The interplay between decentralization and privacy: the case of blockchain technologies

Primavera De Filippi

CERSA — CNRS — Université Paris II
Berkman Center for Internet & Society at Harvard

Abstract:

Decentralized architectures are gaining popularity as a way to protect one's privacy against the ubiquitous surveillance of states and corporations. Yet, in spite of the obvious benefits they provide when it comes to data sovereignty, decentralized architectures also present certain characteristics that—if not properly accounted for—might ultimately impinge upon users' privacy. While they are capable of preserving the confidentiality of data, decentralized architectures cannot easily protect themselves against the analysis of metadata. Accordingly, if not properly designed, decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts.

This paper analyses the case of Bitcoin and other blockchain-based networks, as an example of decentralized infrastructures which suffers from radical transparency. While they provide a series of privacy benefits to end-users, the characteristics of these networks present both advantages and risks to the privacy of end-users. On the one hand, the pseudonymous nature of many blockchain-based networks allows for people to transact on a peer-to-peer basis, without disclosing their identity to anyone. On the other hand, the transparency inherent to these networks is such that anyone can retrieve the history of all transactions performed on a blockchain and rely on big data analytics in order to retrieve potentially sensitive information.

The paper concludes that, in spite of the apparent dichotomy between transparency and privacy, there is no real conflict between the two. With the use of advanced cryptographic techniques, it is only a matter of time before people identify news ways to preserve individual privacy in decentralized architectures.

Keywords: *blockchain technology, decentralization, privacy, transparency, cryptography.*

Electronic copy available at: https://ssrn.com/abstract=2852689

Introduction

With the current state of telecommunication technologies, it is becoming harder to communicate on the Internet without leaving traces or disclosing information to centralized third parties —be they governmental agencies or private companies (Lyon, 2014). The trend towards the growing centralization of online platforms has important privacy implications. Not only do these unifying network points constitute a single point of failure, they also qualify as a valuable source of data that might fall prey to hackers. Centralized online operators can also be coerced by governmental agencies to disclose sensitive information about their user-base (Schneier, 2009).

In the wake of the Snowden revelations, there has been a great deal of debate around the need to protect the privacy and confidentiality of online communication. We can witness a growing interest in decentralized architectures as a way to protect one's privacy against the authority and surveillance of centralized third parties. As a general rule, in fact, decentralized architectures (which operate independently of centralized control) are perceived as being more supportive of individual freedoms and civil liberties, such as privacy and freedom of expression (Ziccardi, 2012).

Yet, decentralized systems are much more difficult to implement than centralized platforms. In order to allow for an effective coordination amongst a distributed network of peers, decentralized architectures generally rely on the disclosure of everyone's interactions. Hence, if the price of centralization is *trust* (as users need to trust centralized operators with their data), decentralization comes at the price of *transparency* (as everyone's interactions are made visible to all network's nodes).

If not properly accounted for, transparency might impinge upon users' privacy. In fact, while decentralized architectures can provide more privacy at the content layer (to the extent that content has been encrypted), they cannot protect themselves against the third parties' analysis of data (or metadata) which are publicly disclosed on a decentralized network. Accordingly, unless additional technical means are used to protect the confidentiality of online communications, it might turn out that decentralized infrastructures —designed to promote privacy and autonomy— end up being more vulnerable to governmental agencies or corporate scrutiny than their centralized counterparts.

This paper will focus on Bitcoin and blockchain technologies more generally, to illustrate how highly decentralized technologies might suffer from a situation of *radical transparency* that could potentially impinge upon the privacy of end-users (Bradbury, 2013). After illustrating the benefits that blockchain technologies provide in terms of individual privacy and autonomy, the paper will investigate how data mining techniques applied to the analysis of public blockchain transactions could be just as intrusive as standard surveillance techniques on centralized platforms. Finally, the paper will analyse how recent advances in cryptography may potentially resolve the (alleged) dichotomy between privacy and transparency for the actual benefit of end-users.

Electronic copy available at: https://ssrn.com/abstract=2852689

I. Centralized online architectures

Despite its original distributed design, today's Internet is highly centralized. Most of the Internet traffic is routed through a few centralized services or platforms, managed and controlled by a few large corporations. Centralized platforms are useful coordination tools, which provide end-users with great comfort and convenience; yet, they often come at the expense of privacy and autonomy.

A. Better control and coordination

Coordination can be easily achieved in centralized systems, where information is routed through a series of trusted nodes that collect the information needed to coordinate network activities. Information is processed centrally and is then dispatched to individual users, only inasmuch as necessary to ensure the proper operations of the network. Centralized coordination thus provides two important benefits: first, it reduces the number of transactions (and transaction costs) necessary to coordinate a disparate group of individuals; second, it reduces the amount of unnecessary disclosure that users would otherwise have to cope with in a more decentralized system.

The drawback is that centralized coordination comes at the price of entrusting a centralised authority with the task of managing the network in line with the interests of its user-base (Duffany, 2012). The large majority of today's online platforms are designed around centralized regulation and control. Regulation is facilitated by the fact that centralized operators generally rely on technical and contractual means in order to dictate how people can (or cannot) interact with their platforms. To the extent that they keep track of all online activities taking place on these platforms, centralized operators can potentially intervene to punish those users who do not abide to the platforms' rules.

Yet, not all centralized authorities are worthy of trust. It is not uncommon for online operators to abuse their dominant position over a centralized platform in order to promote their own (economic) interests, often at the expense of that of their user-base.[1]

B. Privacy implications

The privacy of communications can be jeopardized in a variety of ways, depending on the types of architectures at hand. In most centralized systems, users do not need to worry about securing their own communication channels, which are managed by a centralized operator. Instead, users increasingly need to entrust these operators with personal data, with the hope

[1] A recent example of the power wielded by centralized operators is Facebook's social experiment, which arbitrarily modified the NewsFeed displayed to a certain users to identify whether (and how) their mood would be affected. This experiment raised important moral and ethical concerns (Puschmann & Bozdag, 2014), as Facebook has shown to have the ability to control the mood, and perhaps even the actions of its users.

that they will only use it for legitimate purposes (Bilder, 2006). Yet, given that all users' communications travel through these centralized operators, surveillance remains, almost inevitably, an important threat to privacy.

To the extent that they collect relevant data concerning users' activities and online communications, centralized platforms constitute very valuable sources of information, which can be exploited by both ill-intentioned individuals (*e.g.* hackers) and governmental agencies. Besides, most centralized operators are subject to the regime of intermediary liability limitations, promoting cooperation between public authorities and online operators by encouraging the latter to disclose information about alleged infringers so as to escape from potential liability claims (Peguera, 2009).

Although it is indeed possible to encrypt the content of communications, most Internet users lack not only the technical ability, but also the willingness to secure their personal data through encryption techniques. Besides, in many cases, access to personal data has become a precondition for users to enjoy a more personalised service. Users are thus encouraged to disclose more and more information about themselves, and consenting to online operators profiling them in order to reward them with a service that is allegedly more in line with their respective preferences and needs.

We witness a general trend towards increased surveillance and control, as both centralization and personalisation justify the needs for online operators to control the flow of information, monitoring users' activities and keeping track of everything they do online and offline (Lyon, 2001, 2004, 2014).

This situation of is, however, characterized by strong asymmetries of power (Allmer, 2012; Fuchs, 2012): while centralized online operators can access the personal data of their user-base, end-users are generally left in the dark with regard to the data collected, processed or inferred about them.

Large online operators (such as Google, Facebook, Apple, etc.) constantly collect data provided —either willingly or unwillingly— by their user-base. Such data is subsequently aggregated, analysed, interpreted or otherwise processed with a view to provide users with a more customized service (Dwyer, 2011). But the algorithms subtending the processing of such data are not disclosed to the public. They are generally kept secret, in order to maintain a competitive advantage over other intermediaries (Latzer & al., 2014) —but also because of the assumption that, if they were publicly disclosed, people could simply cheat or bypass them. As a result, users cannot properly understand the way these algorithms ultimately affect them in their daily life (Sandvig, 2013; Bozdag, 2013).

As Frank Pasquale (2015) has eloquently stressed, we are now living in a 'black box society' where powerful interests increasingly rely on secrecy not only in order to increase their profits, but also as a means to control the way in which individuals can (or cannot) act.

II. Decentralized online architectures

Decentralized initiatives have emerged in recent years, as a reaction to the growing centralization of data in the hands of a few large online operators (Aberer & Hauswirth, 2002). Decentralized platforms are —in theory— more difficult to censor and regulate than their centralized counterparts. The impact of decentralization on the privacy and confidentiality of information is, however, much harder to establish: on the one hand, decentralization reduces the chances of monitoring by a centralized authority; on the other hand, the openness and transparency of a decentralized network also make information more vulnerable to third parties' grab. Indeed, given that there is no central authority in charge of managing the network, coordination can only be achieved by disclosing information to all nodes. Decentralized platforms thus require a greater degree of transparency in order to effectively coordinate activities between nodes (Galloway, 2004).

A. Privacy benefits

In more decentralized systems, surveillance is more difficult to achieve (although not impossible) because there no single entity that controls and manages the flow of information. However, to the extent that users need to secure their own communication channels, bad securitization practices and security flaws in client-side software become much more relevant, especially when data is stored on users' devices (Cole, 2011).

This notwithstanding, most of the decentralized platforms we encounter today purport to promote user's privacy by focusing on at least one of the following two paradigms: *data confidentiality* and *data sovereignty*. Data confidentiality aims at giving people the power to communicate outside the purview of state or corporations by shielding online communications and interactions from the eyes of third parties. Tools like *TOR* (*The Onion Router*) and *PGP* (*Pretty Good Privacy*), for example, are used by many people around the globe to escape from the surveillance of governmental agencies and the ubiquitous data collection of existing commercial offerings. Data sovereignty focuses instead on giving individuals control over their personal data, which they can share only to the parties they trust. Rather than concealing the data, it is about empowering people to decide exactly when and with whom to share personal information. This can be achieved, for instance, through the implementation of a secure platform for personal data storage — like Eben Moglen's *FreedomBox,* designed to reduce users' dependency on centralized operators. Or it can be achieved by spreading personal data, subdivided into small chunks, to a decentralized network of peers, in such a way that no one can make sense of the data alone. An interesting initiative of this kind is the MIT *Enigma* project, which relies on decentralized storage and secure multi-party computation to allow for the granular disclosure of personal data, on a selective basis, only to authorized third parties.

Instead of storing personal data into central repositories operated by trusted third parties, decentralized solutions rely on a large number of peers, each hosting only a small chunk of

data, which must all cooperate for the data to be processed by an authorized third party. In this sense, decentralization can reduce the power asymmetries that generally provide unfair advantages to centralized operators (Themelis, 2013) with the drawback, however, of increasing coordination costs.

B. The challenges of decentralized coordination

In a decentralized peer-to-peer (P2P) network, it is difficult to monitor and regulate the behavior of individual users, who interact directly with one another without the approval of any intermediary operator. The supervision and coordination of users is much easier in the context of centralized platforms; however, centralized coordination inevitably requires users to rely on a centralized third party, whose interests are not necessarily aligned with that of its user-base.

Given that there is no central authority in charge of coordinating the network, coordination in decentralized systems needs to be achieved in a more distributed fashion (Oram, 2001). This is generally achieved by disclosing specific data (or metadata) to all nodes in the network, so that they can coordinate themselves directly, without any intermediary operator (Aberer & Hauswirth, 2002).

More precisely, in a centralized platform, communications are first communicated to a centralized (trusted) authority, which is responsible for dispatching the information to all relevant nodes. Conversely, in a decentralized P2P network, every node communicates with every other node in the network to ensure that proper coordination is achieved. Yet, in absence of a central authority in charge of policing the network, malicious users might be tempted to 'cheat' the system for their own gain. Transparency can thus be regarded as a means for the network to police itself, by enabling users to collectively verify the legitimacy of every network transaction (Bradbury, 2013). This need for transparency is well illustrated by the case of blockchain technologies such as Bitcoin for instance, where every transaction is publicly disclosed to the network so that it can be simultaneously verified and validated by every node in the network (Nakamoto, 2008).

Accordingly, it could be said that the more decentralized an infrastructure is, the less it relies on trust and the more it relies on transparency instead. On that regard, it is worth distinguishing between two types of transparency: *content transparency*, which requires the disclosure of the actual content of communication; and *protocol transparency*, which only requires the disclosure of metadata or other kinds of administrative information. While the former is not a prerequisite for decentralized coordination, the latter is needed in virtually all decentralized infrastructures. Hence, if decentralization can contribute to promoting user's privacy and confidentiality at the content layer, it might, however, come at the price of *radical transparency* at the protocol or metadata layer.

III. Privacy and Decentralization: friends or foes? —The case of blockchain technologies

If participants to a decentralized network are, indeed, required to exchange information in order to interact in a coordinated way, decentralization might have both a positive and negative impact on the protection of users' privacy. On the one hand, decentralization might reduce the dependency of individuals on centralized service providers, while improving their ability to protect their own data from the eyes of third parties. On the other hand, the degree of transparency necessary for the purpose of coordinating the activities of a large network of peers might require the disclosure of a significant amount of metadata to be made available to the overall network.

Accordingly, in order to understand the privacy implications of decentralized architectures, we must analyse whether the privacy gains resulting from decentralized coordination are greater than the privacy costs derived from the disclosure of metadata that may possibly reveal personal information.

The analysis will focus, in particular, on the technology underlying the Bitcoin network: the *blockchain* —an emerging technology that represents an important and promising development in information and communication technologies, insofar as it enables people to transact and interact with one another without any centralized intermediary. As a coordination technology, the blockchain relies on transparency to enable new forms of collective action that were previously thought to be impossible (Swan, 2015). The extent to which blockchain-based applications might (either positively or negatively) affect the privacy of end-users is, however, still open to debate.

A. Technical overview of blockchain technologies

A blockchain is a decentralized ledger (or state machine) that relies on cryptographic algorithms and economic incentives in order to ensure the integrity and legitimacy of every transaction (or state change). A copy of the blockchain is shared amongst all nodes connected to the network, which comprises the history of all valid transactions. Each transaction is recorded into a 'block' which is appended *sequentially* to the previous block of transactions (Nakamoto, 2008). In order to prevent anyone from tampering with past transactions, the blockchain acts as an append-only ledger —*i.e.* once information has been recorded onto the blockchain, it can no longer be edited or deleted. The result is a long chain of blocks (or *blockchain*) that represents the whole chain of transaction ever since the first *genesis block* (Sprankel, 2013).

The blockchain can thus be regarded as a secure database that comprises a public log of all transactions which have been thus far validated by the network. In view of its decentralized nature, the security of the blockchain and the validity of every transaction can only be ensured through distributed consensus (*i.e.* through nodes verifying the integrity and legitimacy of each block, independently of any trusted third party). This requires that the

transaction history be made available to the public, so that it can be easily verified by anyone. The consequence is, however, that anyone who has access to a copy of the blockchain also has access to the current (and past) consensus state —with regard to *e.g.* the flow and the amount of all validated transactions (Ober & al., 2013).

The core innovation of the blockchain is its ability to validate transactions in a decentralized manner, without the need for a trusted authority. Until recently, digital currencies were operated through a central operator or trusted intermediary. Blockchain technologies eliminate the need for a central clearinghouse by allowing for transactions to be verified and computer logic to be executed in a decentralized manner. Instead of requesting confirmation for every transaction to a centralized authority, blockchain's distributed consensus is such that any attempt at tampering with the consensus state will most likely be rejected by the network as an invalid transaction.

Initially developed as part of the Bitcoin network, the blockchain is a general purpose technology that can be used for many other kinds of applications which formerly required the existence of a trusted third party: from decentralized domain name systems (*Namecoin*) to decentralized land and commercial registries (*Factom*) or any decentralized application that can be run on the *Ethereum* blockchain. In particular, the Ethereum blockchain enables the creation of so-called *smart contracts* —software applications deployed directly on the blockchain (as opposed to a central server) which are self-executing, in the sense that they are executed automatically whenever someone enters into a transaction with them. The software code is run in a distributed manner, by every node in the network, and the resulting output is validated only if it is agreed upon by the majority of nodes. These emergent technologies introduce one more step towards the process of disintermediation, as many things that previously required a centralized intermediary to coordinate the action of multiple individuals can now achieved in a decentralized manner through the blockchain.

B. Transparency for better contextual integrity

Hellen Nissenbaum (2004) introduces the notion of *contextual integrity* as a new benchmark for privacy that better accounts for the specificities of modern societies. In a world awash in information and communication technologies, surveillance by both governmental agencies and private companies has become commonplace (Schneier, 2009; Lyon, 2014). Traditional expectations of privacy with regard to the gathering and processing of personal data are increasingly difficult to transpose in that new environment. In this sense, contextual integrity extends beyond the customary understanding of privacy as it relates to information flows, to also consider the way data *should* be collected and/or processed according to the social, moral or political norms of the context at hand.

This concept is particularly relevant when we look at the asymmetries of power slowly emerging on the Internet with the advent of the 'blackbox society' (Pasquale, 2015). As mentioned earlier, most of the algorithms subtending centralized online platforms like Google or Facebook are not publicly disclosed. The opacity of these algorithms makes it

difficult for users to understand how their life is actually affected by them. Besides, centralized operators preserve the capacity to unilaterally modify their offer at will, without users' approval. Insofar as they control the platform upon which users interact, they retain the ability to control and regulate all of the online activities, both by contractual means (*e.g.* end-user licensing agreements) and technical means (*i.e.* as a result of technical design).

Blockchain technologies can significantly affect the existing power dynamics between online operators and their users. With the blockchain, users activities are governed exclusively through the code or the protocol of the underlying network or technology. And, as opposed to more centralized systems, no one can impose or even modify any of these technical rules without obtaining the consensus of the network (*i.e.* of a majority of network's nodes). In particular, in view of the inherent transparency of the blockchain network, every participant node has the ability to monitor the whole flow of transactions occurring on that network.

The same applies for every piece of software deployed on the blockchain (a.k.a *smart contracts*), which is always and necessarily *deterministic* and *open state* —*i.e.* even if the code source of the software is not stored on the blockchain, the operations of the code (a.k.a the *bytecode*) are made publicly available for every node in the network to be able to execute and validate the result of these operations. The transparency of the blockchain network thus provides a greater degree of control to end-users, who no longer need to trust online operators with regard to the software they run. Indeed, given that the software bytecode is deployed directly onto the blockchain, users can always look at it in order to better understand the inner workings of that software[2] —knowing that such software comes with a guarantee of execution (*i.e.* it will always lead to the same predeterministic outcome).

Of course, there are also cases in which specific nodes decide not to publicly reveal the way they came to a specific result. These nodes (a.k.a *Oracles*) operate like their own little black-boxes: most of their operations are done *off-chain* (*i.e.* outside of the blockchain infrastructure) and only the outcomes of these operations are published onto the blockchain. Note that these constitute an exception to the traditional functioning of the blockchain, which might significantly reduce the level of trustlessness in the network.

As a general rule, one could say that, in most cases, users are in a better position to evaluate —per Nissenbaum's contextual privacy framework— the workings of the individual operations performed on a blockchain. Yet, as explained more in details below, such a degree of transparency might not always be desirable. In some cases, in fact, the transparency inherent to these decentralized technologies might actually go counter to the traditional expectations of privacy.

[2] This can be done, ideally, by comparing the *bytecode* on the blockchain with the compiled version of the provided source code, so as to ensure that the two are the same.

C. Modified power dynamics

Decentralized technologies offer important advantages to end-users. Not only do they preserve privacy and confidentiality, they also come along with the promise of furthering individual freedoms and emancipation by providing a greater degree of autonomy to end-users.

Many centralized platforms are operated by large commercial players, whose interests are often incompatible with that of end-users, who are obliged to accept the terms and conditions unilaterally imposed on them. Conversely, most decentralized platforms are operated by a community of peers, who get to decide on their own —with all the complexities this may entail— how to best deploy the technology in order to fulfill their needs (Oram, 2001).

Decentralized networks are also generally more open than their centralized counterparts. While there exist a variety of closed decentralized systems (such as the case of the "permissioned" blockchain used by the finance industry), most public blockchain —such as Bitcoin or Ethereum— have been designed as an open network which anyone can join and contribute to. And to the extent that they are *pseudonymous* (*i.e.* there is no centralized authority in charge of verifying the credentials of users), anyone is free to participate to these networks provided that they comply with their protocols and technological standards.

Overall, the combination of decentralization and openness ensures a greater degree of autonomy, diversity and interoperability (*e.g.* multiple clients can implement differents set of features on top of the same protocol layer).

But decentralization is not devoid of any drawbacks. Beyond the issues surrounding coordination and control (listed above), the lack of centralized supervision or oversight also makes decentralized architectures more likely to be co-opted or manipulated by established powers. Given that there is no central authority in charge of managing the network, vested interests might be tempted to jump in and take over the network, or simply manipulate it, either directly or indirectly.[3] As opposed to many centralized platforms with a formalized hierarchical structure with clear and obvious power dynamics, in a decentralized network, as power might eventually consolidate into unofficial clusters, the lack of an formalized power structure makes it harder for people to understand who is actually in control of the network. This informal and invisible power is all the more problematic because its very existence is not properly acknowledged by all (Wainwright, 2006).

Perhaps the best example of such evolving power dynamics in the blockchain space can be observed through the Bitcoin network. As a decentralized payment system, the Bitcoin network relies on the work of peers connected to the network (so-called *miners*) in order to verify the validity and integrity of every transaction. Given the openness of the Bitcoin network, anyone can participate to the operations of the network. However, with the large

[3] For instance, the anonymity of the TOR network has allegedly been jeopardized by the U.S. government, who deployed a large number of relay nodes into the network. Anyone who controls a sufficiently large portion of the TOR network can get a fairly good overview of the traffic routed through the network —thus making it possible to identify the source and/or destination of certain communications.

economic incentives brought about by the recent rise in value of Bitcoin (along with the advent of more sophisticated mining technologies and the existence of cheap electricity and permissive local economies, especially in China), the *mining* of Bitcoin has grown more and more centralized. The Bitcoin network is now for the most part controlled by only a few large mining pools, which —if they were to collude— could easily take over the whole network with a 51% attack (Kroll & al., 2013).

D. Transparency at the detriment of privacy?

As we have seen earlier, decentralized platforms tend to be more respectful to users' fundamental right to privacy to the extent that they make it harder for centralized third parties to have complete control over users' data. In a peer-to-peer system, data is stored either locally on the users' devices (and communicated only to the relevant parties) or is spread all over the network where multiple parties (or peers) are in charge of storing and processing small fragments of such data. While the information is theoretically visible to anyone, the use of end-to-end encryption allows users to communicate privately with one another, without having to entrust anyone with the task of managing and transferring personal information (Clarke & al., 2002; Cutillo & al., 2009).

However, since there is no centralized entity in charge of collecting, storing and processing data, the only way for users to coordinate themselves in a decentralized manner is to make data available to every other user of the network. Although the content of communications can be encrypted so that it can only be accessed by the persons to whom it was actually addressed (*e.g.* by relying on end-to-end encryption), the metadata related to these communications *(i.e.* who is talking to whom, for how long, and what is the type of transaction in which they participate) needs to be visible to a majority of network's nodes.

While this is not an inherent requirement of any decentralized system,[4] it is, in practice, the most common implementation of these systems. The reason is that building decentralized systems is generally much harder than building a centralized platform. Most of the time, the challenges involved in the design of a decentralized architecture are thus made easier by giving up the privacy of metadata. This results in an impending tension between degree of decentralization that a network enjoys and the amount of privacy that users of that network may effectively expect (Filipovikj & Holmstedt, 2013).

This tension is well illustrated by the case of blockchain technologies. It is, in fact, often believed that —because of their decentralized nature— blockchain-based applications might contribute to promoting individual's privacy and autonomy. Indeed, instead of relying on the coordination activities of a centralized authority, the blockchain operates through a

[4] Obviously, there exist many exceptions to that rule. The *Onion Router* (TOR) is a clear example of how a decentralized network can be designed so as to preserve anonymity with regard to the source of online communications. Similarly —although less widely adopted— the *Freenet* project implements a distributed anonymous information storage and retrieval system, whose communications are encrypted by default, and metadata information is obfuscated via sophisticated routing techniques.

decentralized public ledger which is regulated exclusively by code and algorithmical rules. Yet, in order to allow for meaningful coordination, the blockchain must be both accessible and auditable by every node in the network. Without a centralized intermediary, the only way for individuals to properly coordinate themselves is for everyone to share a common datastore with the most updated state of the consensus. The inherent transparency of blockchain technologies represents therefore a useful mechanism to successfully coordinate the behavior of several individuals that do not know (nor trust) each others.

1. Anonymity versus Pseudonymity

The fact that all blockchain transactions need to be publicly available to every node in the network does not necessarily means that blockchain users cannot have any expectation of privacy. Bitcoin and many other blockchain-based applications mitigate the costs of transparency by virtue of pseudonymity. In this regard, Bitcoin is often referred to as an anonymous and decentralized cryptocurrency, in that it allows people to transact with one another without having to disclose any information related to their actual identity. Despite the transaction history being publicly available to anyone, insofar as the public addresses used in every transaction are random numbers that do not need to be associated with an identity, privacy can be preserved as long as it is not possible to trace back these transactions to any given identity.

Yet, the truth is that Bitcoin is not *anonymous*, but rather *pseudonymous*. Anonymity means that it is impossible to link any given identifier to a specific identity; whereas pseudonymity merely refers to the use of an identifier as a way to disguise the real identity. More specifically, in the context of blockchain technologies, anonymity makes it impossible to relate multiple transactions with a single source or destination, whereas pseudonymity only implies that the identity of the person(s) associated with that specific source or destination cannot be (easily) established. While this might provide a limited degree of privacy, this feature alone is not sufficient to ensure a proper amount of privacy protection.

Although blockchain technologies could potentially be implemented in an anonymous way, most of the blockchain-based application implemented so far do not provide strong anonymity support (Reid & Harrigan, 2013). The result is that the transparency of the Bitcoin blockchain may ultimately hinder —instead of furthering— the privacy of end-users.

In particular, the design of the Bitcoin blockchain is such that the more an address is used, the more information can be inferred from this address. While good privacy norms would require people to constantly generate a new address before performing a new transaction, only a minority of people actually engage in these practices. In the Bitcoin space, most non-tech savvy people simply reuse their Bitcoin address without realizing that, by doing so, they are publicly disclosing valuable personal information. This can be quite problematic from a privacy standpoint. Given the transparency and non-repudiability of the Bitcoin blockchain, it is possible to keep track of every transaction involving a particular Bitcoin address. Regardless of how careful a person has been to hide his or her identity in the past, once the

identity of the person owning that Bitcoin address has been established, it then becomes possible for anyone to retroactively associate to that person all the transactions which have previously been made to and from that address (Moser, 2013).
With that in mind, specific data analysis techniques have already been deployed to extract, deduce or infer new information from the transaction history that has been stored on the blockchain.

2. Blockchain analytics

As Bitcoin adoption grows and expands into more and more regulated sectors of activities, the ability to identify the source and destination of financial transactions becomes an even stronger imperative. Indeed, the finance industry is a strongly regulated industry, which needs to comply with significant formalities in order to ensure that it is dealing only with legitimate clients. Given the difficulty to establish the identity of pseudonymous blockchain addresses, the Bitcoin blockchain has often been used for illicit activities —see, *e.g*. the case of the Silk Road market-place (Barratt, 2012). Although these constitute only a marginal portion of all Bitcoin transactions, the risk to be regarded as facilitating criminal activities might be sufficient to dissuade financial or commercial operators from interacting with non-identified Bitcoin addresses (Moser & al., 2013).
In view of the growing commercial impact of Bitcoin, many companies are turning blockchain analytics into a new business model, providing tools for other companies to comply with the law, such the anti-money laundering (AML) regulations. By associating pseudonymous Bitcoin address with real-world entities, these tools identify the list of Bitcoin addresses which are knowingly related to criminal activities, and which should therefore be blacklisted by any law-abiding operator.
For instance, companies such as *Coinalytics*, *Coinometrics*, etc. are building tools for people in the Bitcoin industry to extract new and meaningful insights from the Bitcoin blockchain, so as to support business intelligence and compliance with the law. On that regard, the company *Elliptic* recently launched a new project —the *Bitcoin Big Bang*— which provides an interactive tool for visualizing past and current transactions on the Bitcoin network, along with the identity of the person or company that issued or received these transactions. Thanks to these services, users can immediately get a good grasp of what is going on in the Bitcoin space, in order to make better informed decisions as to whom they should transact with (Moser, 2013).
All of these initiatives are thus challenging the initial conception of the Bitcoin network as a means for people to bypass traditional financial institutions in order to freely and anonymously transfer value. Indeed, the inherent transparency of the Bitcoin blockchain is such that the history of every transaction can potentially be tracked down, back to the place where it originated (the so-called *coinbase transaction*). This means that any Bitcoin transaction which has ever been issued by an allegedly criminal address, or which has simply

transited through a Bitcoin address associated to a criminal identity, will be forever 'tainted' by its own history (Moser & al., 2013, 2014).

This has significant implications as regards the fungibility of Bitcoin. While it has not happened thus far, it is not unconceivable that —as a result of regulatory pressures— a certain number of financial or commercial operators might refuse to deal with specific transactions whose history might lead them to qualify as potentially fraudulent transactions.[5] Hence, two transactions with the same Bitcoin face value might not have the same operational value, depending on whether or not such transactions could be regarded as potentially tainted transactions. The risk is that Bitcoin transactions which are currently not tainted, might eventually be identified as tainted transactions, *i.e.* whenever a public address is found to be associated with criminal activities. Hence, Bitcoin operators might need to look at the history of every transaction they deal with, in order to reduce the risk of accepting a potentially tainted transaction. It might turn out that younger transactions (with a shorter transaction history) end up being perceived as more valuable —because less risky— than those with a longer transaction history.

Of course, technological advances are under a constant race: as the number of initiatives concerned with blockchain analytics increases, also the number of developers seeking to elaborate new mechanisms to preserve the privacy or anonymity of blockchain transactions increases.

E. Modern advances in cryptography

While the blockchain does not, as such, provide any kind of privacy protection, it would be a mistake to believe that the transparency required to operate on the blockchain necessarily and unavoidably goes counter to the privacy of end-users. In spite of the apparently conflictual relationship that subsists between privacy and transparency, the two are not necessarily incompatible with each other.

Transparency only subsists at the most basic layer of the blockchain —that which is responsible for applying the distributed consensus algorithm. But this does not preclude people from building additional layers of encryption and/or obfuscation on top of that layer, with sophisticated mechanisms specifically meant to conceal the source and destination of transactions, as well as potentially even the content thereof (Chaum, 1984).

In this sense, the blockchain today is not so different from the TCP/IP layer of the Internet network, which relies on a system of public IP addresses, with regard to both the source and

[5] Suggestions of this kind have already been raised in the past, albeit with little success. For instance, former Bitcoin core developer Mike Hearn initially proposed to add a "red-flag" feature into the Bitcoin client, to mark bitcoin transactions that originate from illicit. Similarly, Alex Waters, also former Bitcoin developer, launched Coin Validation, a due diligence service for Bitcoin businesses providing a list of well-known Bitcoin address, along with a red-flag system for protecting business from transacting with Bitcoin addresses associated with illicit use. Both ideas met a lot of resistance within the Bitcoin community, as they approached the risk of fraud and money laundering in digital currencies by breaking the fungibility of Bitcoin. Yet, as regulators start to engage more seriously into the Bitcoin ecosystem, these initiatives might actually be endorsed by the law.

destination of online communications. Initiatives such as *TOR* and *Freenet* have specifically addressed this issue, by introducing an additional layer of anonymity on top of the TCP/IP protocol. Similarly, the content of these communications does not have to be neither public nor transparent (*i.e*. clear text), in order for a machine to efficiently route the packets through the network. The development of a public encryption standard (DES) and, in particular, the popularisation of public-key cryptography (RSA) in the mid-90's, have made it possible for people to use the Internet as a public telecommunication infrastructure, while nonetheless being able to preserve the privacy and confidentiality of their communications.

The same can be done with the blockchain. Technologies such as *CoinJoin*, *CoinSwap*, *CoinShuffle*, etc. are designed to mitigate the privacy-drawbacks of the Bitcoin blockchain by means of obfuscation. These mechanisms exploit one of the most basic features of the Bitcoin blockchain (*i.e.* the independent construction of Bitcoin transactions from other transactions) to provide a greater level of anonymity and confidentiality of transactions (Bonneau & al., 2014).

Ring signatures are also gaining popularity in the blockchain space. As a special type of digital signatures, they allow for a group of people to transact with each other, and with third parties, without revealing the link between an individual signature and an individual's public key. More sophisticated systems exist, such as the Zerocash protocol, which extends the Bitcoin protocol with more advanced cryptographic algorithms (based on zero-knowledge proof) in order to enable people to execute direct payments to each other, without disclosing the source, the destination, nor even the actual amount of these transactions. More recently, *Blockstream* has introduced the notion of *confidential transactions* as a means to improve the privacy and security of the Bitcoin network, without introducing any additional cryptographic primitive to the Bitcoin blockchain. Confidential transactions rely on advanced cryptographic techniques (so-called additively homomorphic commitments) in order to provide a means for people to keep the actual amount of their transactions private, while nonetheless allowing for the public network to verify the validity of these transactions (*i.e.* by making sure that the ledger entries add up). When combined with mixing technologies such as *CoinJoin*, these tools could effectively preserve privacy both at the content level (transaction type and amount transferred) and metadata level (source and destination of the transaction).

It is worth noting that these cryptographic techniques —while ensuring that transaction data remains confidential *by default*— are not necessarily incompatible with the notion of transparency. Users retain the ability to uncloak their transaction data to third parties (such as escrow agents, investors, potential business partners, auditors, authorities and law enforcement) in order to disclose relevant information to third party in a certified way.

Conclusion

Centralized and decentralized platform infrastructures have different implications for the privacy of end-users. In the case of centralized architectures, end-users communicate to each other through a centralized platform, operated by a trusted authority. In order to dispatch the information it receives to all relevant parties, centralized platforms are thus, *by design*, required to collect the information concerning at least the metadata of online communications. In the case of decentralized architectures, end-users communicate directly to one another, without passing through any centralized intermediary. Communications are routed through a decentralized network —*i.e.* one that does not rely on any single trusted authority. The flipside of that, however, is that, in order to transfer the information to the right destination, the metadata related to every communication needs to be made available to the network as a whole.

The technical characteristics of these different architectures might dictate the design choice of a particular platform. Assuming that there is a trusted entity, it is much easier to implement a platform that is respectful of people's privacy through a centralized model rather than a decentralized network. However, if one cannot trust the central authority to fully respect people's privacy, then a decentralized infrastructure might constitute a better choice.

As opposed to centralized systems, which are characterized by strong information asymmetries between the operator and its users, open and decentralized network are more egalitarian, to the extent that they bear an equal level of transparency across all the participants in the network. While decentralized coordination may require the disclosure of additional information, transparency does not constitute a loss of privacy in and of itself. Yet, in order to protect their privacy against the scrutiny of third parties, users might need to deploy additional privacy-enhancing technologies (*e.g.* end-to-end encryption, network obfuscation tools, etc.) on top of the existing platform (Ziccardi, 2012; Milan, 2013).

Of course, complete privacy and anonymity can never be guaranteed. For instance, whenever there is a backdoor or a bug in the technology, even the most sophisticated encryption techniques will be unable to protect users' privacy and identities. More generally, regardless of how much effort has been put into the design of a secure decentralized architecture, there is no guarantee that people's privacy will never be compromised. Indeed, in a decentralized system, the responsibility of keeping data private merely shifts from the operator to the individual user. While the former is more likely to be coerced (*e.g.* by government) to disclose information about its user-base, the later is more likely to inadvertently disclose or leak information through an improper use of the platform or tools. All in all, any system whose security ultimately relies on encryption technologies can only be as secure as the ability of users to securely manage their secrets (*e.g.* passwords or private keys).

In this article, we focused on the case of Bitcoin as a particular example of a blockchain-based application that is decentralized both at the infrastructure and governance level. While Bitcoin might serve to promote individual and financial autonomy, the transparency of the

Bitcoin network also raises important challenges as regards the privacy and confidentiality of transactions.

After showing that transparency is a necessary condition to implement a *trustless system* that does not rely on any trusted authority or intermediary, we have shown that transparency is not necessarily in conflict with privacy. While some transparency is required to validate transactions in the current implementation of Bitcoin, modern cryptographic techniques can be used to prove that a particular transaction is indeed legitimate, without having to disclose the source, the destination, nor the actual content of the transaction. Some of these techniques are already well understood (e.g. blind signatures), other are not yet fully mature and still in course of development (e.g. homomorphic encryption) but it is only a matter of time and engineering to perfect them.

Decentralized technologies —and blockchain technologies in particular— are paving the way for new forms of disintermediation which, depending on the uses that are made of them, might either increase or decrease people's ability to protect their privacy and data confidentiality. This paper has analysed the relationship between privacy and transparency in decentralized infrastructure, showing that —although there obviously exists a correlation between them— the interaction between the two is a complicated one, which cannot be fully understood without accounting for both technical and social factors. While it might be harder to implement a decentralized system that is fully privacy-compliant, transparency and privacy should, however, not be regarded as being in a fundamental conflict. Quite to the contrary, the two are to a large extent compatible, and perhaps even complementary to a lesser extent.

References & Bibliography

Aberer, K., & Hauswirth, M. (2002, March). An Overview of Peer-to-Peer Information Systems. In WDAS (Vol. 14, pp. 171-188).

Agre, P. E. (2003). P2p and the promise of internet equality. Communications of the ACM, 46(2), 39-42.

Allmer, T. (2012). Critical internet surveillance studies and economic surveillance. Internet and Surveillance: The Challenges of Web 2.0 and Social Media, 16, 124

Barratt, M. J. (2012). Silk Road: eBay for drugs. Addiction, 107(3), 683-683

Bechmann, A. (2013). Internet profiling: The economy of data intraoperability on Facebook and Google. MedieKultur. Journal of media and communication research, 29(55), 19.

Bilder, G. (2006). In Google we trust?. Journal of Electronic Publishing, 9(1).

Bradbury, D. (2013). The problem with Bitcoin. Computer Fraud & Security,2013(11), 5-8.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for Bitcoin with accountable mixes. In Financial Cryptography and Data Security (pp. 486-504). Springer Berlin Heidelberg.

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. Ethics and information technology, 15(3), 209-227.

Chaum, D. (1984). Blind signature system. In Advances in cryptology (pp. 153-153). Springer US

Chiu, A. T. (2011). Irrationally bound: terms of use licenses and the breakdown of consumer rationality in the market for social network sites. S. Cal. Interdisc. LJ, 21, 167.

Clarke, I., Miller, S. G., Hong, T. W., Sandberg, O., & Wiley, B. (2002). Protecting free expression online with Freenet. Internet Computing, IEEE, 6(1), 40-49.

Cole, E. (2011). Network security bible (Vol. 768). John Wiley & Sons.

Cutillo, L. A., Molva, R., & Strufe, T. (2009, February). Privacy preserving social networking through decentralization. In Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on (pp. 145-152). IEEE.

De Filippi P. (2013), Ubiquitous Computing in the Cloud: User Empowerment vs. User Obsequity, in: Jean-Eric Pelet, Panagiota Papadopoulou (eds.) 'User Behavior in Ubiquitous Online Environments', IGI Global.

Duffany, J. L. (2012). Cloud Computing Security and Privacy. In 10th Latin American and Caribbean Conference for Engineering and Technology (pp. 1-9)

Dwyer, C. (2011). Privacy in the Age of Google and Facebook. Technology and Society Magazine, IEEE, 30(3), 58-63.

Filipovikj, P., & Holmstedt, C. (2012). Comparison between centralised and decentralised systems and how they cope with different threats. Abgerufen am,22(08), 2013.

Fuchs, C. (2012). Critique of the political economy of Web 2.0 surveillance.Internet and Surveillance. The Challenges of Web 2.0 and Social Media, 31-70.

Galloway, A. R. (2004). Protocol: How control exists after decentralization. MIT press.

Hughes, D., Walkerdine, J., Coulson, G., & Gibson, S. (2006). Peer-to-peer: Is deviant behavior the norm on p2p file-sharing networks?. Distributed Systems Online, IEEE, 7(2).

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013).

Latzer, M., Hollnbuchner, K., Just, N., & Saurwein, F. (2014). The economics of algorithmic selection on the Internet. Working Paper, IPMZ. Zurich,
Lyon, D. (2001). Surveillance society: Monitoring everyday life. McGraw-Hill Education (UK).
Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. Information, Communication & Society, 5(2), 242-257.
Lyon, D. (2003). Surveillance after september 11 (Vol. 11). Polity.
Lyon, D. (2004). Globalizing Surveillance Comparative and Sociological Perspectives. International Sociology, 19(2), 135-149.
Lyon, D. (2014). Surveillance, snowden, and big data: capacities, consequences, critique. Big Data & Society, 1(2), 2053951714541861.
Milan, S. (2013). Social movements and their technologies: Wiring social change. Palgrave Macmillan.
Möser, M. (2013). Anonymity of Bitcoin transactions. In Münster Bitcoin Conference
Moser, M., Bohme, R., & Breuker, D. (2013, September). An inquiry into money laundering tools in the Bitcoin ecosystem. In eCrime Researchers Summit (eCRS), 2013 (pp. 1-14). IEEE.
Möser, M., Böhme, R., & Breuker, D. (2014). Towards risk scoring of bitcoin transactions. In Financial Cryptography and Data Security (pp. 16-32). Springer Berlin Heidelberg.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.Consulted, 1(2012), 28.
Ober, M., Katzenbeisser, S., & Hamacher, K. (2013). Structure and anonymity of the bitcoin transaction graph. Future internet, 5(2), 237-250.
Oram, A. (2001). Peer-to-peer: harnessing the benefits of a disruptive technology. " O'Reilly Media, Inc.".
Nissenbaum, H. (2004). Privacy as contextual integrity. Washington law review,79(1)
Pasquale, F. (2015). The Black Box Society. Cambridge, MA: Harvard University Press, 36, 32.
Peguera, M. (2009). The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. Columbia Journal of Law & the Arts, 32, 481.
Puschmann, C., & Bozdag, E. (2014). Staking out the unclear ethical terrain of online social experiments. Internet Policy Review, 3(4).
Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system(pp. 197-223). Springer New York.
Sandvig, C. (2013). The internet as an infrastructure. The Oxford handbook of internet studies, 86-108.
Schneier, B. (2009). Schneier on security. John Wiley & Sons.
Sprankel, S. (2013). Technical basis of digital currencies. Working Paper.
Swan, M. (2015). Blockchain: Blueprint for a New Economy. " O'Reilly Media, Inc.".
Themelis, A. T. (2013). Information and Intermediation, Abuse of Dominance and Internet 'Neutrality':'Updating'Competition Policy under the Digital Single Market and the Google Investigations (?). European Journal of Law and Technology, 4(3).
Wainwright, H. (2006). "Imagine There's No Leaders." in Z Magazine, October 9, p. 3.
Ziccardi, G. (2012). Resistance, liberation technology and human rights in the digital age (Vol. 7). Springer Science & Business Media.
Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.