Mike Sadowski

CP682B-OC1

Tuesday, March 2nd 2021

Quisquis - A New Design for Anonymous Cryptocurrencies: Paper Review

Digital currencies, better known as cryptocurrencies, are intangible and can only be owned/transacted using computers and electronic wallets. Cryptocurrencies such as Bitcoin are emerging forms of electronic payment systems that are being integrated across a number of businesses and exchange markets. While these systems offer solutions to and alleviate some of the headaches that come with managing physical money, they raise a number of privacy and security concerns. Bitcoin and other similar cryptocurrencies rely on what's known as addresses, which allow users to participate in transactions. These addresses pose privacy concerns as transactions consist of a chain of digital signatures, and each individual coin can be publicly tracked and traced back to the original owner (Elli Androulaki et al, 2013).

With the introduction of Bitcoin and similar cryptographic currencies, "the association with public and private key pairs and the use of addresses gave rise to a form of pseudo-anonymity for users interacting with these systems" (Prastudy Fauzi et al, 2019). Cryptocurrencies relying on addresses have some major security issues due to the use of and construction of these addresses. Users are able to create and operate many different addresses which are able to keep track of who owns which coins. The problem with this is these addresses can be linked together, linking the currency to the real-world identity of the user. Providing enhancements and solutions to privacy for cryptocurrencies is becoming increasingly popular due to this.

“Tumblers act as opt-in overlays to existing cryptocurrencies and achieve privacy by allowing senders to mix their coins with those of other senders” (Prastudy Fauzi et al, 2019). While this provides users with some level of anonymity, mixers such as Tumblers come with drawbacks. The entire system relies on trusting a central mixer, which can leave users vulnerable to attacks on availability. In addition to this, they require significant coordination between users wishing to mix due to the reliance on other people to mix with.

“A second form of privacy in some cryptocurrency systems can be built in at the protocol level” (Prastudy Fauzi et al, 2019). For example, Monero allows users to mix in a specific number of addresses as their own into a pool of other addresses. Using this list of public keys, they are able to form a ring signature and hide which specific addresses are their own. This solution also poses some problems, mainly in the form of plausible deniability for users of systems similar to Zcash. Nobody is supposed to be able to tell if a user meant to be involved in a transaction (meaning, no one can tell if their address was used in a ring without their consent).

However, while cryptocurrencies such as Monero and Zcash are able to solve some of the privacy and security flaws that Bitcoin introduces, they also pose some major problems. The biggest issue with cryptocurrencies such as these is that users are not able to store an accurate representation of their coin count within their blockchain. When a Bitcoin is spent, its address is no longer a UTXO (unspent transaction output). In Monero and Zcash, these addresses can never be removed from the UTXO set. It is unclear whether an address spent its contents or was used as part of anonymity set in a transaction with a different sender.

Developers of a new system they named Quisquis decided to pioneer a solution to the shortcomings mentioned above. With their new transaction system, users wanting to trade digital currency would be allowed to do so but with the added protection that the Quisquis model provides. “It achieves this by storing small amounts of data, does not require a trusted setup, and each address appears on the blockchain at most twice; when it is generated as output of a transaction and once when it is spent as input to a transaction” (Prastudy Fauzi et al, 2019). With Quisquis’ concept of updateable public keys, a key is able to be owned by a user but at the same time not look like it belongs to them and, as a result, achieve anonymity. In addition to this, Quisquis solves the forever growing of the UTXO problem posed by Zcash and Monero. They achieve this by “replacing all the input public keys in the UTXO set with the output public keys, allowing the UTXO to behave similarly as it does in Bitcoin” (Prastudy Fauzi et al, 2019).

Quisquis remedies many of the problems posed by other cryptocurrencies and also provides some added bonuses. Users are able to create and perform transactions without relying on other users to mix with and they can involve other keys without user permission and achieve a high degree of plausible deniability. As a bonus, the transactions of Quisquis are inexpensive to compute and verify (471ms for computation and 71ms for verification) (Prastudy Fauzi et al, 2019). To ensure the integrity of a transaction, a sender of coins is able to prove in zero-knowledge that the keys have been correctly updated and they only manipulated their own coins. However, even with all its benefits, Quisquis still comes with its own flaws. A paper written by Aram Jivanyan titled “Lelantus: A New Design for Anonymous and Confidential Cryptocurrencies” discusses these flaws and mentions a new cryptocurrency named Lelantus. In the paper, the author mentions how Quisquis only supports anonymity sets of size 16, which makes it “vulnerable to all attacks endemic to the decoy systems with small anonymity sets”

(Jivanyan, Aram, 2020). Lelantus is able to make transactions truly private. It accomplishes this by leveraging a “zerocoin setup”, which is limited to work with “fixed denominated coins which can be spent anonymously but without any ability of merging, splitting or partially redeeming multiple coins in a confidential way” (Jivanyan, Aram, 2020). Lelantus extends zerocoin coins with secret balances enabling the user to create coins of arbitrary values and later spend them anonymously into fresh new outputs of arbitrary values. The creators then “introduce a new zero-knowledge balance proof construction to ensure that the transaction’s input and output values sum up” (Jivanyan, Aram, 2020).

Lelantus provides advantages over Quisquis and other digital payment systems. It provides stronger anonymity, does not require trusted setup processes, transactions support direct anonymous payments and can admit an arbitrary amount of input and output coins (shielded coins can be merged/split in anonymous and confidential ways). While Quisquis was a good substitute when it was created, Lelantus’ birth brought more changes and innovation that allow for safer and more reliable cryptocurrency trading. Lelantus is not perfect, but it is one of the most secure and reliable forms of cryptocurrency trading we currently have.

To compete with Lelantus, the creators of Quisquis have noted some improvements they will be implementing in the future. They mention that they left an interesting open problem, “the design of a special purpose NIZK for improved communication efficiency” (Prastudy Fauzi et al, 2019). In a NIZK (non-interactive zero-knowledge), a hash function replaces the verifier which provides security by introducing a form of randomness. Another improvement mentioned after the paper was written was how they would deal with asynchrony (what happens if two transactions use the same public key for their anonymity set then only one can get into the blockchain?).

While no cryptocurrency system is perfect, there are some that are worse than others. While Quisquis and Lelantus provide some advantage over Bitcoin, no system will be secure for forever. Attacks are becoming more and more sophisticated, and only time will tell how long it will take for a cryptocurrency system such as Quisquis or even Lelantus to be considered insecure.

Works Cited

1. Prastudy Fauzi, Sarah Meiklejohn, Rebekah Mercer, and Claudio Orlandi. "*Quisquis: A New Design for Anonymous Cryptocurrencies*". Aarhus, Denmark. Pages 1 – 36.
2. Elli Androulaki , Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. "*Evaluating User Privacy in Bitcoin*". Springer, Heidelberg, Germany, 2013. Pages 1 – 18.
3. Jivanyan, Aram. "*Lelantus: A New Design for Anonymous and Confidential Cryptocurrencies".* 2020. Pages 1 – 18.

Other sources:

https://www.investopedia.com/terms/d/digital-currency.asp

https://thenextweb.com/hardfork/2018/11/05/bitcoin-address-explained/

https://micky.com.au/expert-warning-fatal-flaw-embedded-in-all-privacy-coins/

https://lelantus.io/a-new-design-for-anonymous-and-confidential-cryptocurrencies.pdf

http://diyhpl.us/wiki/transcripts/stanford-blockchain-conference/2019/quisquis/

https://crypto.stackexchange.com/questions/14365/what-is-a-non-interactive-zero-knowledge-proof