Jamie Min

CS1699

Deliverable 4

6 December 2018

The Quest for True Anonymization

Cryptocurrency made headlines as a disruptive technology that changed how we view the current global financial system. This particular technology is “a purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution” (Satoshi). In the remnants of the 2007-2008 financial crisis, Satoshi had a vision that would entirely remove the middle-man. His idea of a completely decentralized currency had a ripple effect on how we view transactions in today’s economy from smart contracts to fueling the underground black-market trade. Compared to fiat currency that relies on heavy centralization to control and monitor the market, cryptocurrencies pride itself on the fact of its decentralization and privacy. However, Bitcoin transactions are not anonymous as it once was touted to be. The transactions itself are publicly broadcasted on the blockchain and contain information regarding the sender and the recipient. In other words, every time someone makes a transaction with Bitcoin, stored information such as their physical location, IP addresses, or any other vectors of attack can be used to trace their identity and compromise a wallet. Nowadays, Bitcoin can hardly be said to be a true anonymous cryptocurrency. Enter Monero. Monero offers advantages such as the inherent technology that it is built on, internal security features, and a special security layer protocol called the Kovri Project that truly adheres to Satoshi’s vision of a decentralized and anonymous currency.

While Monero does store transactions publicly on the blockchain, it is virtually impossible to reveal the sender’s address. This is in part due to Monero’s inherent technology that it is built on, which differentiates it from Bitcoin. To take a step back, many cryptocurrencies use a term called “mining” that refers to special algorithms running on a computer or a network that verifies cryptocurrency transactions between the recipient and sender. These transactions are “mined” and broadcasted on the network for people on the network to accept. Essentially, the mining is the work being done that large financial institutions would otherwise be doing; hence, the decentralization. Bitcoin uses a series of complex mathematical problems to mine and verify transactions. In its introduction, Satoshi believed that this proof of work system would exist as “one CPU, one vote” in that anyone can take part in the network. Now, this mining system exists solely on specialized mining hardware called ASICs that make it virtually pointless for any ordinary individual to participate in the mining process. As a result, most of the mining power becomes centralized around mining pools that run expensive ASICs, thus leading to centralization of the network itself. On the other hand, Monero’s mining process is ASIC-resistant in that anyone can use their computer to mine and verify Monero transactions. The goal behind this is that it incentivizes regular individuals to use spare electricity to participate in the network than be completely overshadowed by giant mining pools using specialized hardware. Additionally, transactions that appear on the network are appended to “blocks” that implement an adaptive block size limit. Bitcoin, conversely, uses a fixed block size averaging a new block every ten minutes whereas Monero averages a new block every two minutes. Bitcoin transactions to be added are proportionate to the transactions fees whereas Monero can automatically accommodate future transactions. This, however, introduces a selective issue regarding potential spam attacks of oversized blocks. Monero’s technology implements a dynamic blocksize penalty. This ensures the best strategy for mining is to keep the blocks full of transactions, leaving no incentive to reduce the blocksize when the transaction pool is full. The penalty works in hand with tail emission to ensure this system is secure. We see that the inherent technology that separates it from Bitcoin allows a greater potential yield of future adopters thereby increasing the security of the network overall.

In addition to the certain aspects of technology that Monero is built on, the cryptocurrency incorporates internal security features that Bitcoin does not. For example, Monero uses built in features such as “Stealth Addresses” and “Ring Confidential Transactions” to better anonymize a sender. Stealth addresses are unique wallets addresses that can be used for any and each transaction that an individual makes. Bitcoin does have the option to use this external security feature, but Monero has support for this implicitly. Only the two core parties involved in the transaction will know any identity details associated with the stealth address. Internally, stealth addresses are longer than normal Bitcoin addresses but will look no different on the actual blockchain. The specific implementation of the transaction involves splitting the transaction into two parts where the first half is a persistent OP\_RETURN transaction that the second half uses in a Diffie-Helman-Merkle Key Exchange. This alone does not provide 100% anonymization, however. There is an additional built-in default option in Monero called Ring Confidential Transactions (RingCT) that incorporates a mixing service in the transaction that reveals just enough to confirm the validity of a transaction. Mixing is essentially a process where multiple transactions of the same amount are mixed around from various senders and then redistributed among the senders to make it harder to trace where the origin of the transaction came from. Another crucial aspect of RingCT is the utilization of range proofs. In other words, a range proof prevents transactions of negative values to be sent across the network, thus better securing the circulation of Monero. All of these features are built into the Monero security protocol. While Bitcoin offers similar services, it is up to the sender to be aware of these features and implement it themselves. Clearly, we can see a large overhead for new cryptocurrency users that might not be aware of these features that want to start using decentralized currencies.

While these built-in security features add an extra layer of privacy, stealth addresses and RingCT are not 100% anonymous. As a result, Monero introduces a third security aspect called the Kovri Project which is a special security layer protocol based on I2P features. Kovri uses both garlic encryption and garlic routing to ensure a private and protected layer across the Monero network. Essentially, this provides users a way to completely hide their geographical location and IP address. Take the Bitcoin network in contrast. When an individual makes a transaction, that transaction tells the network that it wants to be included in the next block. Information such as IP addresses and other meta data can be obtained by malicious actors. Monero operates in a similar way, but Kovri will make this virtually impossible by incorporating security aspects of the I2P protocol. Garlic routing is a variant of onion routing that encrypts information, making it more difficult to perform traffic analysis relative to Tor which has its own host of problems. In the name of security, Kovri attempts to solve the issues facing Tor, namely its flow-based onion-routing argued to not be truly decentralized. At a high-level overview, Kovri attempts to hide a user’s IP address and potentially redirect all traffic through its layer. Without Kovri, a malicious actor can identify an individual running a Monero node and attempt to compromise the individual through any means of attack. In short, incorporating security features such as stealth addresses and RingCT with the added security layer of Kovri makes it virtually impossible to trace a transaction to a sender. Bitcoin, on the other hand, is pseudonymous in that an address can be linked to an identity through a variety of different means and anyone can see whether or not an individual is running a Bitcoin node. Since Monero automatically implements these security features in the network itself, Monero clearly has a huge advantage in terms of security and privacy over Bitcoin.

In conclusion, the idea of anonymization of cryptocurrencies have dominated the talks of its adoption and growth in the global network. Taking two popular cryptocurrencies, Bitcoin and Monero, we can start seeing a vastly different approach to the philosophy of anonymity. As cryptocurrency continues to make headlines, it is important that we consider the values that cryptocurrencies hold in the first place. The question remains whether or not Monero can start to compete with Bitcoin. In short, the biggest critical flaw with Bitcoin is its lack of privacy. Monero solves these privacy issues by offering inherent security features that are implemented within the technology itself. Additionally, with the use of Kovri and I2P protocol layering of the Monero network, a Monero user can truly expect to be anonymous. So, we finally come back to Satoshi and the quest of true anonymization. Bitcoin over the years have strayed away from the idea of a truly decentralized cryptocurrency. In its stead, it appears that Monero has begun to take the lead. In the future, we can hopefully expect other cryptocurrencies to adopt Monero’s approach of privacy-centric and stray away from the designs of Bitcoin that make it unsecure. The quest for true anonymization starts with Monero.

References

<https://btcmanager.com/what-is-kovri-why-is-it-important-for-monero/>

<https://monero.org/monero-vs-bitcoin/>

<https://www.monero.how/why-monero-vs-bitcoin>