but effectively a claim for sovereign power by a transnational identity platform to define criteria for 'good identity'.[59] Similar claims can also be found in the attempts to establish epistemic authority of technological solutions for the 'personality assessment', claiming ability to reveal one's 'true', 'real' identity (Youyou et al. 2015).

And this trend manifests itself particularly vividly in the workings of the data-brokers' industry and various credit rating agencies, providing all types of identity assessments for financial institutions, marketers and employers (Ramirez et al. 2014). In the sense these developments also characterise an *identification creep,* where types of social relations that do not require persistent identification of counteracting parties become supplanted by epistemically asymmetric identity based relations, driven by the logic of adversarial thinking. Relations where each party tries to find as much as possible about their counteragents to achieve an information asymmetry to ones' own advantage in a manner of a zero-sum game.[60] These systems, implemented on the basis of proprietary algorithms, create truly Kafkaesque, scenarios when completely arbitrary entities wield power to define the criteria for 'good' or 'bad' identities as a matter of brute facts, power not justified by the legislation or any other kind of social agreement (Lecher, 2019).

---

[59] Another vivid and disturbing example is an educational program for schoolchildren designed and financed by Google with a stated aim to tech children 'the fundamentals of digital citizenship', which present Google to pupils as an impartial and trustworthy entity (Singer & Maheshwari, 2018).

[60] Truly bizarre examples can be found in different consumer applications of solutions for the 'identity assessment', now offering even algorithmic assessments of trustworthiness of baby seaters, on the basis of social network data (Harwell, 2018).

Furthermore, such profiling and rating systems not being confined to legal grey spaces, partially become adopted and legalized post-factum; once again reinstating the paradoxical nature of sovereignty as a capacity to convert cases of illegality into new standards of legality (Christin et al. 2015). Thus, in the domain of identity management systems, the concept of f*unctional sovereignty*, applied as an analytical tool, helps to unfold complex empirical phenomena into its key components – emergence of new powers by various entities not only to assign identities within new sociotechnical systems in the forensic sense, but also powers to define criteria for the normative assessments of assigned identities.

From this investigative empirical perspective, moral claims supporting implementations of these systems are first and foremost legitimizing claims. An attempts to establish a link between certain institutional fact and certain rights and duties following from this fact, that becomes successful when new standards of legality are established (Werner & De Wilde 2001). These observations not only suggest another dimension to the problem of 'arms race' and 'territory of freedom' highlighted by Satoshi Nakamoto, but also define a very complex background for the implementation of SSI systems.

As we can observe, this fixation on identity, warned against by Sen (2007), is not going away in the 21st century. Quite the opposite, fascination with the identity, the framing of identity as 'the solution' to grand ethical challenges, drives the development of identity experiments of an unprecedented scale, and of unprecedented ambitions. And quite often SSI solutions are seemingly surrounded by the same grandiose ethical claims as Aadhaar and Social Credit Score systems. Indeed, among its ambitions, transnational alliance ID2020 claims to offer solutions to such global issues as economic inclusion in developing countries, humanitarian refugee crises, world hunger and many others.[61]

This highlights a certain paradox that state actors and transnational corporations – all those entities that can hardly be suspected as being champions of techno-libertar-

[61] Microsoft, Accenture and Avanade, are partners of ID2020 alliance, collaborating on the development of blockchain based 'self-sovereign' identity solutions. https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/

ianism and libertarian interpretation of individual rights – seem to embrace the label of 'Self-sovereignty'. An unflattering parallel with other experimental identity management systems causes a valid apprehension that these claims may also fall into a category of legitimizing claims, devised merely to justify and validate instalments of new socio-technical structures. To address these concern we need to look into the key technical components that could be considered definitional elements of SSI solutions. And secondly, we need to ask whether the moral claims on the desirability of SSI systems fall into the category of legitimizing claims surrounding installations of new identity management systems, or if these claims do have valid moral foundations.

5.3. Technical components of SSI systems

In comparison with the original blockchain implementations, it is difficult to highlight one single project that could be representative of SSI technology in the same sense as Bitcoin is a flagship example of blockchain-based cryptocurrencies, or Ethereum is a prototypical protocol for smart contracts. At the moment there are at least 100 different projects that employ blockchain technology in order to provide functionality of digital identity in one form or another.[62] All of these projects are in different stages of development, some of them lacking sufficient documentation that would allow for closer scrutiny. And considering how generally volatile the field of blockchain-based projects are, it is reasonable to highlight those in the later stages of development that go beyond mere proof-of-concept implementations.[63]

Two of these projects are: 'uPort' identity project developed by ConsenSys[64], and the 'Sovrin' project by Evernym.[65] At this point it is difficult to predict whether any of these solutions will be widely adopted, so it does not seem feasible to go into details of their particular implementation. But it is helpful to get a high level overview of the

---

[62] Strictly speaking not all these projects aim to provide full solutions, but the list is representative. See: https://github.com/peacekeeper/blockchain-identity

[63] A useful metric can be found on tokendata.io which lists all blockchain based projects using ICO model of funding. On the state of February 2018 around 46% of projects that were listed from the year of 2017 have inactive status.

[64] https://www.uport.me/

[65] https://sovrin.org/

underlying technology that highlights the basic properties of SSI implementations present in most of these projects to a certain degree. Considering that any SSI at this point is very much a bleeding-edge technology, there are no clearly established standards. However, impressive work in this area has been accomplished by W3C Credentials Community Group. Some of these standards are implemented in one form or another both in Sovrin and uPort projects, so we will briefly cover them here.

Three specific technical components that comprise and enable the idea of SSI technology, present key interest here. It should be noted that these standards are not blockchain specific, however it is assumed that practical implementations currently are most feasible on the basis of blockchain technologies. The first key concept here is a standard of *Decentralized Identifier* or DID; essentially a digital identifier. Its core idea is similar to that of a Uniform Resource Locator (URL) identifier. However, DID points to entities (endpoints associated with individuals or organizations, for instance) rather than web resources. And unlike a URL, it is implemented as a data structure in a machine-readable format, though a user-friendly identifier like a name or pseudonym can be mapped to DID. In itself, generic DID can be represented as an index-value pair that contains an identifying string of symbols – ID index, a machine-readable structured piece of data, and DID document as value. DID document does not in itself necessarily contain personal data, but can include an ID string as a designation of the owner, information about context of identification, cryptographic methods of authentication (specific public keys) and pointers to method of authentication (specific blockchain ledger).[66]

The second key concept here is an idea of a *Decentralized Public Key Infrastructure* DPKI – essentially a database containing public keys that can be used in DIDs. To elaborate, it is helpful to keep in mind that the method of two-key encryption (or asymmetric cryptography) can be used both to encrypt messages and sign them. For instance, Alice, the owner of a key pair (public and private key) publishes her public key, so that Bob or anybody else can use it to encrypt messages in such a way that only Alice can decrypt them using the private key. Alternatively, Alice can sign a message with her private key, so that Bob – using the public key – can verify the message was indeed signed by her (given that Alice is a unique holder of the private

[66] This is of course a simplified schematic representation of DID standard, details can be found in W3C specifications: https://w3c-ccg.github.io/did-spec/

key). PKI can be used for both of these purposes, providing an infrastructure for the storage and sharing of public keys. Centralized trusted parties manage traditional PKIs: certificate authorities or messaging service providers, for example. The main novelty of DPKI is that using blockchain as a decentralized database can radically reduce reliance on trusted parties while at the same time ensuring security from manipulation, censorship or compromise (Allen et al. 2015). Schematically, it can be said that DPKI forms the base layer allowing for the management of DIDs. This scheme is not radically different from blockchain-based cryptocurrencies where a wallet address (which is a hash of a public key) represents an identity of its owner for other network participants. Such identities in themselves, however, provide limited functionality of verification.[67]

The third crucial concept of SSI, however, makes a significant difference: a capacity to issue proofs of credentials using DIDs. Analogous to physical credentials (or proofs) such as passports, driving licenses, etc, these are essentially cryptographically signed identifiers that can be used for proof of identity or specific identity attributes. This concept is defined as a V*erifiable Credential* – a set of claims (each claim referring to a certain property of an identifier) that are tamper resistant and the ownership (validity) of which can be cryptographically verified.[68] Represented in a machine-readable format, such credentials allow for a flexible combination of attributes, ranging from representation of government IDs to pseudonyms with one specific claim.

And that is where the 'sovereignty' component in the technical sense comes into play in this scheme. Public key infrastructure allows identity owners to issue claims about themselves and ask publicly known verifiers to sign them, or map to existing verified claims in a pseudonymous way. Furthermore, in a 'sovereign' way user can issue, modify and revoke credentials and choose which identity attributes are shared with which parties. This not only provides capacity for minimised data disclosures, but also enables identity owner to choose where private data is stored, since DID can map to any data repository (for instance personal hardware).

---

[67] However, on the level of the fundamental design assumptions this approach is very different from cryptocurrencies using Proof-of-work protocol (POW) as will be explained later.

[68] See: https://w3c.github.io/vc-data-model/

To illustrate it in a very simplified way, Bob can generate a unique pseudonymous DID that states that the owner of an identifier is older than 21, and using his digital driving license (also issued in this scheme) ask a motor vehicle authority to sign it. This credential can be used, for instance, to buy alcohol online with cryptocurrency, in a privacy preserving way. The vendor can verify that the owner of this DID is indeed older than 21 – since it is signed by a known entity - without learning anything else since. And Bob can generate any number of such claims for different vendors for enhanced privacy.

This scheme is more complicated in practice and can employ complex cryptographic tools such as zero-knowledge proofs. Using this method for extra obfuscation, Bob can prove to a vendor possession of a valid signature without revealing the signature itself (Smith & Khovratovich, 2016, Augot et al. 2017).[69] Such obfuscation of private data is a very promising approach to enhance the privacy of individuals that might use such solutions. Still, arguably the key novel element of this approach is enclosed in the decentralization properties of SSI schemes. It is suggested that in the future blockchain-based DPKIs will have so many cross-references to verified credentials forming cross web of trust, that it will be possible to issue credentials without reliance on trusted authorities such as motor vehicle authority, etc. (Tobin & Reed 2016).

The technical implementation of the uPort project is, in a certain sense, closer to existing cryptocurrency blockchains since it is built on the basis of Ethereum public blockchain. Ethereum, however, is not a cryptocurrency specific chain, since it can be seen as a distributed computation protocol capable of storing and executing programs called 'smart contracts' on virtual machines. Using Ethereum-specific protocols, the uPort SSI scheme creates a number of layers for the management of digital identities and verifiable claims. This scheme is different in some respects from the generic one given above. DIDs in uPort are implemented as smart contracts, where the blockchain address of a smart contract – string serves as a persistent identifier. DID document functionality in uPort is split between Controller Contract, Proxy

[69] It needs to be noted that these schemes are still very much in development and practical privacy assessment, would have to address such issues as identifier based correlations, signature correlations and other potential deanonymization techniques.

Contract and Application Contract.[70] This scheme makes uPort a public infrastructure on the basis of blockchain layer. Using a smartphone app, any user can issue and mange credentials on uPort, and connect these credential to private data stored off-chain (in any other data base separate from Ethereum blockchain). Currently uPort has a practical implementation pilot running in Switzerland, providing citizens of Zug with access to some of the e-government services.[71]

The Sovrin project takes a different approach, aiming to create full infrastructure for the implementation of SSI from scratch. As such Sovrin runs its own blockchain, which employs specific architecture and original consensus protocol. Sovrin blockchain is not public – in the sense that while any entity can use this scheme to manage credentials, in order to become a node in the basis layer network, an entity has to be vetted by the Sovrin foundation (which is an incorporated entity). Furthermore, only a limited number of all nodes have the right to add new records to the blockchain database, thus making this blockchain essentially private.

According to Sovrin, decentralization in such a network can be achieved via economic and political independence of nodes distributed in different countries, complemented with legally binding agreement for nodes formalized as 'Sovrin Trust Framework Agreement'. Individuals who wish to use Sovrin identity management for personal purposes are also supposed to sign a legally binding agreement. It can be argued thus that Sovrin provides a lesser level of decentralization for DPKI compared to public blockchains. However, according to Sovrin privacy is achieved with the focus being on the DID design and the proposed use of zero-knowledge proofs (Smith and Khovratovich, 2016), rather than network architecture in their scheme.

What can be derived from these technical descriptions is that SSI solutions in their current implementation are first and foremost tools for the management of private data. 'Sovereignty' here is largely interpreted as an ability to share verified credentials in a way preferring minimal data disclosures. Self-sovereignty in this sense can be understood as the concept of individual control over identity relevant private data,

---

[70] It needs to be noted that uPort can be compatible with W3C specific DID standard. See for instance: https://github.com/uport-project/secp256k1-did-resolver

[71] See: https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38b-d0ee3702

capacity to choose where such data is stored, and the ability to provide it to those who need to validate it, without relying on any centralized repositories of identity data. Furthermore, while it can be said that these solutions are enabled by blockchain technology, at the fundamental level of general design assumptions SSI systems fall into a completely different category then, say, Bitcoin.

This is a rather nuanced distinction that requires appreciation of different levels of abstraction. The key conceptual difference at a high level of abstraction, stems from basic assumptions laid in the Proof of Work (POW) consensus protocol in the foundation of Bitcoin blockchain (Narayanan et al. 2016). This approach demands the contribution of computationally expensive resources from network participants on a competitive basis to achieve network security, and thus abolishes the traditional requirements of identity, trust, and permissions. SSI solutions, on the other hand, aim to provide the identity layer on top of the blockchain protocol, rather in the traditional paradigm of identity-based systems security.

Thus it can be said that *sovereignty* for individuals takes significantly different forms in SSI solutions and cryptocurrencies. Bitcoin public network absolving requirement of identities both from those who would like to use or contribute resources, does at least – hypothetically – aim for egalitarian decentralisation.[72] The concept of a trust network lying in the foundation of SSI presupposes, of course, that any entity can become verifier, but there are fundamental differences between levels of trust in these entities in the real world. While nodes in Bitcoin network are ultimately replaceable and do not need to be trusted by the network participants, verifiable credential signed by a state entity or transnational bank carries a much higher trust value, both in the scope and in the weigh of claim validity (Wagner et al. 2018)

Thus, entities possessing certain 'trust capital' in the socio-economic sense, quite justifiably expect to claim advantageous positions in the future SSI infrastructures, serving as a nodes of trust. This, of course, is not morally problematic in itself, but

[72] This is also why prototypic blockchain applications are called 'permissionless', since there are no restriction on who can join the network and use its resources. Factual decentralisation of course is a separate issue considering that concentration of hashing power in the hands of entities controlling superior economic resources is a very real possibility. At the moment this balance is very fragile to say the least, but seem to improve at the moment of writing of this paper, compared with the state of network two or three years ago. See: https://www.blockchain.com/pools

rather highlights the limits of sovereignty that individual users may hope to possess; no-one stops Alice from issuing her own claim, verified by herself, but determining the value of such claim for others is not at her deliberation. And, it is also not up for Alice to decide what type of credentials she has to present when this transaction occurs in the existing scheme of power relations. As Sen (2007) remarks, our freedom to assert personal identities can be remarkably limited in the eyes of others.[73]

From that distinction it can be observed that the term SSI itself has two distinct meanings, in the normative sense of the 'Self-sovereignty' and in the descriptive sense referring to specific classes of identity management solutions utilising blockchain-based DPKI. The latter point is also illustrated by the fact that SSI systems are essentially agnostic towards types of entities that can be identified, and can provide a solution for the identification of, say, hardware elements in the Internet of Things systems. In that technical sense, 'Self-sovereignty' refers rather to the root of trust in the very specific technical sense (Conway et al. 2019).[74]

This observation also explains that, despite seeming connections with the original blockchain Bitcoin implementation deeply intertwined with libertarian ideas, technical label of SSI systems has a much more neutral normative meaning. And also partially explains why this label is being empathetically embraced by the wide range of actors who could hardly be suspected to be firebrand supporters of crypto-anarchy. Microsoft, IBM, World Bank, and even the US Department of Homeland Security (Funding donor of Evernym Inc. - developer of Sovrin) are just a few such examples.

This rift between technical and normative concepts in itself not particularly problematic, given that conceptual slippage is a very common occurrence in computer sciences, where concepts are borrowed from the social context, and used in narrow meaning such as 'trust' or 'gossip'. And yet there are instance when concepts borrowed from the social domains lose their original meaning in the technological context, but then get transferred back to the social context carrying over new semantics

---

[73] Again, predetermined power relations are not necessarily problematic in themselves. Mere replication of government ID via SSI scheme within the established and institutionalised ethical framework arguably does not carry the same set of novel ethical issues as for instance ID system provided by company those main business model is private data brokerage.

[74] In general terms the 'root of trust' is a source that can always be trusted within a cryptographic system.

and new normative content, as, for instance, in the case of 'trust'. China's Social Credit System provides an illustration of such a feedback cycle where the concept of 'trust' becomes applied in social systems, just as it is used in fields of cybersecurity. Here trust is just an operationalized parameter in the system to discriminate between 'trusted' entities and 'untrusted' on the basis of identification and past behavior in order to distribute access to the resources of the system, with humans treated as mere technical components (Engelmann et al. 2019).

It is a vivid and uncanny illustration of Chaum's prophetic warnings that security principles of hierarchal computer systems can easily become blueprints for social relations. While it would be too pessimistic to expect the complete depreciation of the moral semantics of 'self sovereignty', this is not an impossible outcome. As we have observed before, far too often highly moralized concepts become co-opted by various actors operationalizing these concepts in very pragmatic ways, as legitimizing claims, as competing claims to exercise sovereign power.

Given these observations, it is possible to say that normative assumptions do not disappear from the process of technological development, but rather become implicit and even obscured. Thus it become a crucial task to locate a valid moral foundation to the normative claims of self-sovereignty, to establish a successful counterclaim to attempts to strip this concept of its normative meaning. A failure to do so carries risks that moral promises of SSI solutions will be distorted and ultimately unfulfilled in the highly adversarial environment, which is the arms race for the control of one's identity.

5.4. Moral foundations of sovereign rights

A starting point in the quest to locate such a moral foundation is to look at how those components are defined by the proponents of SSI. Possibly the most explicit formulation of principles of sovereignty in the context of SSI technologies can be attributed to Allen (2017), who should also be credited with the popularization of the term itself. He formulates normative principles that discern decentralized digital identity management systems from other centralized and federated schemes. Some of the principles suggested by Allen are more concrete, such as the necessity of

open-source software for the implementation of SSI systems, together with calls for the standardization of digital identity formats allowing interoperability and portability. Other principles are more general and refer less to concrete technical aspects but rather to governance aspects of SSI systems, such as the use of decentralized databases, the absence of gatekeeping authorities and adherence to minimization of data disclosures. And finally, principles that can be considered as explicitly ethical ones – the importance of informed consent, the right to be forgotten and control over choice of identity verifiers for system users. It needs to be noted that principles in the latter group are formulated in rather general terms allowing for broad (and somewhat overlapping) interpretations.

But it is the very first of Allen's principles – labeled 'Existence' – that could be considered a key broad motivational principle with strong moral and political connotations:

> *"Users must have an independent existence. Any self-sovereign identity is ultimately based on the ineffable "I" that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the "I" that already exists."*

One fruitful interpretation suggests that this statement about identity independence aims to target this very loaded set of moral and political aspirations regarding individual rights to self-determination, at least in part connected with identity and conceptions of self. Such interpretation in itself, of course, hardly amounts to satisfactory clarification considering the battled status of definitions for these rights in legal and moral philosophy, yet it highlights the strong moral aspirations present in the ideas of 'individual sovereignty'. So it seems then that SSI technologies carry a lot of political and moral aspirations to radically restructure our society, deeply intertwined with ideas of control and ownership of private data.

Another rather insightful suggestion on the moral interpretation of sovereignty of identity is suggested by Marlinspike (2012), who argues about the necessity or recognition of an individual human right to possess data relational to ones individ-

ual identity, (credited by Allen as a source inspiration for his work on the principles on self-sovereignty). His argumentation demonstrates a strong libertarian leaning in the critique of exclusive rights possessed by the government to issues and assigning identities to its citizens. While Marlinspike does not elaborate this position in sufficient detail, it can be taken as a certain illustrative point, providing direction for further investigation.

Indeed in the broader family of blockchain solutions, normative claims on the moral value of self-sovereignty as well seem to take a prominent place. As Reijers et al. (2016) argue, self-sovereignty can be understood as a guiding governance principle in the design of original blockchain protocols, rather reminiscent of arguments found in some of the traditions politico-philosophical theorizing. Some of the parallels they identify reveal a strong connection of 'self-sovereignty', understood as a principle of the decentralization of power – very much in the vein of Rousseau's ideas of decentralized governance. Reijers et al. also draw parallels between certain egalitarian ambitions of the blockchain protocol designs and Rawlsian ideas of justice, understood as the idea of equal rights and liberties for all participants of the network. And rather counterintuitively, they reveal some components of the social contract theory suggested by Hobbes, drawing parallels with the assumptions on the self-serving motivations of the participants.

Latter comparison is particularly interesting given that Reijers et al. demonstrate an uncanny resemblance between Hobbsean delegation of individual rights to abstract power of 'Leviathan', as a stabilising mechanism of interaction between humans driven by selfish interests, and rules of blockchain protocol stabilizing pre-given system of human interactions (property, insurance system) as 'techno-leviathan'. And, indeed, there is a peculiar metaphorical parallel between technical limitations translating into rules dictated by the blockchain and brute facts of absolute power. For instance loss of private keys from cryptocurrency wallet, inevitably and irreversibly leads to the loss of funds, without any space for dispute. Similarly, transaction once validated in the blockchain ledger becomes irreversible and non-contestable. [75]

[75] This parallel, however, breaks apart with the observation that participation in any blockchain application is completely voluntary, and unlike Hobbsean 'Leviathan', power of blockchain protocol is not sustained by the constant threat of punishment.

Yet, as Reijers et al. (2016) suggest, these parallels should not be taken too literally given that the practical implementations of blockchain protocols seem to constitute their own ideas; an amalgam of somewhat contrasting assumptions that outline the idea of 'self-sovereignty' in the vein of social contract theories. It seems then that it might be fruitful to dig a bit deeper into the moral-theoretical arguments on the sovereignty and distribution of power. Interestingly enough in the context of SSI technologies, this argumentation shows a strong parallel with a Lockean classic liberal critique on the sovereignty, government and sources of human rights. In the 'Two Treatises of Government' – work foundational to the modern theory of human rights – Locke targets the idea of sovereign monarchy as a foundation of state and citizenship, juxtaposing to it the normative concept of natural rights (Locke 2003 [1823]). While the historic parallel is not entirely accurate, given that Lockean critique was targeted against absolute monarchy, once we consider the history of identity management systems this comparison suggests a certain validity.

Indeed, the invention of the modern passport as an identification system derives directly from the idea of a sovereign nation state, an exclusive right of a national government to provide and demand identities, circumscribed by the scope of the territorial sovereignty (Lloyd, 2016). In that sense the right of a national state to issue and demand identification for everyone within its territorial scope is reminiscent of an absolute sovereign right, a self-legitimizing fact that requires no external justification. From that perspective, the call to reconsider the source of this right aims to reframe the procedure of an identification not as an obligation or duty of citizens to be identified derived from the sovereign right of a state, but as a natural right of an individual to be represented via mediating role of institutions of identity.

This argument does seem to fall into a broader Lockean argumentation on the foundational status of natural human rights as the source of moral justification for the functions of the state and civil government (Locke 2003 [1823]).[76] This historic paral-

[76] Locke in 'Two Treaties of Government' juxtaposes the moral claim to individual right and monarchical claims to sovereign power, providing a strong rebuttal of the latter. Granted, here it could be objected that Locke does not propose an idea of individual sovereignty, but that of an individual right. Yet as Baranger argues (2010) despite apparent unlikeness the comparison of these concepts is not unjustified, both concepts in the original sense aim to highlight an individual in the legal sense, and both aim to locate source of right and duties in an individual. In the sense Lockean definition of individual right is actually conceptually closer to the original meaning of individual sovereignty, attributed to monarch as an individual bearer.

lel also illustrates another observation, highlighted by the emerging new domains of *functional sovereignty* – that calls to reconsider and redefine sovereignty historically coincided with moments of significant social transformations (Kalmo and Skinner, 2010).

To challenge claims on the legitimate sources of sovereignty in the vein of Lockean investigation on the sources of rights and powers, it is not enough to point out the contradictory nature of legitimizing claims for sovereignty in the vein of empirical analysis highlighted in the previous parts of this chapter. It is also necessary to locate the moral foundations of competing claims to sovereignty suggested by the proponents of the right for 'self sovereign' identity. This deeper moral theoretical aspect of the aforementioned socio-technical transformations can be found in the debates on the changing status of informational privacy and its intertwinement with the moral issues of personal identity formation.

Floridi (2006) suggests such an argument, based on the strong ontological interpretation of personal identity understood in informational terms, where an individual is not just represented by one's personal information but is effectively constituted by it. From that perspective, the unique dynamic status of personal identity defines a moral content of informational privacy as a matter of construction of one's own informational identity. An individual's freedom to mould one's identity, the freedom to build a different and possibly better self, goes against the artificial 'mummification' of identity represented in records and profiles, which takes the power to construct one's identity away from an individual.

Shoemaker (2010), arguing against strong ontological interpretation of informational identity, nevertheless also suggests that the right to informational privacy is also a right to control or manage the presentation of one's self-identity: a right to manage certain public construals of one's self-identity, or at least to have a say in determining how one's identity is interpreted by others. This right, suggests Shoemaker, constitutes a moral objection to data mining and subsequent profiling that effectuates construals of an individual's identity without his or her input in this process. Mander-Huits and van den Hoven (2008) suggest a somewhat different line of argumentation for informational right to privacy that is directly derived from the principles of moral autonomy, epistemic modesty and respect for the persons. The right to moral

autonomy as a precondition for freedom to develop and protect one's identity provides capacity to shape our own moral biographies, to evaluate and identify with one's own moral choices, without pressure or inference from others. The fixation of one's moral identity by others, constrained in the form of database records or identity management systems fails to appreciate the epistemic asymmetry between knowledge by description and first-person knowledge of one's identity. While the former fixes only facts of biography, the latter is deeply intertwined with one's thoughts, emotions, aspirations and higher-order evaluations.

Respect for privacy of persons from that perspective represents acknowledgement for epistemic modesty in explicit or implicit claims to know who someone is. Therefore, argue Manders-Huits and van den Hoven, even when it is impossible to leave it completely to individuals to design their own identities in identity management systems, they have a right to authorize and correct when and where it is appropriate, to avoid a nominalization of identity, and avoid its reduction to a set of externally imposed identifiers. As different first party and functional third party perspective may be, we should not forget that practical fragments of identity - identifiers, serve as building blocks and tools for the more complex 'own' person's identity. And there are always risks of moral failure when such new tools are introduced.

Representation of this aspect of persons is exactly what is missing when personal data is piled up in databases and personal identity become nominalized in administrative procedures, and instead of autonomously construction one's moral identity the person fits oneself into predetermined sets of identifiers (Manders-Huits, 2010). This moral failure takes a wholly different dimension when identity becomes not just nominalized, but also becomes assessed in the normative framework externally and authoritarianly imposed on the bearer of a said identity.

There are then compelling reasons to consider the claim for the 'self-sovereign' source of right to construal of one's own identity. Not just a right for the choice of attributes relevant for the presentation of one's own identity to others, but also a right not to have one's identity be permanently fixated in the externally imposed normative frame of reference. And it would be wrong to assume that this right should somehow be derived from the novel context of the emerging socio-technical structures. Quite the opposite, this right can be traced back to Lockean arguments

on the limits of powers and rights in a free society. While these arguments belong to their own historical context, in which Locke is occupied with the question of religious tolerance, these very issues are still foundational in the context of contemporary liberal society as well, as can be seen from the history of identity politics in the 20th century (Sen, 2007). In 'A Letter Concerning Toleration' Locke observes that moral actions lie both in the jurisdiction of the "magistrate and conscience" (Locke, 2003 [1823]). However, the limit of the civil government, Locke argues, stops in the domain where "one man does not violate the right of another, by his erroneous opinions...nor is his perdition any prejudice to another man's affairs." (p. 242).

The domain of moral choices concerning one's own happiness, argues Locke, belongs to the domain of things "that every man ought sincerely to enquire into himself, and by meditation, study, search, and his own endeavour, attain the knowledge of" (p. 229). Here Locke locates the foundational right to make one's own moral choices and freely identify with these choices "because no man can so far abandon the care for his own salvation as blindly to leave it to the choice of any other" (p. 219). And accordingly, in the matters concerning moral identity and moral choices regarding one's own well being, civil government has power only to persuade by reason and press with arguments, but not with penalties.

Thus, it can be said that the parallel between Lockean classical liberalism and more recent arguments on the role of identity-formation in the context of informational privacy is more than just an instructive metaphor. In that sense, the moral right to define one's own identity is a counterclaim to the nominalization of one's identity, to its fixation within externally predetermined frame of attributes. But what is even more important is a right to define value of one's own identity, to choose the framework of the normative evaluation of one's own identity in the sense of moral autonomy.

And it would be wrong to interpret this right in the vein of naive atomistic individualism, as a utopian world of fully self-sufficient individuals. Rather, it should be understood as a claim to have a degree of freedom; a free space defined by the right to privacy, but also a space free from the externally imposed judgment on one's own moral choices. As Sen (2007) rightly points out, identity cannot be seen as something completely unencumbered by the life circumstances of an individual. Howev-

er, it is crucial that even in the encumbered position one happens to occupy, choice regarding one's own identity continues to exist. This is then not a claim for the proclamation of individual atomism, but rather a counterclaim to creeping powers of self-proclaimed sovereign entities: a counterclaim against attempts by those entities to legitimize their powers to assign and evaluate humans' identities in the new domains of emerging socio-technical systems. And what is more important this claim re-allocates the moral r*aison d'etre* for identity management systems. Existence of such systems is not derived from an obligation or duty of individuals to be identified, but from a natural right of an individual to be represented via mediating role of an institutions of identity.

5.5. Bridging the gap between 'self-sovereignty' and SSI

The ability to issue one's own digital identity, to choose a list of presented attributes, and even to choose which entities could verify these attributes, does present a significant shift from centralised identity management systems. All those key properties of the SSI system, that can provide the individual bearer of identity with an enhanced degree of freedom for self-presentation. Furthermore, the capacity to share only those identity attributes that are relevant to given interactions shifts the distribution of power between the identity owner and the entities interested in his or her private data. From that perspective, SSI solutions can claim a valid moral argumentation on the desirability of such systems as compared to the centralised identity management systems.

These technical elements in themselves, however, do not guarantee the preservation of morally desirable properties in SSI systems implemented on a scale. As Manders-Huits (2010) points out, the very structure of identity management systems promotes a presupposed, nominal notion of identity, resulting in moral tensions between the system logic and reflexive identification of individual. There is an apprehension then, that such tensions will only sharpen with the further depreciation of moral semantics of 'self-sovereignty'. Carrying risks that not only morally desirable properties of these systems will fail to get traction, but that SSIs might rather bring about new ethical complications.

It is also important to appreciate that despite what is argued, in themselves technical elements of SSI solutions do not present a 'paradigm shift' (Wagner et al. 2016). In their current form, SSI systems do not challenge the general paradigm of socio-technical systems whose cornerstone design principles are identification, trust, and permissions. Essentially any system built around identification requires some form of persistent identity to participate in it or use its resources. And any system that does not require the persistent identity of participants to achieve security effectively does not require identity at all. There is always a risk then, that introducing 'solution for identity' we are implicitly considering the 'problem of identity' as something unquestionable and given. And thus creating new scenarios and types of interactions that require identity from individuals, effectively introduce new problems for the application of existing 'solution'.

One such possibility is a normalisation of new standards for cryptographically verified data in the scenarios where individuals previously were not expected to poses and provide such data at all. This possibility can be illustrated by the proposals suggesting that a cell provider can verify the location of an individual in a deterministic way in the SSI system (Sovrin 2018). It may sound like an eccentric application at a first glance, but once we consider the existing practices of insurance providers installing tracking devices in cars in return for discounts, or court cases using data from 'wearables', this *identification creep* takes on a distinctively dystopian flavor.

This brings about another speculative component of SSI proposals - a promise of a sufficiently decentralised 'web of trust' based on a free-market ecosystem of competing verifiers. Such competition would enable individual users to choose between different providers of such services, thus taking away the power from verifiers to dictated standards of identification. The immediate apprehension here is that even with the permissionless blockchain protocols (with lower barriers for participation), the achievement of a meaningful decentralisation is a notoriously difficult task.[77] From that perspective achievement of decentralisation on a basis of private blockchains as for instance suggested by Sovrin, seem to be even a more far-fetched promise. It is also important to appreciate that the proposed free-market mecha-

[77] Not to mention the issue of highly contestable criteria of a 'sufficient' decentralization.

nisms aimed to achieve promised decentralisation are not completely morally unproblematic in themselves.

This apprehension becomes clear once we consider proposals on the global marketplaces for credentials and 'ethical' markets for customers' data (Acxiom 2018; Sovrin 2018; Wagner et al. 2018). Such proposals essentially run into the fallacy that free market mechanisms can bring about morally desirable outcomes – assumption largely construed on the idealized representation of the rationality of such markets. What these assumptions, however, largely ignore is a risk that such market mechanisms would rather fit into the structures of existing private data markets, replicating and even exaggerating moral risks associated with private data propertization.

True enough, cryptographic solutions such as pairwise identifiers, can present a barrier against adversarial profiling, preventing third parties from the aggregation of profiles on DID owners. Yet, there is no guaranteed technical solution that could prevent uses of a single identity or a limited set of identifiers by individuals in SSI systems themselves. And this is not merely a problem of technical design, or education of users as in the case of, say, reuse of the same wallet address by Bitcoin users (Wagner et al. 2018). Rather, this is a critical issue of establishing a successful moral claim about the desirability of multiple identities, which are not fixed in a single normative framework of evaluation, such as for instance consumer identity.

Thus, the biggest challenge to the facilitation of 'self-sovereignty' in SSI systems in the strong sense, is a debunking of claims about the absolute moral desirability of a singular identity, as warned against by Sen (2007). Otherwise, the very same infrastructure enabling SSIs can facilitate aggregation of profiles and scores, if most users are rather encouraged to use the same DIDs through the variety of contexts, or just to use limited sets of DIDs. Here interoperability and standardization can play a negative role, facilitating the emergence of standardized reputation systems, where the normative framework of identity evaluation will not be determined by the individuals themselves.

This chapter has provided an outline for the moral grounding of claims on the desirability of SSI solutions. Yet, somewhat paradoxically, this very set of moral arguments provides a basis for the sceptical arguments on the 'identity problem' motiva-

tion behind these implementations. Far too often it is implicitly assumed that the absence of identity is a problem in the need of a solution, while in fact, the very framing of this question is the problem in itself, revealing much deeper moral issue of a persistent identification creep. And consequently evaluation of the desirability of identification becomes interpreted in the instrumentalist vein - defined by the parameters of a systems' efficiency rather than actual needs of individuals interacting with it. Together, all these concerns about the possibility of further identification creep, private data propertization, and the emergence of new reputation systems, highlight that attempts to dissociate technical meaning of 'self-sovereignty' from its normative contents do not take away moral-philosophical complications. Rather such separation obfuscates and disguises economic (and other) interests of entities expecting to benefit from the advantageous positions in the new ecosystems enabled by SSI.

And as taxing as it may be to try and bridge this gap between the broad range of moral concerns and actual technical implementations, this task is not optional as this chapter demonstrates. It is not enough to merely claim moral motivation for the development of SSI systems derived from the right of an individual to be represented via the mediating role of socio-technical solutions in the Lockean vein of thinking. We should also keep in mind that with the growing dependence of individuals on technical infrastructures, even systems with the completely optional participation quickly become de-facto necessities with the wider adoption and network effects. And any proposed 'identity solution' scenario should always be contrasted to the possibility of an alternative solution that does not require any identity at all.

Thus, further tasks for ethicists and developers working in the field of SSI systems include not just resolution of such issues as moral desirability of multiple identities contrasted with the moralised singular identity. More importantly there is a task for the development of a moral-theoretical framework capable of providing sceptical scrutiny on the moral desirability of the very identification itself. Only doing so we can ensure that SSI systems contribute to the realisation of a 'self-sovereignty' ideals rather than to the emergence of a Hobbsean 'Techno-leviathan'.

Summary

The moral significance of blockchain technologies is a highly debated and polarised topic, ranging from accusations that cryptocurrencies are tools serving only nefarious purposes such as cybercrime and money laundering, to the assessment of blockchain technology as an enabler for revolutionary positive social transformations of all kinds. Such technological determinism, however, hardly provides insights of sufficient depth on the moral significance of blockchain technology. This thesis argues rather, that very much like the cryptographic tools before them, blockchains develop in a constant feedback loop. Blockchain applications are driven by values, normative assumptions, and personal commitments of researchers, which shape moral effects of technology. At the same time these very assumption are often embedded in preexisting moral conception and ethical theories, implicitly or explicitly accepted by blockchain developers. And just as the introduction of one flawed element in the cryptographic application can have mass scale effects, the introduction of flawed normative assumptions can have far reaching consequences in blockchain applications.

Particular significance in that respect present promises to deliver decentralised architectures capable of preserving and promoting such fundamental moral values as privacy, data protection and individual autonomy. This thesis argues that we should not take normative assumptions present in blockchain applications as given. Just like the open-source code is developed through the public revision and scrutiny, we should aim to make normative assumptions transparent and be ready to revise them in case we find some bugs. How can we qualify claims that blockchain technologies enable new types of institutions? Can blockchain technologies eliminate trust in complex socio-technical systems? What does individual sovereignty mean in the context of private data control and privacy? Whether property in private data enabled by blockchain applications can solve moral issues of privacy and commercial surveillance? Answers to these and other questions map some of the key normative assumptions present in the current blockchain projects, and serve as a contribution to the open-source project of the future society.

The first chapter, 'Blockchain technology as an institution of property,' looks into the main theoretical hypothesis and argues, using Bitcoin as an example, that blockchain technology implementation can, indeed, provide alternatives to some existing social institutions such as property. From that perspective, blockchain technology applications do have the potential to replace key elements in the digital infrastructures on an unprecedented scale. However, such observation on the capacity of blockchain technology in itself does not provide normative arguments *per se* about whether we should replace other existing institutions and infrastructures with such solutions. Furthermore, this novel capacity of blockchain protocols to enable cooperation and coordination between entities in a socio-technical systems on a large scale understandably provokes a question whether similar solutions could and should be employed in contexts different from cryptocurrencies. Consumer Internet of Things systems present particular interest in that respect for several reasons.

Indeed, propagation of ubiquitous sensors in IoT implementations present one of the most serious threats to privacy and data protection, arguably more dangerous and problematic than the erosion of financial privacy, which means that any solutions capable of mitigating these issues should be given a try. Chapter two 'Rethinking trust in the Internet of Things' elaborates on the philosophical conception of trust in private data protection. It argues that current developments in digital infrastructures, defined by the propagation IoT, exploits users' trust in the providers of technology, trend deeply intertwined with the reductionist conceptualisations of trust. Centralized architectures based on the client-server model simply cannot justify trust in the guarantees of data privacy offered by the data-collectors in such infrastructures.

These findings strongly support at least one normative assumption present in current blockchain applications – namely, prima facie distrust as a key design component of infrastructures, capable of providing real data protection guarantees. Blockchain solutions embedding this principle can take away the need for individual users to rely on trust. It is also argued that we should be careful not to assume that Blockchain itself is a 'trustless' technology. Allowing for trustless interactions between peers in certain contexts, it does not eliminate completely the necessity to trust in the developers and the technology itself.

There is, however, also a second issue stemming from the observation that IoT blockchain implementations seem to be deeply intertwined with the normative assumptions on privacy as a property in private data. Chapter three 'Blockchain enabled commodification of private data' looks closer into blockchain solutions that promise to enhance privacy of consumers using IoT. It is argued that current proposals in this area are inseparable from the ideas of 'private data markets', and stem from the normative assumptions that private data propertization can enhance individual privacy.

In line with the arguments from technological determinism, it treats propertization of private data as an inevitable process and focuses on the development of techno-economic solutions that would help to make private data markets more fair and transparent. However, as this study shows, there is a significant risk that in the long term, such approach could lead to an effect opposite of what was intended. Furthermore privacy conceptualised as a property in private data fails to address wider range of ethical concerns regarding privacy and its value. And given these apprehensions, it becomes crucial that we take a cautiously critical stance towards normative assumptions on privacy embedded in other blockchain based solutions.

These observations warrant a closer scrutiny of one of the most ambitious implementations of blockchain implementations aimed to provide individuals with enhanced privacy in the various contexts of interactions mediated by socio-technical systems - Self-Sovereign Identity (SSI) solutions. Chapter four 'Sovereignty, privacy, and ethics in blockchain based identity management systems' explores SSI solutions implemented on the basis of blockchain technology, which are seen as alternatives to existing digital identification systems, or even as a foundation of standards for the new global infrastructures for identity management systems.

This chapter aims to highlight a broader range of ethical issues surrounding the changing nature of human identity in the context of ubiquitous private data collection, in order to qualify promises and challenges of SSI systems. It is argued that in their current implementations these solutions operationalize the concept of 'self-sovereignty' in a narrow technical sense, rather removed from the wider set of moral issues inherent to this concept. This chapter argues against the suggestions that

such depreciation of moral semantics can facilitate wider adoption of SSI solutions. On the opposite to ensure moral desirability of these implementations it is necessary to bridge the gap between normative and technical meanings of 'self-sovereignty'. Furthermore, this connection provides a valid moral grounding for the arguments on the desirability of SSI solutions over centralized identity management systems, where ethical issues are glossed over and disguised under the cover of moralized legitimizing claims.

Samenvatting

Anno 2019, is het morele belang van blockchain technologie een veelbesproken onderwerp waarover de meningen sterk gepolariseerd zijn, variërend van in hoeverre cryptocurrencies enkel bijdragen aan criminele activiteiten zoals cybercrime of witwaspraktijken tot in hoeverre blockchain technologie gezien kan worden als een mondiale revolutionaire sociale transformatie. Omdat de ontwikkeling van een technologie niet verbonden is aan het kader van de discussie, biedt het naïef technologisch determinisme dus nauwelijks inzichten van voldoende diepgang over de morele betekenis van blockchain technologie. Dit proefschrift stelt dat net zoals voorgaande cryptografische tools, blockchain technologie zich ook ontwikkeld door middel van een constante feedback-loop.

Blockchain applicaties worden gestuurd door waarden, normatieve veronderstellingen en de persoonlijke inzet van onderzoekers, die de morele effecten van technologie bepalen. Tegelijkertijd zijn deze veronderstellingen vaak al ingebed in bestaande morele opvattingen en ethische theorieën, impliciet of expliciet geaccepteerd door blockchain ontwikkelaars. En net zoals de introductie van een gebrekkig element in een cryptografische applicatie massale gevolgen kan hebben, kan de introductie van gebrekkige normatieve veronderstellingen verstrekkende gevolgen hebben in blockchain applicaties.

Een bijzonder belang in dat opzicht is de belofte om gedecentraliseerde software architecturen te leveren die in staat zijn om fundamentele morele waarden zoals privacy, gegevensbescherming en individuele autonomie te behouden en promoten. Dit proefschrift stelt dat we de normatieve veronderstellingen die door blockchain applicaties worden gesuggereerd niet als een gegeven moeten worden gezien. Net zoals open-source code wordt ontwikkeld door middel van openbare revisie en controle, moeten we ernaar streven om normatieve veronderstelling transparant te maken en voorbereid te zijn om ze te herzien in het geval er fouten worden ontdekt.

Hoe kunnen we de claims kwalificeren waarin wordt gesteld dat blockchain technologie nieuwe type instituten mogelijk maakt? Kan blockchain-technologie het vereiste van vertrouwen in complexe socio-technische systemen elimineren? Wat betekent individuele soevereiniteit in de context van persoonlijke gegevensbeheers-

ing en privacy? Kan eigendom van persoonlijke data, mogelijk gemaakt door blockchain applicaties, de morele kwesties tussen privacy en commercieel toezicht oplossen? Antwoorden op deze en soortgelijke vragen brengen een aantal van de belangrijkste normatieve veronderstellingen in de huidige blockchain projecten in kaart en dragen daarmee bij aan het algemene open-source project van de toekomstige samenleving.

Het eerste hoofdstuk: "Blockchain technologie als eigendomsinstituut", geeft het beeld van de belangrijkste theoretische hypothese en beargumenteert, met als voorbeeld Bitcoin, dat de implementatie van blockchain technologie inderdaad alternatieven kan bieden voor sommige bestaande sociale instituten, zoals eigendom. Vanuit dat perspectief bezit blockchain technologie het potentieel om belangrijke elementen in digitale infrastructuren op ongekende schaal te vervangen. Een dergelijke observatie van de capaciteit van de blockchain technologie op zichzelf levert echter niet per se normatieve argumenten voor het beantwoorden van de vraag of we bestaande instellingen en infrastructuren met dergelijke applicaties zouden moeten vervangen. Bovendien biedt het potentieel van blockchain protocollen grootschalige samenwerking en coördinatie tussen entiteiten in socio-technische systemen, waardoor begrijpelijk de vraag wordt gesteld of soortgelijke oplossingen kunnen en zouden moeten worden gebruikt in contexten die verschillen van cryptocurrencies. Een goed voorbeeld van een soortgelijke oplossing bestaat uit consument gerichte "Internet of Things" (IoT) systemen, welke om verschillende redenen al bijzondere belangstelling vertonen in blockchain technologie.

De verspreiding van alomtegenwoordige sensoren in IoT-implementaties vormt inderdaad een van de meest ernstigste bedreigingen voor privacy en gegevensbescherming, aantoonbaar gevaarlijker en problematischer dan de uitholling van financiële privacy, waardoor oplossingen die deze problemen kunnen beperken daarom zeker een kans moeten krijgen. Het tweede hoofdstuk: "Heroverweging van vertrouwen in het Internet of Things", gaat nader in op de filosofische opvatting van vertrouwen in private gegevensbescherming. Het betoogt dat de huidige ontwikkelingen in digitale infrastructuren, gedefinieerd door de verspreiding van het IoT, gebruikmakend van het vertrouwen van gebruikers in de leveranciers van technologie, een trend is die diep verweven is met de reductionistische conceptualisaties van vertrouwen. Gecentraliseerde architecturen op basis van het "client-server model" kunnen eenvoudigweg niet het vertrouwen rechtvaardigen in de garanties van data

privacy, zoals aangeboden door de gegevensverzamelaars in dergelijke infrastructuren. Deze bevindingen ondersteunen ten minste één normatieve veronderstelling die aanwezig is in de huidige blockchain applicaties: namelijk het prima facie wantrouwen als een essentieel ontwerpcomponent van infrastructuren, die in staat is om echte gegevensbeschermingsgaranties te bieden. Blockchain applicaties die op dit principe voortbouwen, kunnen de noodzaak wegnemen dat individuele gebruikers zich hoeven te berusten op vertrouwen. Er wordt ook beargumenteerd dat men voorzichtig moet zijn met de aanname dat blockchain technologie op zichzelf een "betrouwbare" technologie is. Ondanks de betrouwbare interacties tussen de schakels in bepaalde contexten, is de gebruiker nog steeds genoodzaakt om te vertrouwen in de ontwikkelaars en de technologie zelf.

Er is echter ook een tweede kwestie die voortkomt uit de observatie dat IoT blockchain implementaties diep verweven lijken te zijn met de normatieve veronderstellingen over privacy als een eigenschap in persoonlijke data. In het derde hoofdstuk: "Blockchain realiseert commodificatie van persoonlijke data" wordt nader ingegaan op blockchain oplossingen die beloven de privacy te verbeteren van consumenten die gebruik maken van het IoT. Er wordt beweerd dat de huidige voorstellen op dit gebied niet los kunnen worden gezien van het concept "persoonlijke data markten" en dat dit voortkomt uit de normatieve veronderstellingen dat propriëtaire persoonlijke data de individuele privacy kan verbeteren.

In overeenstemming met de argumenten van het technologisch determinisme, wordt de opkomst van propriëtaire persoonlijke data als een onvermijdelijk proces gezien en ligt de focus op de ontwikkeling van techno-economische oplossingen die kunnen helpen persoonlijke data markten eerlijker en transparanter te maken. Zoals uit deze studie blijkt, bestaat er echter een aanzienlijk risico dat een dergelijke aanpak op lange termijn kan leiden tot een tegengesteld effect. Bovendien kan privacy, geconceptualiseerd als een eigenschap van persoonlijke data, niet ingaan op een breder scala aan ethische kwesties met betrekking tot privacy en de waarde ervan. Gezien het bestaan van deze kans, is het cruciaal dat we een kritische houding aannemen ten opzichte van normatieve veronderstellingen, bijvoorbeeld ten aanzien van privacy, en hoe deze zijn verankerd in andere op blockchain gebaseerde applicaties.

Deze observaties rechtvaardigen een nauwkeuriger onderzoek naar één van de meest ambitieuze implementaties van blockchain-implementaties, die erop gericht is individuen meer privacy te bieden in de verschillende contexten van interacties gemedieerd door socio-technische systemen: Self Sovereign Identity (SSI) oplossingen. Hoofdstuk vier: 'Soevereiniteit, privacy en ethiek in blockchain gebaseerde identiteitsbeheer systemen' verkent SSI oplossingen die geïmplementeerd zijn op basis van blockchain technologie. Deze systemen worden gezien als alternatieven voor bestaande digitale identificatiesystemen, of zelfs als een basis van normen voor de nieuwe globale infrastructuur voor identiteitsbeheer systemen. Dit hoofdstuk heeft als doel een breder scala van ethische kwesties te belichten, die de veranderende aard van menselijke identiteit in de context van alomtegenwoordige persoonlijke data verzamelingen benadrukken, om zodoende de beloften en uitdagingen van SSI systemen te kwalificeren.

Er wordt in een beperkte technische zin beweerd dat deze oplossingen in hun huidige implementaties het concept van “zelf-soevereiniteit” operationaliseren, losstaand van de bredere reeks van morele kwesties die inherent zijn aan dit concept. Dit hoofdstuk pleit tegen de suggesties dat een dergelijke depreciatie van morele semantiek een bredere acceptatie van SSI oplossingen kan vergemakkelijken. Om de morele wenselijkheid van deze implementaties te waarborgen, moet juist het verschil tussen normatieve en technische betekenissen van “zelf-soevereiniteit” worden overbrugd. Bovendien biedt deze connectie een geldige morele basis voor de argumenten over de wenselijkheid van SSI oplossingen ten opzichte van gecentraliseerde identiteitsbeheersystemen, waar ethische kwesties worden verdoezeld en verborgen onder de dekmantel van gemoraliseerde legitimerende claims.

References

Abelson, H., Anderson, R. J., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... Schiller, J. I. (1997). The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal*, *2*(3), 241–257.

Acar, G., Englehardt, S., & Narayanan, A. (2018, April 9). Four cents to deanonymize: Companies reverse hashed email addresses. Retrieved June 10, 2018, from Freedom to Tinker website: https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *52*(2). Retrieved from https://ssrn.com/abstract=2580411

Acxiom Research. (2017, November). *Blockchain in Ad Tech*. Retrieved from https://www.acxiom.com/wp-content/uploads/2017/12/AC-1752-17-3-Point-of-View-Blockchain-in-Ad-Tech.pdf

Adams, T. (2018, March 24). Facebook's week of shame: the Cambridge Analytica fallout. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/mar/24/facebook-week-of-shame-data-breach-observer-revelations-zuckerberg-silence

Adjerid, I., Peer, E., & Acquisti, A. (2018). Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly*, *42*(2), 465–488. https://doi.org/10.25300/MISQ/2018/14316

Agarwal, R., & Krogstrup, S. (2019, February 5). Cashing In: How to Make Negative Interest Rates Work. Retrieved from IMF Blog website: https://blogs.imf.org/2019/02/05/cashing-in-how-to-make-negative-interest-rates-work/

Aggarwal, C. C., Ashish, N., & Sheth, A. (2013). The internet of things: A survey from the data-centric perspective. In *Managing and mining sensor data* (pp. 383–428). Springer.

AIOTI (Alliance for Internet of Things Innovation). (2016, November). *AIOTI Digitisation of Industry Policy Recommendations*. Retrieved from https://aioti.eu/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf

Allen, C. (2017). *The Path to Self-Sovereign Identity*. Retrieved from https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelfSovereignIdentity.md

Allen, C., Brock, A., Buterin, V., Callas, J., & Dorje, D. (n.d.). *Decentralized Public Key Infrastructure. A White Paper from Rebooting the Web of Trust*. Retrieved from https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust/blob/master/final-documents/dpki.pdf

Åm, T. G. (2011). Trust in Nanotechnology? On Trust as Analytical Tool in Social Research on Emerging Technologies. *NanoEthics, 5*(1), 15–28.

Anderson, R. (2004). Cryptography and Competition Policy - Issues with 'Trusted Computing.' In L. J. Camp & S. Lewis (Eds.), *Economics of Information Security* (pp. 35–52). https://doi.org/10.1007/1-4020-8090-5_3

Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication, 8*, 17.

Apthorpe, N., Huang, D. Y., Acar, G., Li, F., Narayanan, A., & Feamster, N. (2018, April 23). Announcing IoT Inspector: Studying Smart Home IoT Device Behavior. Retrieved April 25, 2018, from Freedom to Tinker website: https://freedom-to-tinker.com/2018/04/23/announcing-iot-inspector-a-tool-to-study-smart-home-iot-device-behavior/

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. *CoRR, abs/1705.06805*. Retrieved from http://arxiv.org/abs/1705.06805

Aristotle. (1982). *The Politics of Aristotle* (E. Barker, Trans.). London: Oxford Univ. Pr.

Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web, 5*(2), 58–71.

Atzori, M. (n.d.). Blockchain-Based Architectures for the Internet of Things: A Survey (2016). *Available at SSRN 2846810*.

Baier, A. (1986). Trust and antitrust. *Ethics, 96*(2), 231–260.

Baranger, H. (2010). The apparition of sovereignty. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments. The Past, Present and Future of a Contested Concept* (pp. 47–63). Cambridge; UK: Cambridge University Press.

Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 44–75). https://doi.org/10.1017/CBO9781107590205

Bass, T. (1995, Winter). Whitfield Diffie: a private conversation with the headman of the cypherpunk revolution - semi - inventor of public key encryption. *Omni, 17*(9). Retrieved from http://nest.machinecode.org/intricate/omni_magazine/Omni%20v17%20%239%20Winter%201995.html

Bay, M. (2017). The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone. *First Monday, 22*(2). https://doi.org/10.5210/fm.v22i2.7006

Beck, R., Czepluch, J. S., Lollike, N., & Malone, S. (2016). *Blockchain-the Gateway to Trust-Free Cryptographic Transactions*. Presented at the European Conference on Information Systems ECIS. Retrieved from http://elibrary.aisnet.org/Default.aspx?url=http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1145&context=ecis2016_rp

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. *CoRR, abs/1407.3561*. Retrieved from http://arxiv.org/abs/1407.3561

Bergen, M., & Surane, J. (2018, August 31). Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales

Bocek, V., & Chrysaidos, N. (2018, May 24). Android devices ship with pre-installed malware. Retrieved May 25, 2018, from Avast Blog website: https://blog.avast.com/android-devices-ship-with-pre-installed-malware

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science, 4*(3), 340–347.

Brey, P. (2007). Ethical aspects of information security and privacy. In *Security, privacy, and trust in modern data management* (pp. 21–36). Springer.

Brito, J. (2018, April 5). What does the EU's General Data Protection Regulation mean for open blockchain networks? Retrieved April 20, 2018, from Coincenter.org website: https://coincenter.org/link/what-does-the-eu-s-general-data-protection-regulation-mean-for-open-blockchain-networks

Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM, September*.

Brudner, A. (2013). Private Property and Public Welfare. *Philosophical Foundations of Property Law, Edited by James Penner and Henry Smith*, 68–98.

Bruynseels, K., & van den Hoven, J. (2015). How to do things with personal big biodata. In D. Mokrosinska & B. Rössler (Eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (p. 122). Cambridge: Cambridge University Press.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *Ethereum Whitepaper*. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper

Buterin, V. (2017, April 27). *Visions, Part 2: The Problem of Trust*. Retrieved from https://blog.ethereum.org/2015/04/27/visions-part-2-the-problem-of-trust/

Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). *Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities*. 5–13. https://doi.org/10.1109/HPCC.2008.172

Campbell, R. (2016, October 8). *IRS at a Standstill with Bitcoin; Users and Tax Professionals Remain in the Dark*. Retrieved from https://www.cryptocoinsnews.com/irs-standstill-bitcoin-users-tax-professionals-remain-dark/

Canon, G. (2018, October 23). "City of surveillance": privacy expert quits Toronto's smart-city project. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/oct/23/toronto-smart-city-surveillance-ann-cavoukian-resigns-privacy

CFTC. (2016, June 2). *Docket No. 16–19. "Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, as Amended, Making Findings and Imposing Remedial Sanctions."* Retrieved from http://www.cftc.gov/idc/groups/public/@lrenforcementactions/ documents/legalpleading/enfbfxnaorder060216.pdf

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28*(10), 1030–1044.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Christin, A., Rosenblat, A., & Boyd, D. (2015). Courts and predictive algorithms. *Data & CivilRight*. Retrieved from http://www.law.nyu.edu/sites/default/files/upload_documents/Angele%20Christin.pdf

Christin, D. (2016). Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software, 116*, 57–68. https://doi.org/10.1016/j.jss.2015.03.067

Christl, W., Kopp, K., & Riechert, P. U. (2017). *Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions.* Retrieved from Cracked Labs website: http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Christl, W., & Spiekermann, S. (2016). *Networks of control: a report on corporate surveillance, digital tracking, big data & privacy*. Wien: Facultas.

Chung, F. (2017, July 4). Cash crackdown boss floats nano-chips in notes. *News.Com.Au*. Retrieved from http://www.news.com.au/finance/economy/australian-economy/cash-crackdown-boss-floats-nanochips-in-notes/news-story/05db2212948c7d02e822532de63c170d

Colavita, M., & Tanzer, G. (2018). *A Cryptanalysis of IOTA's Curl Hash Function*. Retrieved from https://www.boazbarak.org/cs127/Projects/iota.pdf

Conway, S., Hughes, A., Ma, M., Poole, J., Riedel, M., Smith, S. M., & Stocker, C. (2019). *A DID for Everything Attribution, Verifcation and Provenance for Entities and Data Items a white paper from Rebooting the Web of Trust VII*. Retrieved from https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/final-documents/A_DID_for_everything.pdf

Cramer, R., Damgard, I. B., & Nielsen, J. B. (2015). *Secure Multiparty Computation and Secret Sharing*. https://doi.org/10.1017/CBO9781107337756

Dam, K. W., & National Research Council (Eds.). (1996). *Cryptography's role in securing the information society*. Washington, DC: National Acad. Press.

Davies, S., Kearnes, M. B., & Macnaghten, M. (2010). *Nanotechnology and public engagement: a new kind of (social) science?* Pan Stanford.

De Filippi, P. (2014). Bitcoin: A Regulatory Nightmare to a Libertarian Dream. *Internet Policy Review*, *3*(2), May 14, 2014.

De Filippi, P. D., & Hassan, S. (2018). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *CoRR*, *abs/1801.02507*. Retrieved from http://arxiv.org/abs/1801.02507

De Fuentes, J. M., González-Manzano, L., González-Tablas, A. I., & Blasco, J. (2014). Security models in vehicular ad-hoc networks: A survey. *IETE Technical Review*, *31*(1), 47–64.

De Hert, P., Papakonstantinou, V., Rodrigues, R., Barnard-Wills, D., Wright, D., Remoti, L., ... Institute for the Protection and the Security of the Citizen. (2014). *EU privacy seals project: challenges and possible scope of an EU privacy seal scheme: final report study deliverable 3.4*. (L. Beslay & N. Dubois, Eds.). Retrieved from http://dx.publications.europa.eu/10.2788/85717

Denning, D. E. (1993). To tap or not to tap. *Communications of the ACM*, *36*(3), 24–33. https://doi.org/10.1145/153520.153523

Dierksmeier, C. (2018). Just HODL? On the Moral Claims of Bitcoin and Ripple Users. *Humanistic Management Journal*, *3*(1), 127–131. https://doi.org/10.1007/s41463-018-0036-z

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and Business Ethics. *Journal of Business Ethics*, *152*(1), 1–14. https://doi.org/10.1007/s10551-016-3298-0

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Diffie, W., & Landau, S. E. (2007). *Privacy on the line: the politics of wiretapping and encryption* (Updated and expanded ed). Cambridge, Mass: MIT Press.

Dittus, M. (2017, September 12). Exploring the Darknet in Five Easy Questions. Retrieved from Oxford Internet Institute Blog website: https://www.oii.ox.ac.uk/blog/exploring-the-darknet-in-five-easy-questions/

Dixon, P. (2017). A Failure to "Do No Harm" -- India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health and Technology*, *7*(4), 539–567. https://doi.org/10.1007/s12553-017-0202-6

Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *ArXiv Preprint ArXiv:1608.05187*.

Durante, M. (2017). The Ontological Interpretation of Informational Privacy. In M. Durante, *Ethics, Law and the Politics of Information* (Vol. 18, pp. 117–140). https://doi.org/10.1007/978-94-024-1150-8_7

EC (European Comission). (2016, April 19). *Comission Staff Working Document. Advancing the Internet of Things in Europe*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

Engelmann, S., Chen, M., Fischer, F., Kao, C., & Grossklags, J. (2019). Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines "Good" and "Bad" Behavior. *Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT* '19*, 69–78. https://doi.org/10.1145/3287560.3287585

Enigma. (2017, July 31). Beyond Catalyst: Enigma's Vision for the Future of Data. Retrieved September 15, 2017, from Enigma Project blog website: https://blog.enigma.co/beyond-catalyst-enigmas-vision-for-the-future-of-data-22fbb5845556?gi=e67e2743f1cd

EP (European Parliament and of the Council). (2016, April). *REGULATION (EU) 2016/679. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved from http://eur-lex.europa.eu/eli/reg/2016/679/oj

EPIC. (2015, February 24). *Complaint, Request for Investigation, Injunction, and Other Relief Submitted by The Electronic Privacy Information Center*. Retrieved from https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf

Evershed, N. (2017, July 14). Australia's plan to force tech giants to give up encrypted messages may not add up. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up

Fairfield, J. A. (2015). Bitproperty. *California Law Review, 88*(5).

Fanti, G. C., Venkatakrishnan, S. B., Bakshi, S., Denby, B., Bhargava, S., Miller, A., & Viswanath, P. (2018). Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. *CoRR, abs/1805.11060*. Retrieved from http://arxiv.org/abs/1805.11060

Fernandes, E., Jung, J., & Prakash, A. (2016). *Security analysis of emerging smart home applications*. 636–654. IEEE.

Finck, M. (2017). Blockchains and Data Protection in the European Union. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3080322

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information Technology, 8*(3), 109–119. https://doi.org/10.1007/s10676-006-9121-3

Friedman, D. (1996). A World of strong privacy: promises and perils of encryption. *Social Philosophy and Policy, 13*(2), 212–228.

Fussell, S. (2018, November 17). The Next Data Mine Is Your Bedroom. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/11/google-patent-bedroom-privacy-smart-home/576022/

Gambetta, D. (1988). Can we trust trust. In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). Oxford: Basil Blackwell Ltd.

Gasser, U., Gertner, N., Goldsmith, J. L., Landau, S., Nye, J. S., O'Brien, D., ... Schneider, B. (2016). Don't Panic: Making Progress on the" Going Dark" Debate. *The Berkman Center for Internet & Society Study at Harvard University*. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Glorioso, A., Pagallo, U., & Ruffo, G. (2010). The Social Impact of P2P Systems. In X. Shen, H. Yu, J. Buford, & M. Akon (Eds.), *Handbook of Peer-to-Peer Networking* (pp. 47–70). https://doi.org/10.1007/978-0-387-09751-0_2

Govier, T. (1997). *Social trust and human communities*. McGill-Queen's Press-MQUP.

Green, M. (2016, June 15). What is Diffirential Privacy? Retrieved from A Few Thoughts on Cryptographic Engineering website: https://blog.cryptographyengineering.com/2016/06/15/what-is-differential-privacy/

Green, M. (2018, December 17). On Ghost Users and Messaging Bckdoors. Retrieved from A Few Thoughts on Cryptographic Engineering website: https://blog.cryptographyengineering.com/2018/12/17/on-ghost-users-and-messaging-backdoors/

Grennspan, G. (2016, June 12). Smart Contracts and the DAO Implosion. Retrieved from Multichain Blog website: http://www.multichain.com/blog/2016/06/smart-contracts-the-dao-implosion/

Greveler, U., Justus, B., & Loehr, D. (2012). Multimedia content identification through smart meter power usage profiles. *Computers, Privacy and Data Protection, 1*, 10.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.

Ha, A. (2016, March 14). Blockai Uses the Blockchain to Help Artists Protect Their Intellectual Property. Retrieved from Techcrunch website: https://techcrunch.com/2016/03/14/blockai-launch/

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*(2), 99–111. https://doi.org/10.1007/BF00196791

Hardin, R. (2002). *Trust and trustworthiness*. Russell Sage Foundation.

Harwell, D. (2018, November 23). Wanted: The 'perfect babysitter.' Must pass AI scan for respect and attitude. *Washington Post*. Retrieved from https://

www.washingtonpost.com/gdpr-consent/?destination=%2ftechnology%2f2018%2f11%2f16%2fwanted-perfect-babysitter-must-pass-ai-scan-respect-attitude%2f%3f&utm_term=.0b13f88d45a1

Hawley, K. (2014). Trust, Distrust and Commitment: Trust, Distrust and Commitment. *Noûs*, *48*(1), 1–20. https://doi.org/10.1111/nous.12000

Haynes, J., Ramirez, M., Hayajneh, T., & Bhuiyan, Md. Z. A. (2017). A Framework for Preventing the Exploitation of IoT Smart Toys for Reconnaissance and Exfiltration. In G. Wang, M. Atiquzzaman, Z. Yan, & K.-K. R. Choo (Eds.), *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (pp. 581–592). Springer International Publishing.

Hegel, G. W. F., & Inwood, M. J. (2007). *Hegel's philosophy of mind*. Oxford: New York: Clarendon Press; Oxford University Press.

Hegel, G. W. F., Wood, A. W., & Nisbet, H. B. (2011). *Elements of the philosophy of right* (15. print). Cambridge: Cambridge Univ. Press.

Hellman, M., Merkle, R., Schroeppel, R., Washington, L., Diffie, W., & Pohlig, S. (1976). *Results of an initial attempt to cryptanalyze the nbs data encryption standard*. Retrieved from https://ee.stanford.edu/~hellman/resources/1976_sel_des_report.pdf

Hendrickson, J. R., Hogan, T. L., & Luther, W. J. (2016). The Political Economy of Bitcoin. *Economic Inquiry*, *54*(2), 925–939. https://doi.org/10.1111/ecin.12291

Hertig, A. (2016, July 18). Ethereum's Two Chains. *Coindesk*. Retrieved from www.coindesk.com/ethereum-classic-explained-blockchain/

High, D. R., Wilkinson, B. W., Mattingly, T., Cantrell, R., O'brien, V., John, J., … Jurich Jr, J. (2018). *US Patetnt & Trademark Office Patent No. 20180167200*. Retrieved from http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=%220180167200%22.PGNR.&OS=DN/20180167200&RS=DN/20180167200

Hoffstein, J., Pipher, J., & Silverman. (2008). *An Introduction to Mathematical Cryptography*. https://doi.org/10.1007/978-0-387-77993-5

Hohfeld, W. N. (1917). Fundamental Legal Conceptions as Applied in Judicial Reasoning. *The Yale Law Journal*, *26*(8), 710. https://doi.org/10.2307/786270

Höller, J. (Ed.). (2014). *From machine-to-machine to the Internet of things: introduction to a new age of intelligence*. Amsterdam: Elsevier Academic Press.

Hon, W. K., Millard, C., Singh, J., Walden, I., & Crowcroft, J. (2016). Policy, legal and regulatory implications of a Europe-only cloud. *International Journal of Law and Information Technology*, *24*(3), 251–278.

Honoré, A. M. (1961). Ownership. In A. G. Guest (Ed.), *Oxford essays in jurisprudence* (Vol. 107, pp. 107–128). Oxford: Claredon Press.

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest L. Rev.*, *49*, 261.

Hoofnagle, C. J., Urban, J. M., & Li, S. (2012). Mobile Payments: Consumer Benefits & New Privacy Concerns. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2045580

Hughes, T. C. (2001). A Cypherpunk's Manifesto. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 65–83). Cambridge, Mass: MIT Press.

Hume, D. (1987). *Essays, Moral, Political, and Literary.* (E. F. Miller, Ed.). Retrieved from http://www.econlib.org/library/LFBooks/Hume/hmMPL6.html

IERC (European Research Cluster on the Internet of Things). (2015, January). *Internet of Things IoT governance,privacy and security issues.* Retrieved from http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf

Jones, R. (2017, July 24). Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder. *Gizmodo*. Retrieved from https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829

Kalmo, H. (2010). A matter of fact? The many faces of sovereignty. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments. The Past, Present and Future of a Contested Concept* (pp. 114–131). Cambridge; UK: Cambridge University Press.

Kalmo, H., & Skinner, Q. (2010). Introduction: a concept in fragments. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments. The Past, Present and Future of a Contested Concept* (pp. 1–25). Cambridge; UK: Cambridge University Press.

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Journal of Social Theory*, *15*(1), 23–36. https://doi.org/10.1080/1600910X.2013.870083

Karp, P. (2018, December 7). Australia's war on encryption: the sweeping new powers rushed into law. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law

Kharif, O. (2014, December 14). Bitcoins Seized from Silk Road Offered in Second Auction. *Bloomberg*. Retrieved from https://www.bloomberg.com/ news/articles/2014-12-04/bitcoins-seized-from-silk-road-offered-in-second-auction

Kim, K. J. (2016). Interacting Socially with the Internet of Things (IoT): Effects of Source Attribution and Specialization in Human–IoT Interaction. *Journal of Computer-Mediated Communication*, *21*(6), 420–435.

Kirkpatrick, D. (2011). *The Facebook effect: the inside story of the company that is connecting the world* (1st Simon & Schuster trade pbk. ed). New York: Simon & Schuster Paperbacks.

Koblitz, N., & Menezes, A. J. (2016). Cryptocash, cryptocurrencies, and cryptocontracts. *Designs, Codes and Cryptography, 78*(1), 87–102. https://doi.org/10.1007/s10623-015-0148-5

Koskenniemi, M. (2010). Conclusion: vocabularies of sovereignty – powers of a paradox. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments. The Past, Present and Future of a Contested Concept* (pp. 222–242). Cambridge; UK: Cambridge University Press.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. (2017). *The (unfulfilled) potential of data marketplaces*. Retrieved from The Research Institute of the Finnish Economy website: https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-53.pdf

Kruithof, K., Aldridge, J., Hétu, D., Sim, M., Dujso, E., & Hoorens, S. (2016). *The role of the "dark web" in the trade of illicit drugs*. https://doi.org/10.7249/RB9925

Laudon, K. C. (1996). Markets and privacy. *Communications of the ACM, 39*(9), 92–104. https://doi.org/10.1145/234215.234476

Lauzon, E. (1998). The Philip Zimmerman Investigation: The Start of the Fall of Export Restrictions on Encryption Software Under First Amendment Free Speech Issues. *Syracuse Law Review, 48*, 1307.

Lecher, C. (2019, February 1). Automated background checks are deciding who's fit for a home. *The Verge*. Retrieved from https://www.theverge.com/2019/2/1/18205174/automation-background-check-criminal-records-corelogic

Leenes, R., van Brakel, R., Gutwirth, S., & Hert, P. de (Eds.). (2018). *Data protection and privacy: data protection and privacy*. Oxford; Portland, Oregon: Hart Publishing.

Lessig, L. (2002). Privacy as Property. *Social Research, 69*(1), 247–269.

Lessig, L. (2006). *Code* (Version 2.0). New York: Basic Books.

Levine, B. (2018, June 1). Nebula Genomics readies a marketplace to sell a precious dataset: You. *Martech Today*. Retrieved from https://martechtoday.com/nebula-genomics-readies-a-marketplace-to-sell-a-precious-dataset-you-216479

Levy, S. (2002). *Crypto: how the code rebels beat the government saving privacy in the digital age*. New York: Penguin Books.

Litman, J. (2000). Information Privacy/Information Property. *Stanford Law Review, 52*(5), 1283. https://doi.org/10.2307/1229515

Lloyd, M. (2008). *The passport: the history of man's most travelled document*. Canterbury: Queen Anne's Fan.

Locke, J. (2003). *Two treatises of government: and a letter concerning toleration* (I. Shapiro, Ed.). New Haven, Conn.; London: Yale University Press.

Lorenzetti, L. (2014, December 4). Bitcoin Seized from Silk Road Offered in Second Auction. *Fortune*. Retrieved from http://fortune.com/2014/12/ 04/bitcoins-seized-from-silk-road-on-offer-in-a-second-auction/

Luhmann, N. (1979). *Trust and power: two works*. Ann Arbor, Mich: UMI Books on Demand.

Ma, M., Rumore, C., Gisolfi, D., Kussmaul, W., & Greening, D. (2018). *SSI: A Roadmap for Adoption*. Retrieved from https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/a-roadmap-for-ssi.pdf

Machkovech, S. (2018, May 24). Amazon confirms that Echo device secretly shared user's private audio. *Arstechnica*. Retrieved from https://arstechnica.com/gadgets/2018/05/amazon-confirms-that-echo-device-secretly-shared-users-private-audio/

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks, 102*, 83–95.

Manders-Huits, N. (2010). Practical versus moral identities in identity management. *Ethics and Information Technology, 12*(1), 43–55. https://doi.org/10.1007/s10676-010-9216-8

Manders-Huits, N., & van den Hoven, J. (2008). Moral identification in Identity Management Systems. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato, & L. Martucci (Eds.), *The Future of Identity in the Information Society* (pp. 77–91). Springer US.

Marlinspike, M. (2012, February 15). What is "Sovereign Source Authority"? Retrieved from https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

Mashal, I., Alsaryrah, O., Chung, T.-Y., Yang, C.-Z., Kuo, W.-H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks, 28*, 68–90.

Mathews, L. (2017). Equifax Data Breach Impacts 143 Million Americans. *Forbes. Last Modified September, 7*.

May, T. C. (2001). Crypto Anarachy and Virtual Communities. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 65–83). Cambridge, Mass: MIT Press.

McCarthy, K. (2018, April 25). ISO blocks NSA's latest IoT encryption systems amid murky tales of backdoors and bullying. *The Register*. Retrieved from https://www.theregister.co.uk/2018/04/25/nsa_iot_encryption/

McKnight, D. H., & Chervany, N. L. (2001). Trust and Distrust Definitions: One Bite at a Time. In R. Falcone, M. Singh, & Y.-H. Tan (Eds.), *Trust in Cyber-societies* (pp. 27–54). Springer Berlin Heidelberg.

McMillan, R. (2014, March 3). The Inside Story of Mt. Gox Bitcoin s $460 Million Disaster. *Wired*. Retrieved from https://www.wired.com/2014/03/bitcoin-exchange/

Melendez, S. (2016, May 20). Amid Arrests and Prosecutions Rules Around Selling Bitcoin Remain Fuzzy. *Fastcompany Magazine*. Retrieved from https://www.-fastcompany.com/3059770/selling-bitcoin-could- land-you-in-jail-but-rules-remain-fuzzy

Menn, J. (2013, December 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220

Merrill, T. W., & Smith, H. E. (2001). What Happened to Property in Law and Economics? *The Yale Law Journal*, *111*(2), 357. https://doi.org/10.2307/797592

Miller, S. (2001). *Social action: a teleological account*. Cambridge; New York: Cambridge University Press.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.

Monti, A. (2010). Trust in the Shell. *Knowledge, Technology & Policy*, *23*(3–4), 507–517. https://doi.org/10.1007/s12130-010-9131-7

Mooney, J. A. (2013). Locked Out on LinkedIn: LinkedIn Account Belongs to Employee, Not Employer. *Intellectual Property & Technology Law Journal*, *25*(6), 16–18.

Moore, A. (2000). Privacy and the encryption debate. *Knowledge, Technology & Policy*, *12*(4), 72–84.

Munzer, S. R. (1990). *A theory of property*. New York: Cambridge University Press.

Munzer, S. R. (2013). Property and Disagreement. In J. Penner & H. Smith (Eds.), *Philosophical Foundations of Property Law* (pp. 289–319). Oxford, United Kingdom: Oxford University Press.

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., & Felten, E. (2016). *Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction*. Princeton: Princeton University Press.

Neisse, R., Steri, G., & Nai-Fovino, I. (2017). *A Blockchain-based Approach for Data Accountability and Provenance Tracking*. 1–10. https://doi.org/10.1145/3098954.3098958

Nickel, P. J. (2015). Design for the Value of TrustTrust. In J. van den Hoven, P. E. Vermaas, & I. van de Poel (Eds.), *Handbook of Ethics, Values, and Technological Design* (pp. 551–567). https://doi.org/10.1007/978-94-007-6970-0_21

Nickel, P. J., Franssen, M., & Kroes, P. (2010). Can we make sense of the notion of trustworthy technology? *Knowledge, Technology & Policy, 23*(3–4), 429–444.

Nicolescu, R., Huth, M., Radanliev, P., & De Roure, D. (2018). Mapping the values of IoT. *Journal of Information Technology*. https://doi.org/10.1057/s41265-018-0054-1

Ning, H., & Wang, Z. (2011). Future internet of things architecture: like mankind neural system or social organization framework? *IEEE Communications Letters, 15*(4), 461–463.

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.2812239

Nozick, R. (1974). *Anarchy, State, and Utopia*. New York: Basic Books.

Ohlberg, M., Ahmed, S., & Lang, B. (2017). *Central Planning, Local Experiments. The complex implementation of China's Social Credit System*. Retrieved from MERICS. Mercator Instituite for China Studies website: https://www.merics.org/sites/default/files/2017-12/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf

Oras, E. (2017, May 12). Alexa Calling Has a Major Privacy Flaw. Retrieved September 2, 2017, from Medium website: https://medium.com/@elise81/alexa-calling-has-a-major-privacy-flaw-7ee42ddcb493

Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., ... Myllymäki, P. (2012). *Long-term effects of ubiquitous surveillance in the home*. 41–50. ACM.

Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: a Textbook for Students and Practitioners*. Heidelberg; New York: Springer.

Pagallo, U., Durante, M., & Monteleone, S. (2017). What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT. In *Data Protection and Privacy:(In) visibilities and Infrastructures* (pp. 59–78). Springer.

Pearce, R. (2019, February 6). Australian government clamping down on security research, academic says. *Computerworld*. Retrieved from https://www.computerworld.com.au/article/657157/government-clamping-down-on-security-research-academic-says/

Penner, J. E. (2003). *The idea of property in law* (Reprint). Oxford: Oxford Univ. Press.

Pentland, A. (2009). Reality mining of mobile communications: Toward a new deal on data. *The Global Information Technology Report 2008–2009*, 1981.

Perera, C., Wakenshaw, S. Y. L., Baarslag, T., Haddadi, H., Bandara, A. K., Mortier, R., ... Crowcroft, J. (2017). Valorising the IoT Databox: creating value for everyone. *Transactions on Emerging Telecommunications Technologies, 28*(1), e3125. https://doi.org/10.1002/ett.3125

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Sensing as a service model for smart cities supported by Internet of Things. *Transactions on Emerging Telecommunications Technologies, 25*(1), 81–93. https://doi.org/10.1002/ett.2704

Poon, J., & Buterin, V. (2017, August 11). *Plasma: Scalable Autonomous Smart Contracts. Working Draft.* Retrieved from https://plasma.io/plasma.pdf

Postma, F. (2018, July 8). After Strava, Polar is Revealing the Homes of Soldiers and Spies. Retrieved July 15, 2018, from Bellingcat website: https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Pouwelse, J., de Kok, A., Fleuren, J., Hoogendoorn, P., Vliegendhart, R., & de Vos, M. (2017). Laws for Creating Trust in the Blockchain Age. *European Property Law Journal, 6*(3). https://doi.org/10.1515/eplj-2017-0022

Proudler, G., Chen, L., & Dalton, C. (2015). *Trusted Computing Platforms TPM2.0 in Context.* Cham: Springer International Publishing.

Pufendorf, S., & Carr, C. (1994). *The political writings of Samuel Pufendorf.* New York: Oxford University Press.

Ramirez, E., Brill, J., Ohlhausen, M. K., Wright, J. D., & McSweeny, T. (2014). *Data Brokers. A Call for Transparency and Accountability.* Retrieved from US Federal Trade Commission website: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Reijers, W., & Coeckelbergh, M. (2018). The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. *Philosophy & Technology, 31*(1), 103–130. https://doi.org/10.1007/s13347-016-0239-x

Reijers, W., O'Brolcháin, F., & Haynes, P. (2016). Governance in Blockchain Technologies & Social Contract Theories. *Ledger; Vol 1 (2016) DO - 10.5195/Ledger.2016.62.* Retrieved from https://www.ledgerjournal.org/ojs/index.php/ledger/article/view/62

Reuters. (2016). Bitcoin Worth $72M Was Stolen in Bitfinex Exchange Hack in Hong Kong. *Fortune.* Retrieved from http://fortune.com/2016/ 08/03/bitcoin-stolen-bitfinex-hack-hong-kong/

Riphagen, W. (1975). Some Reflections on "Functional Sovereignty." *Netherlands Yearbook of International Law, 6,* 121. https://doi.org/10.1017/S0167676800004906

Ripstein, A. (2013). Possession and Use. In J. Penner & H. Smith (Eds.), *Philosophical Foundations of Property Law* (pp. 156–181). Oxford, United Kingdom: Oxford University Press.

Rodrigues, R., Wright, D., & Wadhwa, K. (2013). Developing a privacy seal scheme (that works). *International Data Privacy Law*, *3*(2), 100–116. https://doi.org/10.1093/idpl/ips037

Rodrigues, Rowena, Barnard-Wills, D., De Hert, P., & Papakonstantinou, V. (2016). The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR. *International Review of Law, Computers & Technology*, *30*(3), 248–270. https://doi.org/10.1080/13600869.2016.1189737

Rogaway, P. (2015). The Moral Character of Cryptographic Work. *IACR Cryptology EPrint Archive*, *2015*, 1162.

Rogaway, P. (2016). Practice-Oriented Provable Security and the Social Construction of Cryptography. *IEEE Security & Privacy*, *14*(6), 10–17. https://doi.org/10.1109/MSP.2016.122

Rössler, B. (2015). Should personal data be a tradable good? On the moral limits of markets in privacy. In B. Rössler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 141–161). Cambridge: Cambridge University Press.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness, and gullibility. *American Psychologist*, *35*(1), 1.

Rusbridger, A. (2013, November 21). The Snowden Leaks and the Public. *The New York Review of Books*. Retrieved from http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/

Sahnoune, Z., Aimeur, E., Haddad, G. E., & Sokoudjou, R. (2015, August). *Watch Your Mobile Payment: An Empirical Study of Privacy Disclosure*. 934–941. https://doi.org/10.1109/Trustcom.2015.467

Samuelson, P. (2000). Privacy As Intellectual Property? *Stanford Law Review*, *52*(5), 1125. https://doi.org/10.2307/1229511

Sandel, M. J. (2013). *What money can't buy: the moral limits of markets* (1. paperback ed). New York, NY: Farrar, Straus and Giroux.

Schindler, H. R., Cave, J., Robinson, N., Horvath, V., Hackett, P., Gunashekar, S., ... RAND Europe. (2013). *Europe's policy options for a dynamic and trustworthy development of the Internet of things*. Retrieved from http://dx.publications.europa.eu/10.2759/22004

Schmidt, D. C. (2018). *Google Data Collection* (p. 53). Retrieved from Digital Content Next website: https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

Schneier, B. (2007, November 15). The Strange Story of Dual_EC_DRBG. *Schneier on Security*. Retrieved from https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html

Schneier, B. (2015, February 20). Man-in-the-Middle Attacks on Lenovo Computers. Retrieved June 5, 2017, from Schneier on Security website: https://www.schneier.com/blog/archives/2015/02/man-in-the-midd_7.html

Schneier, B. (2016). Security or Surveillance? In *Don't Panic: Making Progress on the" Going Dark" Debate*. Retrieved from https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Sehra, A., Smith, P., & Gomes, P. (2017). *Economics of initial coin offerings*. Retrieved from http://www.allenovery.com/SiteCollectionDocuments/ICO-Article-Nivaura-20170822-0951%20%20-%20Final%20Draft.pdf

Sen, A. (2007). *Identity and violence: the illusion of destiny* (1. paperback. ed). New York, NY: Norton.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). *Towards Blockchain-based Auditable Storage and Sharing of IoT Data*. 45–50. https://doi.org/10.1145/3140649.3140656

Sharwood, S. (2018, April 9). Russian regulator asks courts to disconnect Telegram. *The Register*. Retrieved from https://www.theregister.co.uk/2018/04/09/russian_regulator_asks_courts_to_disconnect_telegram/

Shcherbak, S. (2014). How should Bitcoin be regulated? *European Journal of Legal Studies*, *7*, 45–91.

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics and Information Technology*, *12*(1), 3–15. https://doi.org/10.1007/s10676-009-9186-x

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164.

Simpson, T. W. (2011). e-Trust and reputation. *Ethics and Information Technology*, *13*(1), 29–38. https://doi.org/10.1007/s10676-010-9259-x

Singer, N., & Mahshwari, S. (2018, October 23). Google Is Teaching Children How to Act Online. Is It the Best Role Model? *The New York Times*. Retrieved from https://www.nytimes.com/2018/10/23/business/google-kids-online-safety.html

Skinner, C. (2016). Will the Blockchain Replace Swift? *American Banker*. Retrieved from https://www.americanbanker.com/opinion/will-the-blockchain-replace-swift

Skinner, Q. (2010). The sovereign state: a genealogy. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments. The Past, Present and Future of a Contested Concept* (pp. 26–46). Cambridge; UK: Cambridge University Press.

Smith, S. M., & Khovratovich, D. (2016). *Identity System Essentials*. Retrieved from https://www.evernym.com/wp-content/uploads/2017/02/Identity-System-Essentials.pdf

Sovrin. (2018, January). *SovrinTM: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust*. Retrieved from https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*(2), 161–167. https://doi.org/10.1007/s12525-015-0191-0

Spiekermann, S., & Novotny, A. (2015). A vision for global privacy bridges: Technical and legal measures for international data markets. *Computer Law & Security Review*, *31*(2), 181–200. https://doi.org/10.1016/j.clsr.2015.01.009

Stajano, F. (2003). Security for Whom? The Shifting Security Assumptions of Pervasive Computing. In M. Okada, B. C. Pierce, A. Scedrov, H. Tokuda, & A. Yonezawa (Eds.), *Software Security -- Theories and Systems Mext-NSF-JSPS International Symposium, ISSS 2002 Tokyo, Japan, November 8-10, 2002 Revised Papers* (pp. 16–27). Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg: Springer e-books.

Streamr. (2017, July 25). *Unstoppable Data for Unstoppable Apps: DATAcoin by Streamr. Version 1.0*. Retrieved from https://s3.amazonaws.com/streamr-public/streamr-datacoin-whitepaper-2017-07-25-v1_0.pdf

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Swan, M., & de Filippi, P. (2017). Toward a Philosophy of Blockchain: A Symposium: Introduction: INTRODUCTION. *Metaphilosophy*, *48*(5), 603–619. https://doi.org/10.1111/meta.12270

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Taddeo, M. (2010). Modelling Trust in Artificial Agents, A First Step Toward the Analysis of e-Trust. *Minds and Machines*, *20*(2), 243–257. https://doi.org/10.1007/s11023-010-9201-3

Tavani, H. T. (2015). Levels of Trust in the Context of Machine Ethics. *Philosophy & Technology*, *28*(1), 75–90. https://doi.org/10.1007/s13347-014-0165-8

Taylor, E., & Michael, K. (2016). Smart Toys that are the Stuff of Nightmares. *IEEE Technology and Society Magazine*, *35*(1), 8–10.

Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. *The Sovrin Foundation*.

Tragos, E. Z., Bernabe, J. B., Staudemeyer, R. C., Luis, J., Ramos, H., Fragkiadakis, A., ... Gluhak, A. (2016). Trusted IoT in the complex landscape of governance, security, privacy, availability and safety. *Digitising the Industry-Internet of Things Connecting the Physical, Digital and Virtual Worlds. River Publishers Series in Communications*, 210–239.

Tu, K., & Meredith, M. W. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review*, *90*(1), 271.

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In *Architecting the internet of things* (pp. 1–24). Springer.

Van den Hoven, J. (2008). Information technology, privacy and the protection of personal data. In J. Van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy*. New York: Cambridge University Press.

van den Hoven, J., & Vermaas, P. E. (2007). Nano-Technology and Privacy: On Continuous Surveillance Outside the Panopticon. *Journal of Medicine and Philosophy, 32*(3), 283–297. https://doi.org/10.1080/03605310701397040

Van Hoecke, M. (2011). Legal doctrine: which method (s) for what kind of discipline? In M. Van Hoecke (Ed.), *Methodologies of legal research: which kind of method for what kind of discipline?* (pp. 1–18). Hart Publishing.

van Niekerk, M., & van der Veer, R. (2017). *Databroker DAO. Global market for local data. v 1.2*. Retrieved from https://databrokerdao.com/whitepaper/WHITEPAPER_DataBrokerDAO_en.pdf

Van Saberhagen, N. (2013). *Cryptonote v 2.0*. Retrieved from https://cryptonote.org/whitepaper.pdf

Vardi, N. (2016). Bit by Bit: Assessing the Legal Nature of Virtual Currencies. In G. Gimigliano (Ed.), *Bitcoin and Mobile Payments: Constructing a European Union Framework* (pp. 55–71). https://doi.org/10.1057/978-1-137-57512-8_3

Velasco, P. R. (2017). Computing Ledgers and the Political Ontology of the Blockchain: COMPUTING LEDGERS. *Metaphilosophy, 48*(5), 712–726. https://doi.org/10.1111/meta.12274

Velleman, J. D. (2005). The self as narrator. In J. Anderson & J. Christman (Eds.), *Autonomy and the challenges to liberalism: New essays*. Cambridge; New York, NY: Cambridge University Press.

Wagner, K., Nemethi, B., Renieris, E., Lang, P., Brunet, E., & Holst, E. (2018). *Self-Sovereing Identity. A position paper on blockchain enabled identity and the road ahead*. (p. 56). Retrieved from Blockchain Bundesverband website: https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf

Waldron, J. (1990). *The Right to Private Property*. https://doi.org/10.1093/acprof:oso/9780198239376.001.0001

Waldron, J. (2013). To Bestow Stability upon Possession: Hume s Alternative to Locke. In J. Penner & H. Smith (Eds.), *Philosophical Foundations of Property Law* (pp. 1–12). Oxford, United Kingdom: Oxford University Press.

Werner, W. G., & De Wilde, J. H. (2001). The Endurance of Sovereignty. *European Journal of International Relations, 7*(3), 283–313. https://doi.org/10.1177/1354066101007003001

Wörner, D., & von Bomhard, T. (2014). *When your sensor earns money: exchanging data for cash with Bitcoin*. 295–298. https://doi.org/10.1145/2638728.2638786

WP29 (Article 29 Data Protection Working Party). (2014, September 16). *Opinion 8/2014 on the on Recent Developments on the IoT, EU Data Protection Working Party*. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Wright, A., & De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Retrieved from https://ssrn.com/abstract=2580664

Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*, 120–134. https://doi.org/10.1016/j.jnca.2014.01.014

Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences, 112*(4), 1036–1040.

Zeilinger, M. (2018). Digital Art as 'Monetised Graphics': Enforcing Intellectual Property on the Blockchain. *Philosophy & Technology, 31*(1), 15–41. https://doi.org/10.1007/s13347-016-0243-1

Zetter, K. (2016, February 18). Apple's FBI Battle Is Complicated: Here's What's Really Going On. *Wired*. Retrieved from https://www.wired.com/ 2016/02/apples-fbi-battle-is-complicated-heres-whats-really-going-on/

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks, 7*(12), 2728–2742.

Zimmerman, P. (n.d.). *Why I Wrote PGP*. Retrieved from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

Zomet, A., & Shlomo, R. U. (n.d.). *Privacy-Aware Personalized Content for the Smart Home*. Retrieved from https://patentimages.storage.googleapis.com/a4/2d/3b/f4c35feb228ded/US20160260135A1.pdf

Zyskind, G. (2016). *Efficient Secure Computation Enabled by Blockchain Technology* (Master Thesis, Massachusets Institute of Technology). Retrieved from https://dspace.mit.edu/bitstream/handle/1721.1/105933/964695278-MIT.pdf

Zyskind, G., Nathan, O., & Pentland, A. (2015a). Enigma: Decentralized Computation Platform with Guaranteed Privacy. *CoRR, abs/1506.03471*. Retrieved from http://arxiv.org/abs/1506.03471

Zyskind, G., Nathan, O., & Pentland, A. "Sandy." (2015b, May). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. 180–184. https://doi.org/10.1109/SPW.2015.27

Acknowledgments

The trajectory of PhD research is often said to be unpredictable not only at the beginning but even during the good part of the path. And while this unpredictability can be challenging at times, it also brings most unexpected and pleasant surprises of intellectual fruits. This is certainly true of this research, and I have been extraordinarily fortunate to have opportunities to engage with the most amazing people on this path, without whom I would not be able to solve all the challenges and reap all the fruits.

My great gratitude goes to my promotor Jeroen van den Hoven, who made this project possible and provided me with an uncountable set of philosophical insights and inspirations. And what is crucial for a successful and serendipitous research journey, his most kind support and guidance has provided me with the space of true intellectual freedom combined with invaluable maps of his expertise and experience. I also want to express sincere gratitude to my co-promotor Udo Pesch, who has helped me to adjust the trajectory of my research in the right direction with his advice and kind support. Our collaboration on the research paper has not only provided me with the new insights but also has helped me to see the value of the chosen research topic in a rather important moment.

I would also like to extend my gratitude to the members of my defense committee - Stefanie Roos, Marijn Janssen, Balazs Bodo, Andrei Zwitter, and Nelke Doorn who have honored this project with their participation. I am most humbled by your interest in my research and very grateful for your eagerness to take part in the defense. I also would like to give warm thanks to the members of the philosophy section at TU Delft. To my paranymph Taylor for the insightful thoughts, down to earth pragmatism, and optimism that he is always happy to share with the others. I am truly honored to call you not just a peer member of the two-strong cohort of this PhD wave but also my friend. This research would certainly not be the same if we never met here. To my paranymph Filippo - thank you for the honor of agreeing to be part of this defense, and thank you for the most interesting and enjoyable discussions that we had from the moment of my arrival.

I want to thank the previous cohort of PhD students who made me feel most welcome when I joined the section - Jan, Shannon and Zoe. Jan, for persuasively demonstrating and convincing me that that philosophical argumentation not only becomes more enjoyable but even more fruitful if combined with a proper Belgian beer. Shannon, for the introduction to the Dutch culture and for the amazing opportunities to appreciate some of the most interesting local traditions and celebrations. Zoe, for the fun discussions we had and endless cheerfulness. I would also like to thank Jonas and Scott who joined the community of sections' PhD students later, it was great to have you as peers and comrades.

I would also like to extend my gratitude to all other members of the section whose presence has created the most stimulating intellectual atmosphere: Ibo, Peter, Maarten, Behnam, Pieter, Sabine, Phil, Jelle, Sjoerd, Michael. Especially I am grateful to all participants of philosophical lunches at the glass room for substantial intellectual enrichment that made Sodexo food feel enjoyable. I also want to express my gratitude to the members of the section who joined later in my PhD trajectory, for the most interesting discussion and just pleasant talks - Aimee, Giulio, Paul, Martin, Juan, Anya, Joost. I also have to express my gratitude for benefits of discussions of our peer group - that included not only some of the above mentioned fellow PhD students of philosophy section - but also Klara, Christine, Laura, Thijs, and Tom. Thank you for your most helpful comments and feedback on my papers.

And of course, I have to mention especially, the help and support of the section's secretaries Diana and Nathalie. Diana from the beginning and up to the finish of my research journey has been providing me with the most invaluable help regarding all kinds of administrative matters. Her ability to address these issues at times seemed like real magic for which I am ever grateful. Nathalie who has always been incredibly helpful with all the kinds of requests and questions I had. I am most grateful for her accurate, timely responses and sometimes crucial reminders. I would also like to thank Janine for her kind support with the graduate school matters. And speaking of TU Delft, I would also like to thank the members of the Blockchain lab who inspired me with their most interesting work in this field.

I also have to extend my gratitude to people from the outside of TU Delft who have helped to shape the trajectory of my PhD research. Luciano Floridi, to whom I am ever grateful for the profound impact on my perception of philosophy as a live discipline that can and should address complex, emerging phenomena of our times. I want to express my sincere gratitude to Primavera De Filippi, who has lighted the path of interdisciplinary blockchain studies for me and provided most kind support with her comments and feedback on the last chapter. I also want to thank Manuel Mazzara who provided me with the most interesting insights on the role of computer science in the rapidly changing world that we live in. And I would like to thank Victor Shreiber who many years ago had helped me to see the unique value of philosophical reasoning in its capacity to bring clarity, coherence, and openness of mind.

A very special thank you goes to a number of pseudonymous members of the online blockchain communities united in their relentless pursuit of new horizons. An eclectic but extremely welcoming amalgam of coders, thinkers and technology enthusiasts who make blockchain more than just a technology but an amazing new space of possibilities and intellectual challenges. I also want to thank my Dutch friends Vincent, Marc, and Josephine who made me feel much more at home in the Netherlands and made me appreciate the local ways of life. And a special acknowledgment goes to Laurence - a person with the unique capacity to generate relentless enthusiasm, paradoxical judgments, and positive thoughts whom I am happy to call my friend.

And last but not least I would like to thank my parents for their unconditional and endless support without which none of this would be achievable. They have provided me with a sense of direction, determination, and meaning - something that can make even seemingly impossible dreams happen.

About the Author

Georgy Ishmaev was born in Chelyabinsk, Russia (1983). He has completed his PhD in Ethics of Technology at the Technical University of Delft between January 2015 and April 2019. He holds a Specialist Diploma (with honours) from the Russian State University of Trade and Economics (Russia) where he studied International Economics, and Candidate of Sciences in Social Philosophy degree from the Chelyabinsk State University (Russia). He also holds a Master by Research degree in Philosophy from the University of Hertfordshire (UK).

List of Publications

Academic Publications

Ishmaev, G. (2017). Blockchain Technology as an Institution of Property. *Metaphilosophy, 48*(5), 666–686. https://doi.org/10.1111/meta.12277

Ishmaev, G. (2018). Rethinking Trust in the Internet of Things. In R. Leenes, R. van Brakel, S. Gutwirth, & P. de Hert (Eds.), *Data Protection and Privacy: The Internet of Bodies* (pp. 203–230). Oxford; Portland, Oregon: Hart Publishing.

Ishmaev, G. (2019). The Ethical Limits of Blockchain Enabled Markets for Private IoT Data. *Philosophy & Technology*. https://doi.org/10.1007/s13347-019-00361-y

Pesch, U., & Ishmaev, G. (2019). Fictions and frictions: Promises, Transaction Costs and the Innovation of Network Technologies. *Social Studies of Science*, 0306312719838339. https://doi.org/10.1177/0306312719838339

Ishmaev, G. (Submitted). Sovereignty, privacy, and ethics in blockchain-based identity management systems.

Academic Presentations and Proceedings

Ishmaev, G. (2018). 'Ethics, Blockchains, and Consumer IoT'. Amsterdam Privacy Conference, Amsterdam, 2018, 5 - 7 October

Ishmaev, G. (2018). 'Trust in the Internet of Things'. Computer Privacy and Data Protection, Brussels, 2018, 24 -26 January

Ishmaev, G. (2015). 'Ethical issues of private data protection in MEMS sensor enhanced biometric information systems'. Amsterdam Privacy Conference, Proceedings, Ed. B. Roessler, Amsterdam, 2015, pp. 201-206

Ishmaev, G. (2014). 'On the Ethical Justification of Privacy'. European Meeting on Cybernetics and System Research, EMCSR. Proceedings, Eds. J. Wilby, S. Blachfellner. Vienna, 2014, ISSN: 2227-7803

Ishmaev, G. (2013). 'Privacy as an Ethical Value '. XXIII Congress of Philosophy, Athens, 2013, 4 - 10 August

Ishmaev, G. (2012). 'On the Information Closure Principles and Ethics of Data Mining'. International Association for Computing and Philosophy, AISB/IACAP Congress. Birmingham 2012, 2 - 6 July

Ishmaev, G. (2011). 'Information closure principle and the sceptical argument'. Seventh European Conference of Analytic Philosophy, ECAP 7. Milan, 2011, 1 - 6 September

Ishmaev, G. (2010). 'Conceptualisations of Information and Knowledge in the Structure of Labour'. Fourth International Conference on the Foundations of Information Science. Beijing, 2010, 21 - 24 August

Ishmaev, G. (2009). 'On the ontological status of information'. VII-th European conference on Philosophy and Computing, Proceedings, Ed. J. Valverdu, Barcelona, 2009, pp. 132-133