Privacy and anonymity in Bitcoin

Andrea Merlina

July 5, 2019

1 Introduction

I claim that we should favor the development of any tool that increases privacy and at the same time regulate behavior and misbehavior. I believe privacy to be a right of every human being and crucially important nowadays because of the increasingly technological and interconnected world in which we live in. Data, information and knowledge are exchanged faster and cheaper than any previous moment in human history. Those achievements open scenario that were unimaginable until recently and call for particularly thorough discussion since they require counterfactual lines of reasoning.

I am going to argue that privacy is something we must refrain to give up easily because there are real world situations that require hiding information to prevent injustice and harm. Privacy becomes thus a moral value to be defended, as it shields from injustice and mistakes. The discussion becomes thorny when privacy conflicts with other values such as security and accountability. I believe the answer cannot be devoid of any contextual information, especially acknowledging the mutability of such values. As a consequence, tracing a decision border is a task that I cover only superficially.

I will illustrate my claim and guide the reader first introducing Bitcoin, focusing on its anonymity aspect, then I will present ways that such technology has been misused and argue for regulations. We might wonder why not to suppress Bitcoin at all. I counter this line of reasoning presenting motivations and examples that support the existence of privacy-preserving payment systems, explaining why they are still valuable in our society and why we should defend them.

I conclude saying that because of the illustrated examples and possibly more yet to emerge thanks to the advancement of technology, there are reason to justify the development of anonymous payment systems, which might benefit the whole society if well regulated.

2 Background

2.1 Privacy and anonymity

Privacy is a concept familiar to most of us and still hard to define in its meaning and value, as shown by lack of consensus on those matters [7]. The debate about privacy appeared first in 1890 when Warren and Brandeis started arguing about a "right to be left alone" [26]. By no chance this was the period of time the world got to experience the introduction of press and photography. For our purpose we can think of informational privacy as of control on our own information [14] and that it is related to the concept of personal intimacy as a mean to "protect the extent to which one's thoughts, sentiments, and emotions could be shared with others" [6]. Some degree of privacy protection has been part of common law and moral customs, but with the advancement of technology it is becoming increasingly important to explicitly and separately recognize its value.

Anonymity can be regarded as a mean to achieve privacy, in which no personal identifiable information or knowledge about the subject is disclosed to others, thus preventing the establishment of any relationship between subjects themselves and their actions. As we are going to detail in Section 2.2, Bitcoin [16] is an electronic payment system that offers high degree of anonymity. Its popularity justifies the choice to approach the subject of anonymous payment systems through the lenses of Bitcoin. For the sake of completeness, [6] citing Gavison [18] refers to anonymity as one out of three way to obtain privacy, the others being secrecy and solitude. As mentioned, we are going to focus on anonymity while for their definition we defer to the original text.

2.2 Bitcoin, the power of money and accountability

I have previously introduced Bitcoin but I would like to take a step back and talk about a strictly related technology, the blockchain. Meaning and relationship between the two will be clearer at the end of the passage.

Blockchain is a recent advancement in the field of distributed computing systems that brought scientific and technical innovation, and discussion about its social and ethical impact along with it. To put it simply, the blockchain, as suggested by the name, is a sequence of blocks. Each block is linked with the previous and the following one, hence the term chain. This chain is formed and managed by a network of nodes which communicate exchanging messages as the purpose is to agree on the state and the evolution of the state, represented by the chain itself. The state is important because is regarded as the shared and

transparent truth of the system. For instance, in blockchains used for crypto currency systems (as in Bitcoin), the state encodes *who owns what and in which amount*. As mentioned, many nodes manage the blockchain and they do it by keeping their own copy of the chain. This is done because the participating nodes do not trust each other, thus avoid any kind of delegation, but they still need to cooperate to establish a state.

Important topic up for debate concerns privacy and anonymity of blockchains. In some kind of blockchain, users are not required to identify themselves and still are able to use the system. Those are called permissionless blockchain (as opposed to permissioned) and I am going to detail more about them, since it is an important aspect of the discussion.

Bitcoin, on the other hand, is a financial-oriented application based on the blockchain technology. Exemplifying to the extreme, we can say that a blockchain without Bitcoin do exist (indeed there are many open researches in this direction [13]), but there could not be Bitcoin without blockchain. Thus, it makes sense to keep a distinction between the two.

Bitcoin itself was launched in 2008 by a person (or perhaps a group of people) that as of today is still unidentified and who operated under the pseudonym of Satoshi Nakamoto. This is perfectly in line with the philosophy of Bitcoin as a decentralized and anonymous payment system. The system itself is very elegant and combines different well known elements with a few innovations that allow something that was not possible before 2008: pay somebody without revealing any personal information and without trust between the interacting parties [24]. It should appear evident the difficulty of devising such a system, where it is possible exchange digital money at a distance, anonymously and without trust. This is what Bitcoin does and the reason it got to be famous. The system is able to work because the selfish behavior of every participant that seeks to maximize its profits is perfectly tailored to make the whole system secure and functioning [16]. The essence of the process can be illustrated with a metaphor. We can imagine each node of the Bitcoin network competing against the others to win an endless relay race in which each running chunk takes on average 10 minutes to complete. This race started in 2008 and there is no set ending time. Differently from normal races though, a stochastic component prevents the fastest runner to win consistently chunk after chunk. We can assert that the fastest runner is simply more likely to win. Although everybody is selfishly interested to be the first to cut the finish line (and earn a monetary reward), losers are motivated to recognize they have lost that chunk of the race because doing so allows them to start running for the following chunk, which they might win this time. A node that does not follow the rules of the race is simply left behind without possibility to damage the progress the system.

Furthering our metaphor, is has been shown that as long as at least half of the runners follow the rules, the blockchain is secure [16]. In ten years of Bitcoin's activity, nobody proved otherwise. Key innovation in Bitcoin is that users are not forced anymore to identify themselves to spend and receive money, but instead of a name they use addresses. "32pdqr3MPD1MkcgmQgHfnCthqByV3E7iBq" is an example of a real address that everybody in complete autonomy is able to create and share with friends and colleagues. The owner of the address possesses the associated money and since (a) there is no capped limit to the number of addresses to be created and (b) it is fast and cheap to create and dispose of them, the result is a practical privacy-preserving money-exchange system [24].

3 Misuses of Bitcoin

In this section I am going to illustrate two examples of unethical and illegal uses of Bitcoin. It has been argued that unlimited privacy "functions negatively, as the cloak under which one can hide domination, degradation, or physical harm" [6] and assures no consequences for immoral or illegal actions. In that sense privacy prevents accountability in a deleterious way for societal norms. We might be brought to argue that identifying every owner of Bitcoin would deter illegal behavior, preventing the situations we are about to describe.

3.1 Silkroad

Silkroad was an online black market that operated between 2011 and 2013, selling different kind of items although it got famous mostly for selling illegal drugs [11]. Such marketplace developed thanks to Bitcoin as the payments system and the anonymity that it provided both for customers and sellers. The administrator of the platform, called by the nickname of Dread Pirate Roberts, has been arrested and sentenced to life in prison [9]. One of its declaration points out how Silkroad would not have existed without Bitcoin. Section 4 provide a short discussion of this case and its implications.

3.2 Ransomware

A ransomware is a computer program that infects its victim, ciphering the file system and asking for a ransom to decipher it. Cryptography has a long history, dating back to the Roman empire, Julius Caesar and the ciphering algorithm named after him [2]. Cryptography evolved throughout centuries as a way

to protect the confidentiality of our own private information. In the perverse, illegal but nonetheless innovative use of cryptography in ransomware, the paradigm is turned upside down, and the rightful owner of the information is prevented from accessing them. In the ill fated event of impossibility to recover the valuable information otherwise, the victim has no way out but to pay and hope. The amount to be paid is usually asked in Bitcoin or similar variation called altcoins. Researchers have shown that the most profitable ransomware profited more than two million dollars [8] to its creator. Worst of all, the malware targets critical infrastructures like hospitals, police and fire stations [22], posing a threat to public safety infrastructures.

4 Discussion on Bitcoin uses and misuses

It looks like the level of anonymity provided by Bitcoin allows nefarious actions and to some extent this is true and documented (see Sections 3.1 and 3.2). Those examples might point to the fact that anonymity implies impunity, but the story of Silk road teaches otherwise. After all, Dread Pirate Roberts is right now facing the consequences of his actions. Banning Bitcoin altogether, on the other hand, looks like a partial solution that does not take into account the positive aspects of an anonymous, border-less currency.

Venezuela's political and socioeconomic crisis started in 2010 and has caused marked inflation, crime and deaths. With a national currency that registered in 2018 an inflation level of 80.000% [10] and still loses its value from one day to the following, Venezuelan families are going through a lot a troubles even to buy food. As the economy is collapsing, payment systems that are not the inflated national currency cannot be used because of exchange controls. In such a situation, the anonymity of Bitcoin provided Venezuelans a way to access a more stable currency. To protect themselves from the inflation, families trade Bolivares and Bitcoin on a daily basis to buy milk and cheese [1].

As the example shows, there is room for ethical uses of anonymous currencies and I believe this morally justifies its development. On the other hand, abuses and misuses must not remain undetected, but investigated and punished. This requires a system of comprehensive and well structured regulations, in order to establish what is permitted and what is not. Regulations are already taking place all over the world. The most important online platforms to exchange fiat currency with crypto currency are deploying mechanism to identify their users by uploading documents, such as bank invoices and passport pictures. The resulting system goes against the original design of Satoshi Nakamoto but limits the possibility of

illegal activities and money laundering [4]. It is a necessary trade off to make national sovereignties accept cryptocurrencies. A deeper look shows how governments have gone a step further, establishing taxes on the possession of digital coins. Norway, for instance, classifies Bitcoin as an "asset" and demands the according taxation [20].

5 On defense of privacy

I want to argue now more generally about the value of privacy and draw connections to Bitcoin whenever possible.

Most people feel like privacy possesses something valuable that should not be given up altogether without thinking, but at the same time is hard to pin down what the valuable part actually is and its ethical implication. On this regard, philosophers are divided in mostly two categories. The first category supports the idea that high levels of privacy are dangerous and undesirable for society, while the other claim that privacy is backed by good moral reasons since it protects individuals [25]. Bitcoin's supporters fall obviously in the second category and my personal view as well. There are different reasons both practical and ethical.

First of all, most of the time we have no knowledge of the use that is made of our personal information. The scandal of Cambridge Analytica teaches how easily this can happen and how far it can go [15]. For example, let's consider an absolutely honest person called Daniel who complies to every rule and law, and perhaps most importantly behaves in a way we would consider morally unstained. We could argue that he might give up his right to privacy since there is nothing to hide and anything that could possibly damage him. Unfortunately, this is not true. Imagine that Daniel resembles very much a car thief who happen to steal a car of the same model as his own. He got stopped by the police, but the agent is having troubles with his wife and is not very understanding that day, moreover the shift change happens to be in a few minutes. Daniel is forced to spend one night in prison and his stay leaves and electronic trace in the police database. Fast forward 10 years. John is a recruiter in the Dream company, where Daniel is at the last stage of selection. It is out of the company's policies but John has a good friend at the police department who runs a check on Daniel for him. The arrest happened long ago and regards a minor issue but is enough for John to select a different candidate. Who is to blame about what just happened? The problem lies in the fact that although the collected information regards us, we have no control about how it is being used or, more importantly misused. As soon as it is collected and extracted, we have to

trust the data processor to act morally and fairly since it might cause unfathomable effects on the data subject. This motivates privacy as legal right and the employment of strategies to limit and control data processing.

We can draw a parallel between control on personal data and control over money. As soon as we do deposit money in a bank, we give up the control about how it is being used and invested. Clients still own their money (and perhaps even more thanks to interest rate), but there is no way to influence how it is going to be invested. Clients do not steer the allocation of the investment portfolio in a way they might believe to be more ethical. Banks are indeed for-profit organizations, driven by the maximization of return over investment (RoI). It comes to no surprise then that a few of them have been reported to invest in dubiously ethical industries as the weapon production [23]. In Bitcoin instead, there is no reliance on trust, by system design. The owner of Bitcoin is the only one authorized to move the coins, maintaining full control on the asset and spending as she pleases according to her moral values.

5.1 On surveillance, whistle-blowing and the relativity of privacy value

The second motivation to advocate about privacy is more subtle and deals with the psychology of human beings. The assumption here is that we value liberty and freedom of choice. Many democratic societies, indeed, have high regard for those values and they are taught in schools to children. Now imagine that somebody, a controller, watches you and does it constantly in time. This is consistent with the idea of giving up the right to privacy altogether. In such case, the human psyche comes into play. Since we are being observed and we are aware of it, a subtle psychological mechanism tries to identify us with the controller and as a consequence we unconsciously tend to do what we think pleases him. This description sketches the idea of Panopticon by Jeremy Bentham [12]. Lack of privacy or its limitation has repercussions to freedom, and more broadly to democratic societies. To some extent, this describes how totalitarian regimes happen to gain consensus and to reinforce themselves, strengthening their support through stricter and stricter control.

A famous and controversial case is Edward Snowden's leakage of classified information related to the surveillance program started by the American government following the September 11 terrorist attack [19]. Snowden is regarded both as a traitor of the country or an hero of privacy, depending on whom the question is asked, at any rate he undoubtedly raised awareness on the effects of the Patriot Act, the law that has been signed by President George W. Bush in less then two months after the attack [5].

I introduced Snowden's case to illustrate two points. First thing first, Snowden recently revealed that

"the servers used to leak thousands of documents to journalists were paid for using Bitcoin" [21]. The declaration shows how anonymous currencies can help enable and protect whistle blowers. It is likely that without servers, Snowden would have had harder time to snatch information and convince the world about what was going on.

The second point I want to bring forward thanks to Snowden and the example of the Patriot Act, is on the extremely mutable importance attributed to privacy relatively to other moral values, security in particular. The hideous terrorist attack struck America and swept away all objections about privacy protection to favor security. This has been the purpose and the underpinning philosophy of the Patriot Act when it got promulgated [5]. Two months were enough for a radical change in the legal consideration of privacy. This "liquidity" contributes to the difficulty to define privacy and its value once and for all. The described conflict between privacy and security applies to money flow as well, and anonymous payment systems like Bitcoin threatened the system. Not by chance, the American government was among the first to regulate crypto currencies with the introduction of a licence, which have been appropriately baptized BitLicence [17].

5.2 Awareness and context privacy as guidance for policies and regulations

Previously, I have claimed that privacy right concerns control over one self information. Obviously, such control is prevented if even the mere existence of personal data being collected is ignored by the data subject. Thus, it is of paramount importance the concept of awareness. Each person should understand and willingly consent to the treatment of personal data. National and European regulations, such as the General Data Protection Regulation (GDPR) [3], move steps in this direction. Starting from May 2018, the GDPR is a substantial achievement to set a uniform standard for privacy protection in several countries. This is especially important, considering that data is so easy to transfer regardless political border. It follows that the broader agreed-upon regulation, the better.

A borrower applying for a loan might expect the bank to inquire about his financial situation. Similarly, a doctor is likely and even welcome to ask about previous medical conditions if they could help the diagnosis. People are willing to disclose even extremely personal information if it appears resonable given the context. On the other hand, it feels a violation of privacy if there is a transfer of information across imaginary boundaries of competence. This concept is regarded as contextual privacy [14] or "spheres of justice and access" by Micheal Walzer [25].

I consider those two to be fair guiding principles to be followed in devising the regulations I have

been advocating so far. I do not argue surveillance is bad and privacy should always trump other values. What emerges throughout the whole argumentation is that privacy is a complex value intertwined with fairness and democracy and its importance ought to be recognized.

6 Conclusion

Anonymous payment systems are thorny and non-trivial applications of privacy related subjects. I believe of privacy itself to be of paramount importance, as the demand of personal data for different purposes is not going to subside but instead is more likely to raise in the future. We have established that anonymity can be put to use for both ethical and unethical purposes. Complete lack of privacy might cause harm or limit liberty and democratic principles that are at the heart of many modern societies, while at the same time its unconditioned and blind application provides room for impunity and prevents accountability. This applies both to the personal as well the financial sphere.

The conclusion is that anonymous payments as provided by Bitcoin can find good uses and as such, they must be regulated and protected. Striking a balance in the regulations is necessary for a fair system but acknowledged hard as well. The task of tracing the better trad off between guaranteeing privacy and assuring security remains an open question for the future and subject to individual cases. What is apparent though is that legislation is moving on, running as close as possible behind technology. In a word where data is extremely easy to generate in one place and transfer to the other side of the world, a global and unified law about data protection is what we should aim for.

References

[1] Bitcoin has saved my family. https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html. Accessed: 2019-06-19.

[2] Caesar cipher. https://www.cs.mcgill.ca/~rwest/wikispeedia/wpcd/wp/c/Caesar_cipher.htm. Accessed: 2019-07-03.

[3] General data protection regulation. https://gdpr-info.eu/. Accessed: 2019-06-16.

[4] Global money-laundering watchdog launches crackdown on cryptocurrencies. https://www.reuters.com/article/us-moneylaundering-crypto-fatf/

global-money-laundering-watchdog-launches-crackdown-on-cryptocurrencies-idUSKCN1TM1I8. Accessed: 2019-06-26.

[5] The patriot act: What is the proper balance between national security and individual rights? https://www.crf-usa.org/america-responds-to-terrorism/the-patriot-act.html. Accessed: 2019-06-27.

[6] Privacy. https://plato.stanford.edu/entries/privacy/. Accessed: 2019-06-16.

[7] Privacy and information technology. https://plato.stanford.edu/entries/it-privacy/. Accessed: 2019-06-16.

[8] True scale of bitcoin ransomware extortion revealed. https://www.technologyreview.com/s/610803/true-scale-of-bitcoin-ransomware-extortion-revealed/. Accessed: 2019-06-19.

[9] United states district court judgment in ross ulbricht criminal case. https://www.docketalarm.com/cases/New_York_Southern_District_Court/1--14-cr-00068/USA_v._Ulbricht/269/. Accessed: 2019-06-26.

[10] Venezuela's hyperinflation hits 80,000% per year in 2018. https://www.forbes.com/sites/stevehanke/2019/01/01/venezuelas-hyperinflation-hits-80000-per-year-in-2018/#656fbeb94572. Accessed: 2019-06-26.

[11] David Adler. Silk road: The dark side of cryptocurrency. https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/. Accessed: 2019-06-18.

[12] Jeremy Bentham. Panopticon, 1995 (1787). Edited by Miran Bozovic. London: Verso.

[13] J. Clark A. Narayanan J. A. Kroll J. Bonneau, A. Miller and E. W. Felten. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, 2015.

[14] Deborah G. Johnson. *Computer Ethics*. Pearson International Edition, 4 edition, x.

[15] Issie Lapowski. How cambridge analytica sparked the great privacy awakening. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/. Accessed: 2019-06-21.

[16] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf, 2008.

[17] Jose Pagliery. New york unveils bitcoin license rules. https://money.cnn.com/2014/07/18/technology/bitcoin-license. Accessed: 2019-06-27.

[18] Gavison R. Privacy and the limits of law, 1980. Yale Law Journal, 89: 421–71.

[19] Alan Rusbridger and Ewen MacAskill. Edward snowden interview. https://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript. Accessed: 2019-06-27.

[20] Maria Santos. Norway classifies bitcoin as an "asset" and announces a tax on cryptocurrency. https://99bitcoins.com/norway-classifies-bitcoin-as-an-asset-and-announces-a-tax-on-cryptocurrency/. Accessed: 2019-07-04.

[21] Thomas Simms. Edward snowden used bitcoin to pay for servers used in nsa leak. https://cointelegraph.com/news/edward-snowden-used-bitcoin-to-pay-for-servers-used-in-nsa-leak. Accessed: 2019-07-03.

[22] Annie Sneed. The most vulnerable ransomware targets are the institutions we rely on most. https://www.scientificamerican.com/article/the-most-vulnerable-ransomware-targets-are-the-institutions-we-rely-on-most/. Accessed: 2019-06-20.

[23] Jessica DiNapoli Tom Hals. U.s. banks provide rescue financing for gunmaker remington. https://it.reuters.com/article/companyNews/idUKKBN1H204F. Accessed: 2019-07-04.

[24] F. Tschorsch and B. Scheuermann. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys Tutorials*, 18(3):2084–2123, thirdquarter 2016.

[25] Jeroen Van Den Hoven. *Information Technology, Privacy, and the Protection of Personal Data*, page 301–321. Cambridge Studies in Philosophy and Public Policy. Cambridge University Press, 2008.

[26] S. Warren and L. Brandeis. The right to privacy, 1890. Harvard Law Review, 4: 193–220.