Citação: (COSTARDI, 2021)

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

Referência bibliográfica: COSTARDI, C. M. DE O. C. THE IDEOLOGICAL BACKGROUND OF BITCOIN: the unintended, but predicted, convenience of anonymity for criminal activities. **Revista Brasileira de Ciências Policiais**, v. 12, n. 4, p. 75–99, 26 jan. 2021.

Fichamento

|  |  |  |
| --- | --- | --- |
| Pagina | Texto | Comentário |
| 3 | Bitcoin, the first of blockchain-based cryptocurrencies, was highly influenced by the countercultural movement known as Cypherpunks.  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 |  |
| 4 | 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) |  |
| 5 | (satoshi nakamoto) 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.  “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) |  |
| 8 | 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 (...)Cypherpunks are, indeed, crypto-anarchists.  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 pseudonym4 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) |  |
| 9 | 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). |  |
| 11 | Satoshi Nakamoto – disappeared shortly after 2010.  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 |  |
| 12 | 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. |  |
| 13 | 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). |  |
| 14 | 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).  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 |  |
| 15 - 16 | “Among the virtual currencies, BTC is the dominant cryptocurrency 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)  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  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). |  |
| 16 | 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. |  |
| 17 - 18 | 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 darknet6 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).  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 operation (i.e. e-gold, ecash). Nevertheless, no changes were made either to prevent or to counter the use of Bitcoin in illicit transactions. |  |
| 18 | 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). | Conclusão |