The Ideological Background of Bitcoin: The Unintended, but Predicted, Convenience of Anonymity for Criminal Activities

CARLA MARIA DE OLIVEIRA COSTARDI
Polícia Federal – Rio de Janeiro/RJ

ABSTRACT

Bitcoin, the first cryptocurrency and the first known application of Blockchain, is closely related to the countercultural movement called Cypherpunks. The activism of Cypherpunks, as stated in their manifesto, was – and still is – directed to developing tools to provide a virtual environment where privacy is protected. To them, privacy is not secrecy; privacy is the power to selectively reveal oneself to the world. Bitcoin is a direct outcome of this aspiration, as Satoshi Nakamoto – while developing Bitcoin – committed his efforts to produce an innovative software that reflected this ambition and was successful at developing one that, at once: (i) sheltered privacy through pseudo-anonymity, (ii) provided an unchangeable public ledger of all transactions completed with Bitcoin and (iii) challenged the state-centric monetary policy and the traditional banking system through a decentralized network of operating nodes functioning as validators of the information carried in the public ledger. In this article, through the establishment of relations between the Cypherpunk ideology and Bitcoin, the central argument is that the convenience of using Bitcoin in criminal activities is, originally, an unintended effect of the ideology that supported the development of cryptocurrencies but, more likely, a collateral risk the creator was willing to take.

Keywords: Bitcoin. Cypherpunks. Organized Crime. Terrorism. Privacy Protection.

Introduction

"We should shut down cryptocurrencies" warns the 2001 Nobel Prize winner, the economist Joseph Stieglitz (DAVIS,

2019). The reasons he states to support this claim, which he has made a few times before (BBC MUNDO, 2017; BLOOMBERG, 2017), are mainly related to cryptocurrencies' most controversial features: volatility and lack of transparency. In fact, as he argues that cryptocurrencies cannot be classified as a trustworthy currency and, additionally, that it encourages illegal financial activities – such as money laundering – by moving money off "from a transparent platform into a dark platform" (DAVIS, 2019).

Despite these severe accusations of providing a favourable environment to criminal activities, the first blockchain based cryptocurrency – Bitcoin – was not intended to do so. As a matter of fact, it stems from a countercultural movement that advocated for strengthening privacy: the Cypherpunks; not from a criminal organization. It is important to stress that, to these activists, "privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world" (HUGHES, 1993).

The question underlying this discussion is: was Bitcoin created for criminal purposes? The answer is not easy. In this article, the central argument is that, even though predicted, the use of Bitcoin in criminal activities is an unintended effect of the privacy protection design of Bitcoin, which stems from libertarian speeches made by Cypherpunks, in whose mailing list Satoshi Nakamoto decided to first reveal it to the world. Such an analysis is important because it historically places Bitcoin as a tool developed by cryptographers acting as activists in order to materialize their libertarian speech in the international system, made to defend one's privacy and confront the governmental control over daily personal activities. On the other hand, it is likely that the potential and actual use of Bitcoin in criminal activities was predicted – especially considering the actions intended against the governmental control of private individual life – but it was considered a minor issue when compared to the necessity to protect the individuals' right to privacy (MAY, 1988).

Despite the limitations of this research, which was made through the revision of primary and secondary sources and unable to

interview the developers of Bitcoin, the goal is to address and describe the idea behind the original development of the first cryptocurrency and how it relates to the technology that was developed and potential criminal activity. To this purpose, the relations between the Cypherpunk ideology and Bitcoin will be illustrated throughout a historical and conceptual outline.

The beginning

> *"Crypto moves fast"*
> *(BURNISKE; TATAR, 2018)*

Bitcoin, the first of blockchain-based cryptocurrencies, was highly influenced by the countercultural movement known as Cypherpunks. It is also the most successful result of a number of different intents of creating anonymous electronic means of payment.

Before Bitcoin's blockchain, cryptographers around the world were working on creating anonymous and cryptographed electronic means of payment. The first modern alternative to cash was the Diners Card, back in the '50s (SIMMONS, 2016), which was already a revolution by itself, being the first of credit cards and forever changing how humanity related to cash. In turn, cryptography entered the equation some decades later, when some developers envisioned its use in virtual financial transactions in the internet environment (CHAUM, 1985).

The most renowned digital currency before Bitcoin was created by David Chaum in 1989 using the DigiCash protocol, in which the currency was called "ecash"(CHAUM; FIAT; NAOR, 1988). It shared some of Bitcoin's most important features: the anonymity of users (but not of merchants) and a cryptographic authentication similar to the proof-of-work used by Bitcoin. On the other hand, contrary to Bitcoin, it required a centralized server as a central authority. Despite that, it was a groundbreaking development and David Chaum was able to promote and patent the technology, which was used experimentally by some banks in the United States and Finland (NARAYANAN *et al.*, 2016). On this matter, the picture

Burniske and Tartar (2018) draw on Chaum's character and how he handled the ecash episode is curious:

> *However, while Chaum was widely regarded as a technical genius, as a businessperson he left much to be desired. Bill Gates approached Chaum about integrating e-cash into Windows 95, which would have immediately given it global distribution, but Chaum refused what was rumored to be a $100 million offer. Similarly, Netscape made initial inquiries about a relationship, but management was quickly turned off by Chaum's attitude. In 1996, Visa wanted to invest $40 million into the company but were dissuaded when Chaum demanded $75 million (if these reports are correct, it's clear that the potential price for Chaum's creation was dropping).*
>
> *If all had gone well, DigiCash's ecash would have been integrated into all our web browsers at the ground floor, serving as the global Internet payment mechanism and potentially removing the need for credit cards in online payments. Sadly, mismanagement ultimately ran DigiCash into the ground, and in 1998 it declared bankruptcy. (p. 34)*

There were some other enterprises on this matter, but none as successful. The e-gold was one of them and, after a few years of operation, the U.S. Department of Justice indicted the company that carried e-gold and three of its owners on 2007, under the accusation of conspiracy to launder monetary instruments, conspiracy to operate an unlicensed money transmitting business, among others (U. S. DEPARTMENT OF JUSTICE, 2007). The Attorney General's Office argued that "the E-Gold payment system has been a preferred means of payment for child pornography distributors, identity thieves, online scammers, and other criminals around the world to launder their illegal income anonymously" (DEPARTMENT OF JUSTICE, 2007).

Bitcoin was a product of this context. Its developer, Satoshi Nakamoto (or group of creators[1], as some believe it to be) chose to use *The Cryptography Mailing List* to broadcast the result of his work (NAKAMOTO, 2008a, 2008b). Through it, they debated the social and political changes they wanted to implement employing cryptography. Every participant had the chance to be anonymous, and the mailing list was made operative by a cryptographed mailing server

1 For the purposes of this article, Satoshi Nakamoto will be referred to as a male individual.

(NARAYANAN *et al*., 2016). As Timothy May (1994) explains:

> *The Cypherpunks group was mainly formed by Eric Hughes, John Gilmore, and me. It began with physical meetings in the Bay Area and elsewhere and with virtual meetings on an unmoderated mailing list. The name was provided by Judith Milhon as a play on the cyberpunk fiction genre and the British spelling of cipher. The mailing list can be subscribed to by sending the single message, subscribe cypherpunks, in the body of a message to majordomo@toad.com. Expect at least fifty messages a day. About six hundred subscribers in many countries are presently on the list. Some are pseudonyms. (p. 10)*

When Satoshi Nakamoto posted his first announcement of Bitcoin and its respective White Paper[2] (NAKAMOTO, 2008a, 2008b) at *The Cryptography Mailing List*, only some of the members paid him attention. However, it is now largely believed to be one of the most disruptive financial enterprises after the credit card. His creation (Bitcoin and the technology supporting it), nevertheless, reflected the ideological aspirations of Cypherpunks concerning information management, privacy protection and the challenge of the government control of individuals. This technology is currently known as *Blockchain;* its original version is the Bitcoin's blockchain, from which most of the new cryptocurrencies started and most of the latest projects involving Blockchain – such as smart contracts, newly designed voting and banking systems, to name a few – have drawn on.

Bitcoin and Cypherpunks

> *"In fact, technology represents one of the most promising avenues available for re-capturing our freedoms from those who have stolen them"(HAMMILL, 1987)*

In a very brief account, "Cypherpunks were activists who opposed the power of governments and centralized institutions, and sought to create social and political change through cryptography" (NARAYANAN; CLARK; HAVE, 2017). Or, as Julian Assange, a self-declared cypherpunk, defined: "Cypherpunks are activists who advocate the mass use of strong cryptography as a way protecting our basic freedoms against this onslaught." (ASSANGE *et al*., 2012)

2 According to Merriam-Webster (2019), White Paper is defined as "a detailed or authoritative report".

Founder of the Crypto Anarchy movement and a founding member of the Cypherpunks, Timothy May recollects that it all goes back to September 1992, when about 20-25 members got together in Eric Hughes' house for Cypherpunks' inaugural meeting (MAY, 2016). In this gathering, May read the Crypto Anarchist manifesto (MAY, 1992), which was sent to all members on November 1992 through *The Cryptography Mailing List*, along with *the Crypto Glossary* (HUGHES; MAY, 1992). The fact that the Crypto Anarchist manifesto[3] was an object of discussion in the inauguration of the Cypherpunks indicates that the latter shared part of the Crypto Anarchist ideology, synthesized by Peter Ludlow (2001):

> *Crypto anarchy is a phrase initially coined by Timothy C. May (chapters 6 and 7) to describe a possible (inevitable?) political outcome from the widespread use of encryption technologies like Pretty Good Privacy. The leading idea is that as more and more of our transactions take place behind the veil of encryption, it becomes easier and easier for persons to undertake business relations that escape the purview of traditional nation states. For example, not only will certain "illegal" transactions become more widespread (or at least easier to carry out), but nation states will find it increasingly difficult to enforce their taxation laws. Indeed, full-fledged black-market economies may emerge that will eventually become larger and more vibrant than the legitimate economies that are controlled by the nation states" (p. 5-6)*

Shortly after the first meeting, on March 17th, 1993, T*he Cryptography Mailing List* was used to broadcast *A Cypherpunk's Manifesto* by Eric Hughes (1993):

> *From: Eric Hughes hughes@soda.berkeley.edu*
>
> *Date: Wed, 17 Mar 93 11:54:59 PST*
>
> *To: cypherpunks@toad.com*

3 The Crypto Anarchist manifesto was originally written in 1988 and states: "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation" (MAY, 1992).

Subject: RANTS: A Cypherpunk's Manifesto

Message-ID: <9303171951.AA18216@soda.berkeley.edu>

MIME-Version: 1.0 Content-Type: text/plain

[...]

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

[...]

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

[...]

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

[...]

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

This manifesto's fundamental claim is, therefore, the defence

of privacy – understood as the faculty of revealing one's identity only when desired. It makes it clear that the role of Cypherpunks is writing code, in other words, programming to create softwares capable of protecting privacy and building anonymous systems.

In this sense, when confronting the Crypto Anarchist Manifesto to the Cypherpunks', it is possible to deduce that the cypherpunks perform the operative work necessary to enforce the new world order that crypto-anarchists envisioned to be carried out via encryption. In consequence, not only because both groups were founded by Timothy May and seek the same socio-political revolution, but also because they work together as a team, Cypherpunks are, indeed, crypto-anarchists.

From another perspective, Narayanan deepens the analysis by associating the cypherpunks beliefs to the creation of Bitcoin (NARAYANAN, Arvind *et al.*, 2016):

> *In any event, early work in that area came together with cypherpunk beliefs—in particular, the desire to have a strong currency that would be decentralized, online, and relatively private—to sow the seeds from which Bitcoin would be born. It's also the basis for the philosophy that many of Bitcoin's supporters follow. (p. 342)*

The inspiration in the cypherpunks ideals is probably the reason why, in the development of Bitcoin, pseudo-anonymity and transaction privacy have always been the greatest aspirations of Satoshi Nakamoto. At this point, one clarification is needed: it is yet unclear who the actual developer (or group of developers) was; the only certainty is that one Satoshi Nakamoto signed the Bitcoin's White Paper and, also, used the Cypherpunks' mailing list (at that time named *The Cryptography Mailing List*) to broadcast it and discuss its impacts during a brief period (NAKAMOTO, 2008a, 2008b, 2009). Indeed, the possible use of a pseudonym[4] by Bitcoin's creator is coherent with the Cypherpunks ideology of protection of privacy. In addition to that, there might have been some extra incentives of self-preservation not to unveil Satoshi Nakamoto's real identity, as speculated by Jacob Appelbaum and Julian Assange (ASSANGE *et al.*, 2012):

4 In spite of many attempts (KHARIF, 2019; SCHUIL, 2016; VILNER, 2019), the identity of Satoshi Nakamoto is still unknown.

> **Jacob:** *[...] There is a reason why the person that created another electronic currency, Bitcoin, did so anonymously. You do not want to be the person that invents the first really successful electronic currency.*
>
> **Julian**: *The guys who did e-gold ended up being prosecuted in the U.S. (p. 94)*

As mentioned before, owners and proprietors of e-gold were indicted by the U.S. Department of Justice for, among other accusations, *conspiracy to engage in money laundering* (U. S. DEPARTMENT OF JUSTICE, 2007; ZETTER, 2009).

It is also worth mentioning that the model designed by Satoshi Nakamoto chooses an unobvious system to guarantee privacy: a *public record of information*, but with protection to the privacy of the parties involved:

> *The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. (NAKAMOTO, 2008a, p. 6)*

As he goes on with an explanation of his model, Satoshi clearly states his intention to protect the privacy of users and points out one vulnerable aspect of the idealized system: "the risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner"(NAKAMOTO, 2008, p. 6). This revelation can either be deliberate or not; in the latter, it is the consequence of an unintended action. When intentional, Satoshi Nakamoto leaves up to the users the choice of creating a public key identifying themselves with their true identity or using a pseudonym, a feature that is coherent with the Cypherpunks' definition of privacy mentioned before.

As a known Bitcoin's user and notorious Cypherpunk, Julian Assange (ASSANGE *et al*., 2012) summarizes the design of this cryptocurrency:

> **Julian:** *Bitcoin is a very interesting hybrid, as the account holders are completely private and you can create an account at will, but the transactions for the entire Bitcoin economy are completely public. And that is how it works; it needs to be that way in order for everyone to agree that a transaction has occurred, that the sending account now has less money and the destination that much more. That's one of the few ways to run a distributed currency system that doesn't require a central server, which would be an attractive target for coercive control. It is the distribution that is really innovative in Bitcoin, and the algorithms that permit that distribution, where you do not trust any particular part of, if you like, the Bitcoin banking network. Rather the trust is distributed. And enforcement is not done through law or regulation or auditing, it is done through the cryptographic computational difficulty that each part of the network has to go through to prove that it is doing what it claims. So the enforcement of honest Bitcoin "banking" is built into the architecture of the system. (p.97)*

Following Bitcoin, more than 3 thousand altcoins (here defined as any cryptocurrency developed based on Bitcoin's source code) have been crafted and negotiated (COINMARKETCAP.COM, 2020). Some with highly regarded prospects backing them up, such as Ethereum, Ripple, Litecoin, Tether, Monero, Dash, to name just a few. There have also been companies, and even countries, that dared to explore and innovate in this territory, such as Kodak, Venezuela and, more recently, Facebook (CHRISTINE KIM, 2018; DANIEL PALMER, 2019a, 2019b)

Nonetheless, little over ten years after the inauguration of the first cryptocurrency, Bitcoin remains the most valuable crypto asset among all others that followed it. By October 1st, 2020 (COINMARKETCAP.COM, 2020), the market value of Bitcoin ($196.637.284.601) exceeded almost five-fold that of Ethereum ($40.192.626.028), which is the second most valued crypto asset. Perhaps more illustrative than this figure is the notion that, if combined with the market values of the ten most valued cryptocurrencies after Bitcoin, on this same day, the total sum reaches nearly half of the market value of the Bitcoin in U.S. dollars.

If the market value is not enough of a reason to highlight it from its peers, Bitcoin has another unique feature: its developer –

Satoshi Nakamoto – disappeared shortly after 2010. According to Burniske and Tartar (2018a):

> *Shortly after, Satoshi vanished. Some speculate it was for the good of Bitcoin. After all, being the creator of a technology that has the potential to replace much of the current financial system is bound eventually to invoke the wrath of powerful government and private sector forces. By disappearing into the ether, Satoshi removed the head of Bitcoin, and with it a single point of failure. In his wake stands a network with thousands of access points and millions of users. (p. 9)*

With that, Satoshi made materially real the decentralization of Bitcoin, which he had already projected in his source code and announced when he presented the Bitcoin White Paper: "It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. [...] The result is a distributed system with no single point of failure." (NAKAMOTO, 2009). Besides, the unlikelihood of identifying or even locating Satoshi protected not only himself, but also made Bitcoin a system shielded from the creator's direct interference and, too, less vulnerable to governmental interference, one of the main goals of Cypherpunks.

It is important to stress that Satoshi himself, during a discussion held in The Cryptography Mailing List with an anonymous party, made clear his political aspirations (NAKAMOTO, 2008c, p. 1):

> *Re: Bitcoin P2P e-cash paper*
>
> *Satoshi Nakamoto Fri, 07 Nov 2008 09:30:36 -0800*
>
> *[...] >>You will not find a solution to political problems in cryptography.*
>
> *Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years.*
>
> *Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.*
>
> *Satoshi*
>
> ---
>
> *The Cryptography Mailing List*

With this message, Satoshi expressed that the main goal was to undermine the government's power over virtual settings, so that it could be a "new territory of freedom" (NAKAMOTO, 2008c, p. 1). And that is, again, coherent with the Cypherpunks ideology exposed on their Manifesto.

While on this subject, it is the fact that Satoshi conceived the Bitcoin as a distributed system that makes it highly resilient to external attacks, including law enforcement potential intents to shut it down. That, networks to have the ability to survive, is also a feature desired by these activists. It is important to note that Satoshi's idea of a distributed system is completely aligned with Paul Baran's[5] conclusion in his paper on the resilience of communication networks. In this paper, the distributed system has been characterized as the system that is more likely to resist external destructive attempts, that is, the one that was more likely to survive (BARAN, 1962).

This author, in his seminal paper On Distributed Communications Networks (BARAN, 1962, p. 2) defines survival as:

> *This communications network shall be composed of several hundred stations which must intercommunicate with one another. Survivability as herein defined is the percentage of stations surviving a physical attack and remaining in electrical connection with the largest single group of surviving stations. This criterion is a measure of the ability of the surviving stations to operate together as a coherent entity after attack.*

And he goes on to explain his concern with the question of system security:

> *We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable structures can be built – even in a thermonuclear era. In order to build such networks and systems we will have to use a large number of elements. [...] To design a system that must anticipate a worst-*

5 Paul Baran, aside of a being a pioneer in the development of computer networks and a researcher at RAND Corporation, had huge influence in the design of internet as we know it (RAND CORPORATION, s. d.).

> *-case destruction of both enemy attack, and normal system failure [...]" (BARAN, 1962, p. 18)*

The parallelism between Baran's theory of "several hundred of stations which can intercommunicate with one another" (BARAN, 1962, p. 2) and Satoshi's conception of peer-to-peer nodes is evident (NAKAMOTO, 2008a), in ways that – directly or indirectly – the latter nourished from this concept. It is also an indication that the purpose Satoshi pursued was the survivability of Bitcoin's network, essential to provide a trustworthy monetary system.

On the other hand, an unexpected practical result from Satoshi's incentives embodied in Bitcoin's source code, though, is that it has generated some degree of centralization (here understood as the decrease of the system's distribution). That, of course, could affect the survivability of Bitcoin's network against external attacks (HEILMAN, *et al*., 2015), potentially coming from agents who want to change the public ledger (in what could be interpreted similarly to a bank robbery) or from law enforcement trying to shut Bitcoin down, for example.

The decrease of the degree of centralization of Bitcoin's network is pointed out in academic papers and crypto-specialized media articles indicating that this fact is mostly due to the creation of mining pools and the unforeseen use of exchanges in bitcoin transactions (BALAJI S. SRINIVASAN, 2017; BONNEAU *et al.,* 2015; GENCER *et al*., 2018; KARAME; ANDROULAKI, 2016; ORCUTT, 2018; POON; DRYJA, 2016). Nevertheless, despite these findings, Bitcoin remains mainly a distributed system (GENCER *et al*., 2018).

In that respect, it is important to clarify that *decentralization* is referred here not only as a feature that presupposes *distributed system,* where there are no designed central or intermediate servers, as in the case of Bitcoin's peer-to-peer network. Decentralization also supposes the lack of a central authority, assuring the impossibility of external interference.

In what concerns the lack of central authority, also, decentralization is not an omnipresent feature among cryptocurrencies and crypto-assets. For example, mostly all attempts made by governments

to create their State-sponsored cryptocurrencies, even though having a distributed system, are centralized because they are designed to have a central governmental authority that controls it (CHOHAN, 2018, 2020). As a matter of fact,"[c]ountries that are piloting blockchain-based technology to create their own cryptocurrencies are experimenting with varying degrees of centralization and control, involving national government-backed cryptocurrencies to central bank–issued cryptocurrencies with collaboration with private firms" (KETHINENI; CAO, 2019, p. 328).

With the description made in this section, my goal was to draw on the technological aspects of Bitcoin that related to the Cypherpunk ideology. In a few words, the highly complex and innovative technology developed by Satoshi Nakamoto was able to materialize the aspirations of this group, such as pseudo-anonymity, decentralization and cryptographic authentication of transactions, all aiming to provide a protected environment from the government to private interactions.

In the following section, the convenience of Bitcoin's technical and ideological assemblage to criminal activity will be further debated.

Crime Seizes Opportunity

> *"Certainly, some of the earliest adopters of Bitcoin were criminals"*
>
> *(BURNISKE; TATAR, 2018)*

Now that the connections between *Bitcoin, Blockchain* and the *Cypherpunks* are somewhat more evident and the ideological background that justifies Bitcoin's development is further exposed, it is easier to understand the kind of threat it poses to public security. The operative costs deriving from its high volatility and defect of liquidity are costs that, somehow, outlaws are willing to pay in order to either launder their revenue or anonymously finance their criminal activities.

In a recent study about the illegal use of cryptocurrencies, the authors concluded that:

> *Among the virtual currencies, BTC is the dominant crypto-currency used in criminal activities because of its high value and faithful followers. Most of the crimes involving BTC are property crimes, although Silk Road, Alpha Bay, and Hansa platforms are used for money laundering, drug trafficking, hacking, sex trafficking, and human trafficking. However, traditional crimes such as kidnapping, murder, and extortion are slowly becoming part of the cryptocurrency world" (KETHINENI; CAO, 2019, p. 337)*

Although relevant due to its methodology, this is not an unexpected finding. The possibility of Bitcoin's features providing a convenient setting for criminal operations was not unpredicted. On the contrary, when referring to the possible effects of encrypted systems (such as Bitcoin), the Crypto Anarchist Manifesto is candid:

> *The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy. (MAY, 1992)*

In this same spirit, the Cypherpunks' Manifesto expresses their disregard for those that do not agree with their actions: "We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down. (...) *We will not, however, be moved out of our course because some may disagree with our goals*" (HUGHES, 1993).

Both speeches imply that, to Crypto Anarchists and Cypherpunks, there is no asset more valued than privacy. To defend it and enable its exercise through encryption, they were willing to consent to criminal activity as a collateral consequence of their primary objective.

In addition to the features that were initially put together in Bitcoin's design (most notably pseudo-anonymity, decentralization, public and immutable ledger), scholars have found that, in practice,

there are several other incentives to the criminal use of it. From the transactional point of view, incentives can derive from the irrevocable nature of transactions, the ease of international portability, the almost immediate completion of transactions (when compared to the time required by banks), and low transaction costs (BRENIG; ACCORSI; MÜLLER, 2015). Also, after examining the case of Silk Road, Kathineni, Cao and Dodge (2018) concluded that "[f]our factors—identity and flexibility, dissociative anonymity, ease of associating in cyberspace, and lack of deterrence—were found to facilitate Darknet illegal business" (p.150).

In contrast to the transactional incentives mentioned above, a competing perspective is that cryptocurrencies, in general, are much more traceable than cash itself (ROGOFF, 2017). Cash is considerably more anonymous since it does not demand any register or leave any virtual footprint to be analyzed and linked to each other in the future as do cryptocurrencies in general. Nevertheless, it cannot be easily transported, and this particularity significantly increases the risk of law enforcement searches and the costs related to internationally transferring cash.

With that in mind, the story of the cases of illegal use of anonymous means of payment has the same constant: where entrepreneurs and activists envisioned opportunities, so did criminals. One example of that is the indictment mentioned above of the business that carried e-gold. While the idea of its developers was to provide a secure environment for private transactions, the illegal activities executed by the anonymous users were related to heinous crimes, such as human slavery, children pornography, among others (DEPARTMENT OF JUSTICE, 2007). That was before Bitcoin, and even without all the security and privacy design that Bitcoin has, criminals found it attractive.

When Bitcoin came into the picture, the convenience was readily recognized. And, even though Ross Ulbricht was only a college boy with some coding abilities and a deep interest in the libertarianism and marihuana, he envisioned the possibility to materialize his beliefs of individual's right to use drugs without governmental interference and, at the same time, supposedly get rid of the risk involved in buying

drugs from dealers (BILTON, 2017). In his trial, he said:

> *I remember clearly why I created the Silk Road," Mr. Ulbricht said. "I wanted to empower people to be able to make choices in their lives, for themselves and to have privacy and anonymity.*
>
> *I'm not saying that because I want to justify anything that's happened. I just want to set the record straight, because from my point of view, I'm not a selfcentered sociopathic person that was trying to express some kind of inner badness. I just made some very serious mistakes. (WEISER, 2015)*

Although Ross Ulbricht was not a self-declared cypherpunk, his statement is an example of such speech. Also, his intentions might not have been that of becoming a criminal. Still, the direct effect of them was that he designed – with a little help from his friends – an illicit marketplace comparable to Amazon, providing an anonymous environment initially designed to link drug providers directly to consumers. The market was named *The Silk Road* and consisted of an anonymous interface in the *darknet*[6] that could only be accessed through the Tor browser. What even himself did not expect was that criminals would also be very interested not only in the environment he designed but also in receiving payments anonymously in Bitcoin (LACSON, 2016).

Ulbricht was arrested and sentenced to life in prison in 2015 (WEISER, 2015).

These two cases are examples that happened either before or during Satoshi's creation and first years of Bitcoin operation. They put into evidence that the illicit use of tools like Bitcoin was predictable and predicted. In fact, both Timothy May and Eric Hughes were candid about the probability of illegal use of the anonymous payment systems that carried the features Bitcoin did. Bitcoin was created in this context and its White Paper was first made available to cypherpunks. Considering that Satoshi was part of this community of activists, he was likely aware of both May's and Hughes' prediction of criminal use of instruments like Bitcoin, as well as the cases that preceded its

6 The Tor darknet is designed to avoid a central stable repository of existing sites. In contrast to the conventional internet, there are no easy website registries where one might look up information on who is managing what website and where they are registered as doing so (MOORE; RID, 2016).

operation (i.e. e-gold, ecash). Nevertheless, no changes were made either to prevent or to counter the use of Bitcoin in illicit transactions.

Conclusion

As argued before, the use of Bitcoin for criminal enterprises was not unpredicted or, better said, unknown. In the context of Bitcoin's creation, it was accepted as a risk worth taking considering the benefits of privacy protection against government interference in private transactions (highly desired by Cypherpunks) that it provided.

Where entrepreneurs and activists envisioned opportunities, so did criminals. Lawbreakers could and did easily recognize the convenience of this ideological structure to their endeavors, either because of the difficult traceability of transactions due to privacy protection mechanisms, or because of increasing liquidity of the cryptocurrencies market, among other reasons. It is clear that Bitcoin also created opportunities for criminals to conceal their activity (KETHINENI; CAO, 2019, p. 329).

It is uncertain if Satoshi Nakamoto consciously decided to provide a secure private environment not only to good citizens that wanted to have their privacy respected and protected, but also accepted the risk of offering incentives to the illicit use of this new currency. He never wrote about it on the documents archived in internet forums. But he did make public his intention of gaining "a new territory of freedom" by excluding government control of peer-to-peer networks, as he did with Bitcoin (NAKAMOTO, 2008c). Despite that, as debated in the last section of this article, some outlaw activities were morally tolerable in the context of privacy protection and of the attempts made by cryptographers to defy the statecentric world order.

In future works, I believe it to be useful to explore the impact Bitcoin had in the international system in terms of its relationship with law enforcement institutions and the government itself. Such a work, focusing on the international cooperation on this matter, would enlighten actors about possible next steps to increase enforcement of their legal measures to prevent and investigate crimes committed

with cryptocurrencies. This goal could be reached either aiming at evaluating the effectiveness of the actions already taken, or at identifying possible loopholes that could be explored in order to prevent its use by criminals.

Carla Maria De Oliveira Costardi

Delegada de Polícia Federal

Mestranda em Assuntos Internacionais pela Universidad Externado de Colombia e Doctoranda em Ciências Jurídicas pela Pontificia Universidad Javeriana

O Antecedente Ideológico da Bitcoin: A Conveniência não Intencional, mas Prevista, do Anonimato para Atividades Criminosas

RESUMO

Bitcoin, a primeira criptomoeda e a primeira aplicação conhecida do Blockchain, está relacionada de perto com o movimento contracultural chamado Cypherpunks. O ativismo dos Cypherpunks, como consta em seu manifesto, foi – e ainda é – dedicado ao desenvolvimento de ferramentas para proporcionar um ambiente em que a privacidade seja protegida. Para eles, privacidade não é sigilo; privacidade é o poder de se revelar seletivamente para o mundo. Bitcoin é um resultado direto dessa aspiração, já que Satoshi Nakamoto – enquanto desenvolvia a Bitcoin – empenhou seus esforços para criar um software inovador que refletisse essa ambição e foi bem sucedido no desenvolvimento de um que, de uma só vez: (i) abrigou a privacidade através do pseudoanonimato; (ii) forneceu um registro público inalterável de todas as transações concluídas com Bitcoin; e (iii) desafiou a política monetária estadocêntrica e o sistema bancário tradicional através de uma rede descentralizada de nós operacionais que funcionam como validadores das informações contidas no registro público. Neste artigo, por meio do estabelecimento de relações entre a ideologia Cypherpunk e Bitcoin, o argumento central é que a conveniência do uso do Bitcoin em atividades criminosas é, originalmente, um efeito não intencional da ideologia que lastreou o desenvolvimento das criptomoedas mas, provavelmente, um risco colateral que o criador estava disposto a correr.

Palavras-Chave: Bitcoin. Cypherpunks. Crime organizado. Terrorismo. Proteção da privacidade.

El Trasfondo Ideológico del Bitcoin: La Conveniencia no Intencionada, pero Predicha, del Anonimato para Actividades Delictivas

RESUMEN

Bitcoin, la primera criptomoneda y la primera aplicación conocida de Blockchain, está estrechamente relacionada con el movimiento contracultural llamado Cypherpunks. El activismo de los Cypherpunks, como se indica en su manifiesto, estaba, y sigue estando, dedicado al desarrollo de herramientas para proporcionar un entorno donde la privacidad esté protegida. Para ellos, la privacidad no es secreto; la privacidad es el poder de revelarse selectivamente al mundo. Bitcoin es un resultado directo de esa aspiración, ya que Satoshi Nakamoto, mientras desarrollaba el Bitcoin, prometió sus esfuerzos para crear un software innovador que reflejara esa ambición y tuvo éxito en el desarrollo de uno que, en uno solo momento, (i) albergaba la privacidad a través del pseudoanonimato, (ii) proporcionó un registro público inalterable de todas las transacciones completadas con el Bitcoin y (iii) desafió la política monetaria centrada en el estado y en el sistema bancario tradicional a través de una red descentralizada de nodos operativos que actúan como validadores de la información contenida en el Registro Público. En este artículo, al establecer relaciones entre la ideología Cypherpunk y el Bitcoin, el argumento central es que la conveniencia de usar el Bitcoin en actividades delictivas es originalmente un efecto no intencionado de la ideología que sustenta el desarrollo de las criptomonedas, pero probablemente un riesgo colateral que el creador estaba dispuesto a asumir.

Palabras Clave: Bitcoin. Cypherpunks. Crimen organizado. Terrorismo. Protección de la privacidad.

.

References

ASSANGE, Julian *et al*. Cypherpunks. New York: OR Books, 2012. E-book. Disponível em: http://ebookcentral.proquest.com/lib/bibliojaveriana-ebooks/detail.action?docID=4535983

BALAJI S.; SRINIVASAN. Quantifying Decentralization - news.earn.com. [s. l.], 2017. Disponível em: https://news.earn.com/quantifying-decentralization-e39db233c28e.

BARAN, Paul. On Distributed Communications Networks. RAND

Corporation. Santa Monica: [s. n.], 1962. Disponível em: https://www.rand.org/pubs/papers/P2626.html.

BBC MUNDO. Por qué el Premio Nobel de Economía Joseph Stiglitz cree que se deben prohibir los bitcoins. [s. l.], 2017. Disponível em: http://www.bbc.com/mundo/noticias-42196322.

BLOOMBERG. ¿Qué opinan los premios Nobel de Economía sobre el bitcoin?. [s. l.], 2017. Disponível em: http://www.portafolio.co/economia/ganadores-del-nobel-en-estan-en-desacuerdo-con-el-bitcoin-512239.

BONNEAU, Joseph *et al*. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security & Privacy, [s. l.], p. 104–121, 2015. Disponível em: https://doi.org/10.1109/SP.2015.14

BRENIG, Christian; ACCORSI, Rafael; MÜLLER, Günter. Economic Analysis of Cryptocurrency Backed Money Laundering. [s. l.: s. n.]. E-book. Disponível em: http://aisel.aisnet.org/ecis2015_crhttp://aisel.aisnet.org/ecis2015_cr/20. Acesso em: 5 out. 2020.

BURNISKE, Chris; TATAR, Jack. Cryptoassets : the innovative investor's guide to bitcoin and beyond. [S. l.: s. n.]. E-book.

CHAUM, David. Security without identification: transaction systems to make Big Brothe obsolete. Communications of the ACM, [s. l.], v. 28, n. 10, 1985. Disponível em: https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf

CHAUM, David; FIAT, Amos; NAOR, Moni. Untraceable electronic cash. In: 1988, Conference on the Theory and Application of Cryptography. [s. l.]: Springer, 1988. p. 319–327.

CHOHAN, Usman W. Cryptocurrencies as Asset-Backed Instruments : The Venezuelan Petro Cryptocurrencies as Asset-Backed Instruments : The Venezuelan Petro. [s. l.], 2018.

CHOHAN, Usman W. State-Sponsored Cryptocurrencies: The Diverse Motivations. SSRN Electronic Journal, [s. l.], 2020. Disponível em: https://doi.org/10.2139/ssrn.3543085

CHRISTINE KIM. The Kodak KashMiner's Flashy Debut Ends In Failure : CoinDesk. [s. l.], 2018. Disponível em: https://www.

coindesk.com/the-kodak-kashminers-flashy-debut-ends-in-failure.

COINMARKETCAP.COM. Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap. [s. l.], 2020. Disponível em: https://coinmarketcap.com/1/. Acesso em: 1 out. 2020.

DANIEL PALMER. Tensions Rising at Facebook Libra as Backers Consider Quitting: Report - CoinDesk. [s. l.], 2019a. Disponível em: https://www.coindesk.com/tensions-rising-at-facebook-libra-as-backers-consider-quitting-report.

DANIEL PALMER. Venezuela's Maduro Orders Top Bank to Make Petro Available to Public : CoinDesk. [s. l.], 2019b. Disponível em: https://www.coindesk.com/venezuelas-maduro-orders-top-bank-to-make-petro-available-to-public.

DAVIS, Andrew. Joseph Stiglitz: "We should shut down the cryptocurrencies". [s. l.]: CNBC, 2019. Disponível em: https://www.cnbc.com/2019/05/02/joseph-stiglitz-we-should-shutdown-the-cryptocurrencies.html?__source=twitter%7Cmain

GENCER, Adem Efe *et al*. Decentralization in Bitcoin and Ethereum Networks. [s. l.], 2018. Disponível em: https://arxiv.org/pdf/1801.03998.pdf

HAMMILL, Chuck. From Crossbows to cryptography: thwarting the state via technology. Future of Freedom Conference. [s. l.], n. November, p. 1–17, 1987. Disponível em: http://libertarianalliance.wordpress.com/2008/05/01/from-crossbows-to-cryptography-thwarting-the-state-via-technology/

HUGHES, Eric. A Cypherpunk's Manifesto : Cypherpunks Mailing List. [s. l.], 1993. Disponível em: https://www.activism.net/cypherpunk/manifesto.html.

HUGHES, Eric; MAY, Timothy. Crypto Glossary. [s. l.], 1992. Disponível em: https://nakamotoinstitute.org/crypto-glossary/. Acesso em: 4 out. 2020.

KARAME, Ghassan; ANDROULAKI, Elli. Bitcoin and Blockchain Security. Norwood, MA: Artech House, 2016. (Artech House Information Security and Privacy Series).E-book. Disponível em: http://ezproxy.javeriana.edu.co:2048/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=15118

48&lang=es&site=eds-live

KETHINENI, Sesha; CAO, Ying. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. International Criminal Justice Review. [s. l.], v. 30, n. 3, 2019. Disponível em: https://doi.org/10.1177/1057567719827051

KETHINENI, Sesha; CAO, Ying; DODGE, Cassandra. Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. American Journal of Criminal Justice, [s. l.], v. 43, n. 2, p. 141–157, 2018. Disponível em: https://doi.org/10.1007/s12103-017-9394-6

KHARIF, Olga. Who Is Satoshi Nakamoto? McAfee Vows to Unmask Bitcoin Creator - Bloomberg. [s. l.], 2019. Disponível em: https://www.bloomberg.com/news/articles/2019-04-23/john-mcafee-vows-to-unmask-crypto-s-satoshi-nakamoto-within-days.

LUDLOW, Peter. New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures. In: LUDLOW, Peter (org.). Crypto Anarchy, Cyberstates and Pirate Utopias. [s. l.]: MIT Press, 2001. E-book.

MAY, Timothy. E-mail: The Crypto Anarchist Manifesto. [s. l.: s. n.] Disponível em: https://activism.net/cypherpunk/crypto-anarchy.html

MAY, Timothy. Crypto Anarchy and Virtual Communities. [s. l.: s. n.] Disponível em: https://nakamotoinstitute.org/virtual-communities/. Acesso em: 4 out. 2020.

MAY, Timothy. Thirty Years of Crypto Anarchy at 3rd Hackers Congress Paralelní Polis. Prague: [s. n.], 2016. Disponível em: https://www.youtube.com/watch?v=TdmpAy1hI8g&list=PLGJQS0h-wqLQ5RLCnOkT0Vi9KSzcyyBgO&index=4

MOORE, Daniel; RID, Thomas. Survival Global Politics and Strategy Cryptopolitik and the Darknet. [s. l.], 2016. Disponível em: https://doi.org/10.1080/00396338.2016.1142085

NAKAMOTO, Satoshi. Bitcoin P2P e-cash paper. [s. l.], 2008a. Disponível em: http://article.gmane.org/gmane.comp.encryption.general/12588/.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [s. l.: s. n.] Disponível em: www.bitcoin.org

NAKAMOTO, Satoshi. Re: Bitcoin P2P e-cash paper. [s. l.], 2008c. Disponível em: https://doi.org/19:4:25 -0800. msg09997.

NAKAMOTO, Satoshi. Bitcoin open source implementation of P2P currency. [s. l.], 2009. Disponível em: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

NARAYANAN, Arvind *et al*. Bitcoin and Cryptocurrency Technologies Introduction to the book. Princeton, New Jersey: Princeton University Press, 2016. E-book. Disponível em: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf

NARAYANAN, B. Y. Arvind; CLARK, Jeremy; HAVE, I. F. Y. O. U. Bitcoin ' s Academic Pedigree. Communications of the ACM, [s. l.], v. 60, n. 12, p. 36–45, 2017. Disponível em: https://doi.org/10.1145/3132259

ORCUTT, Mike. Bitcoin and Ethereum have a hidden power structure, and it's just been revealed - MIT Technology Review. MIT Technology Review. [s. l.], p. 2–5, 2018. Disponível em: https://www.technologyreview.com/s/610018/bitcoin-and-ethereum-have-a-hidden-power-structure-and-its-just-been-revealed/

POON, Joseph; DRYJA, Thaddeus. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. [s. l.: s. n.]. Disponível em: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf.

RAND CORPORATION. Paul Baran and the Origins of the Internet : RAND. [s. l.], [s. d.]. Disponível em: https://www.rand.org/about/history/baran.html.

ROGOFF, Kenneth S. The curse of cash: How large-denomination bills aid crime and tax evasion and constrain monetary policy. [s. l.]: Princeton University Press, 2017. E-book.

SCHUIL, Frank. Why Satoshi Nakamoto's Identity Matters : CoinDesk. [s. l.], 2016. Disponível em: https://www.coindesk.com/why-matters-satoshi-nakamoto.

SIMMONS, Matty. The day cash died. [s. l.: s. n.] Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=113413622&site=eds-live

U. S. DEPARTMENT OF JUSTICE. Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting. [s. l.], 2007. Disponível em: https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.

VILNER, Yoav. Can The Real Satoshi Nakamoto (Or Craig Wright) Please Stand Up?. [s. l.], 2019. Disponível em: https://www.forbes.com/sites/yoavvilner/2019/05/30/can-the-real-satoshi-nakamoto-or-craig-wright-please-stand-up/#ff4e9d51fcf4.

ZETTER, Kim. Bullion and Bandits: The Improbable Rise and Fall of E-Gold | WIRED. Wired, [s. l.], 2009. Disponível em: https://www.wired.com/2009/06/e-gold/