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

Ishmaev, Georgy

DOI
10.1007/s13347-019-00361-y

Publication date
2019

Document Version
Final published version

Published in
Philosophy and Technology

Citation (APA)
Ishmaev, G. (2019). The Ethical Limits of Blockchain-Enabled Markets for Private IoT Data. *Philosophy and Technology*, *33*(3), 411-432. https://doi.org/10.1007/s13347-019-00361-y

Philosophy & Technology
https://doi.org/10.1007/s13347-019-00361-y

RESEARCH ARTICLE

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

Georgy Ishmaev [1]

Received: 18 August 2018 / Accepted: 2 June 2019/Published online: 26 June 2019

Abstract

This paper looks at the development of blockchain technologies that promise to bring new tools for the management of private data, providing enhanced security and privacy to individuals. Particular interest presents solutions aimed at reorganizing data flows in the Internet of Things (IoT) architectures, enabling the secure and decentralized exchange of data between network participants. However, as this paper argues, the promised benefits are counterbalanced by a significant shift towards the propertization of private data, underlying these proposals. Considering the unique capacity of blockchain technology applications to imitate and even replace traditional institutions, this aspect may present certain challenges, both of technical and ethical character. In order to highlight these challenges and associated concerns, this paper identifies the underlying techno-economic factors and normative assumptions defining the development of these solutions amounting to technologically enabled propertization. It is argued that without careful consideration of a wider impact, such blockchain applications could have effects opposite to the intended ones, thus contributing to the erosion of privacy for IoT users.

Keywords Privacy · Private data · IoT · Blockchain · Data markets

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 and Spiekermann 2016). The same apprehension applies to many current consumer IoT products that combine client-server models

✉ Georgy Ishmaev
g.ishmaev@tudelft.nl

[1] Technical University of Delft, Jaffalaan 5, 2628 BX Delft, The Netherlands

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, b). 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 (Karlstrøm 2014; Ishmaev 2017; 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.[1] 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 paper 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"

[1] 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.

and Satoshi Nakamoto. 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 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 artifact.[2]

This latter point is of particular interest in the context of this paper 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, b; Streamr 2017; Van Niekerk and 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 propertization 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 the 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 1996). 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; Rössler 2015; Samuelson 2000). Samuelson (2000) aptly condensed this criticism in the maxim that propertization as the solution to privacy is highly misleading since personal data markets are "the problem."[3]

[2] 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.

[3] 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 Rössler (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 (Filippi and Hassan 2018), the term "propertization" seems more appropriate in the given context.

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 constraints 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 (Ishmaev 2017; Reijers and Coeckelbergh 2018; Filippi and 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. Rössler (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.[4] 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, b). 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, b). Based on the analysis of the proposed solutions, the paper argues that blockchain-enabled regimes of property in private data do not in fact solve the ethical

[4] 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).

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 paper is structured as follows: 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. Section 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.

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.[5] 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 and Spiekermann 2016; Ishmaev 2018; 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 between private

[5] Neither, strictly speaking, is there a single standard definition of a 'smart' technology. This paper 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.

data and non-private data is rather difficult to address in the context of physical spaces inhabited by humans.[6]

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.[7] 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 (Ishmaev 2018; Christl and 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 and van den Hoven 2015; Haynes et al. 2017).

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" Zomet and Shlomo (2016). 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

[6] 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 paper; thus, "private data" is used here in the sense of meaningful data.

[7] 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.

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 artifacts, but also privacy invasions based on the inferred information.[8] As Durante (2017) argues, this requires us to move beyond *reactive* conceptualizations 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 the 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 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 and 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 conceptualizations 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 and van den Hoven 2015; Haynes et al. 2017).

It seems, then, that this contradiction between privacy cast as a moral right and 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; Rössler 2015). Furthermore, in the context of IoT, this contradiction adds to the

[8] 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.

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.

3 Blockchain-Based IoT Solutions

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.[9] Thus, this paper 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 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

[9] 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).

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).[10] 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 blockchain.[11] 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.

[10] 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 Walmart. 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 (High et al. 2018).

[11] 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 paper.

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).[12] 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 and Buterin 2017).

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 and 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.[13] 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 paper, 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 paper) the idea of a distributed marketplace for IoT-sourced sensor data.

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

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

[13] 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

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.

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 and 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 nevertheless 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).[14] 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 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

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

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.[15] 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 (Höller 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.

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 (Wörner and 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; Perera et al. 2017; Spiekermann and 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

[15] The number of emerging start-ups 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).

answer this question, we need to evaluate the qualitative novelty of such technologically enabled propertization, and outline its affordances and limits.

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 de-facto 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, b; 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.[16] 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 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.[17] 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.[18]

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

[16] See "Enigma" protocol documentation: https://enigma.co/protocol/AboutThisRelease.html

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

[18] 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).

(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, and 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).[19] 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 themselves 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 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.

4.2 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

[19] Apthorpe et al. (2017) 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.

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 and 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 provide not only excludability and alienability but also transparent asset ownership claims. And, just a brief overview of digital management rights (DRM), technologies show 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 (Spiekermann and 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. 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 and utility tokens. 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.[20] 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.

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-conceptualize 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 blockchain 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-conceptualization of the value of privacy understood and implemented as a property right. However, as this paper demonstrates, 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 and Vermaas 2007). It does not seem plausible though that blockchain-based data provenance solutions can help data owners to exercise property

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

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 paper. 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."[21] 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.

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 propertization 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 and van den Hoven 2015). Monetary compensations as fees fail to address these concerns and other complex

[21] 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).

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 and 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.[22]

These observations avidly demonstrate 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 (Pentland 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 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 cannot be morally desirable from the privacy perspective. Quite the

[22] 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.

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.

References

Acar, G., Englehardt, S., & Narayanan, A. (2018). Four cents to deanonymize: companies reverse hashed email addresses. https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/. Accessed 10 June 2018.

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. Accessed January 2018.

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). New York: Cambridge University Press. https://doi.org/10.1017/CBO9781107590205.

Benet, J. (2014). *IPFS - content addressed, versioned, P2P file system. CoRR, abs/1407* (Vol. 3561). http://arxiv.org/abs/1407.3561. Accessed May 2018.

Brito, J. (2018). What does the EU's general data protection regulation mean for open blockchain networks? Retrieved April 20, 2018, from 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.

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*. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed April 2018.

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. *IEEE*, 5–13. https://doi.org/10.1109/HPCC.2008.172.

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

Colavita, M., & Tanzer, G. (2018). *A cryptanalysis of IOTA's curl hash function*. https://www.boazbarak.org/cs127/Projects/iota.pdf. Accessed June 2018.

Cramer, R., Damgard, I. B., & Nielsen, J. B. (2015). *Secure multiparty computation and secret sharing*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781107337756.

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.

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 (Ed.), *Ethics, law and the politics of information* (Vol. 18, pp. 117–140). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-024-1150-8_7.

Enigma. (2017). *Beyond catalyst: enigma's vision for the future of data.* . From https://blog.enigma.co/beyond-catalyst-enigmas-vision-for-the-future-of-data-22fbb5845556?gi=e67e2743f1cd. Accessed Sept 2017.

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. Accessed March 2018.

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.

Gasser, U., Gertner, N., Goldsmith, J. L., Landau, S., Nye, J. S., O'Brien, D., … Schneier, B. (2016). Don't panic: making progress on the "Going Dark" debate. *The Berkman Center for Internet & Society Study at Harvard University.* https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Accessed Feb 2018.

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

Haynes, J., Ramirez, M., Hayajneh, T., & Bhuiyan, M. 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.

High, D. R., Wilkinson, B. W., Mattingly, T., Cantrell, R., O'brien, V., John, J., … Jurich Jr J. (2018). *US Patent No. US 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=%2220180167200%22.PGNR.&OS=DN/20180167200&RS=DN/20180167200. Accessed July 2018.

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

Ishmaev, G. (2017) Blockchain Technology as an Institution of property. *Metaphilosophy, 48*(5), 666–686.

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.

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.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. (2017). The (unfulfilled) potential of data marketplaces. *The research Institute of the Finnish Economy.* https://www.etla.fi/wp-content/uploads/ETLA-Working-Papers-53.pdf. Accessed April 2018.

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

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). Nebula genomics readies a marketplace to sell a precious dataset: You. *Martech Today.* https://martechtoday.com/nebula-genomics-readies-a-marketplace-to-sell-a-precious-dataset-you-216479. Accessed June 2018.

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

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). US: Springer.

Nakamoto, S. (2008). *Bitcoin: a peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf. Accessed May 2018.

Neisse, R., Steri, G., & Nai-Fovino, I. (2017). *A blockchain-based approach for data accountability and provenance tracking* (pp. 1–10). New York City: ACM Press. https://doi.org/10.1145/3098954.3098958.

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.

Pentland, A. (2009). Reality mining of mobile communications: toward a new deal on data. In *The global information technology report 2008–2009* (p. 1981).

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.

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

Poon, J., & Buterin, V. (2017). Plasma: scalable autonomous smart contracts. *Working draft*. https://plasma.io/plasma.pdf. Accessed Aug 2018.

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

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.

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.

Rogaway, P. (2015). The moral character of cryptographic work. *IACR Cryptology EPrint Archive*, 1162. https://eprint.iacr.org/2015/1162. Accessed Jan 2018.

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.

Sehra, A., Smith, P., & Gomes, P. (2017). *Economics of initial coin offerings*. Allen & Overy. http://www.allenovery.com/SiteCollectionDocuments/ICO-Article-Nivaura-20170822-0951%20%20-%20Final%20Draft.pdf. Accessed Jan 2018.

Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). *Towards Blockchain-based auditable storage and sharing of IoT data* (pp. 45–50). New York City: ACM Press. https://doi.org/10.1145/3140649.3140656.

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.

Streamr. (2017). *Unstoppable data for unstoppable apps: DATAcoin by Streamr*. Version 1.0. https://s3.amazonaws.com/streamr-public/streamr-datacoin-whitepaper-2017-07-25-v1_0.pdf. Accessed Jan 2018.

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 Niekerk, M., & van der Veer, R. (2017). *Databroker DAO. Global market for local data*. v 1.2. https://databrokerdao.com/whitepaper/WHITEPAPER_DataBrokerDAO_en.pdf. Accessed Jan 2018.

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

Zomet, A., & Shlomo, R. U. (2016). *US Patent No. US 20160260135A1*. Retrieved from https://patentimages.storage.googleapis.com/a4/2d/3b/f4c35feb228ded/US20160260135A1.pdf. Accessed July 2018.

Zyskind, G. (2016). *Efficient Secure Computation Enabled by Blockchain Technology (Master Thesis)*. Massachusets Institute of Technology. https://dspace.mit.edu/bitstream/handle/1721.1/105933/964695278-MIT.pdf . Accessed March 2018.

Zyskind, G., Nathan, O., & Pentland, A. (2015a). Enigma: decentralized computation platform with guaranteed privacy. *CoRR, abs/1506.03471*. http://arxiv.org/abs/1506.03471. Accessed Jan 2018.

Zyskind, G., Nathan, O., & Pentland, A. "Sandy." (2015b). *Decentralizing privacy: using blockchain to protect personal data* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27