A Review of Zcash as a Cryptocurrency Platform Aimed Towards Maintaining Privacy Between All Parties

Daniel Ramos, Gabriel Zanko, *MobileyourLife – Bogotá, D.C., Colombia*

Abstract

As the general population becomes more knowledgeable about cryptocurrency, the problems inherently associated with their mechanisms also become more noticeable, and one of the main concerns that keeps users discouraged from entering this landscape.

Zcash aims to implement a new way to validate transactions using zero-knowledge proof mechanisms, allowing each of the involved parties in a transaction to keep private all the data on their end, tackling the concern of leaving information like transaction volumes and addresses out in the open.

Index Terms **– cryptocurrency, Zcash, zero-knowledge, privacy, transaction, commerce, bitcoin, security.**

I. Introduction

Despite the popularity of cryptocurrency being constantly on the rise for the last couple of years, experts on the field are increasingly worried about the phenomenon of cryptocurrency – and blockchain, inherently – is following a path of sacrificing certain intrinsic values in exchange of profitability, and the most preoccupying of these sacrifices is in privacy[1].

Since its conception in 2008, as explained in the original Bitcoin whitepaper published by Satoshi Nakamoto[2], one of the main advantages of the implementation of blockchain was how it represented a decentralized ledger, meaning that the information of all transactions is stored and updated simultaneously in all nodes of the chain, while privacy is only kept behind the encryption of the blocks, meaning that nodes have access to all the information of transactions.

However, as the interest of the general population towards cryptocurrency kept increasing, some started to ask about ways to keep certain information private. Not everyone feels comfortable with their digital address, balance, and the data of every transaction they performed being publicly available to thousands of computers around the world, which is why multiple advances have been made in ways to enhance the privacy of the data, which is why projects like Zcash have caught the attention of potential users.

In this document we will cover Zcash and their initiative that plans to bring cryptocurrency to a new era focused on the privacy of the transaction and user data, its primary features, how it compares to the current state of the market and what its success may bring for the future of digital currencies as an alternative for traditional financial systems.

II. Primary Functionalities

As we already mentioned, the main focus of Zcash is that it gives its users additional options regarding the privacy of their personal data and the information regarding their wallets and transactions. To ensure this, they developed a new technology to create the proof required to validate a transaction, without actually revealing the information that is being proven.

This technology, called "zk-SNARKs" (acronym for *zero-knowledge Succinct Non-interactive Argument of Knowledge*) allows one of the involve parties to prove to another that certain information exists without giving away any other information. For example, the prover could present the cryptographic hash of a random number and convince the verifier that said number

exists, without explicitly sharing the number. Furthermore, zk-SNARKs are a system that allows the prover that the number not only exists, but they also know the number, and all of it without sharing extensive lengths of information or multiple trivial back-and-forth communications between the parties.

They explain that, at a high level, sk-SNARKs first turn the information that will be proved Into an equivalent form about knowing a solution to some algebraic equations. The first step of this process is to create an arithmetic circuit that represents the equation that will be proven, which is composed of a series of simple arithmetic operations (addition, subtraction, multiplication, and division). Figure 1 shows an example of the arithmetic circuit that represents the equation $(a + b) * (b * c)$, on top of which a layer of verification is created, called the "Rank 1 Constraint System" or R1CS.

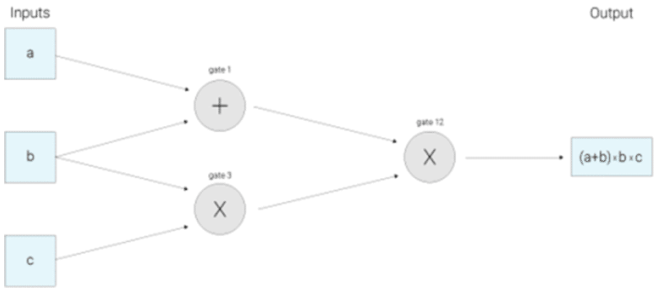

Figure 1.: Representation of an arithmetic circuit, going from the inputs (left) to the output (right). Note how each step of the circuit is meant to include less operations between the results of the previous steps, meaning that later steps carry more information than earlier ones.

However, implementing an R1CS that verifies every step of the circuit would mean the verification would take large amounts of time, so Zcash implemented a Quadratic Arithmetic Program[3] to bundle multiple constraints into one. By switching the verification from numbers to polynomials, which makes identities safer to be verified, and then the system only needs to verify that two of these polynomials match at a randomly chosen point, which also prevents malicious users to prepare for the verification process.

Unlike in Bitcoin, where the verification of the transaction requires the linking of the addresses of the sender and the receiver, and the input and output values of the transaction on the public blockchain, the sender of a shielded transaction needs only to send proof with high probability that (1) the input values sum to the output values, (2) they know the private spending keys of input notes and (3) these private keys are cryptographically linked to a signature over the entire transaction. With this information, the consensus algorithm is able to automatically verify the validity of a transaction even if the owners of the addresses wish not to reveal the details of it, which covers the main concern regarding privacy that has been growing among the community.

III. Comparison with Other Assets

When compared to other assets, the main benefit of Zcash is quite clear: the option to maintain the details of transactions in complete secret. They use the word "option" since one or both parties are allowed to disclose the data on their end (address or input) with trusted parties, which allows for auditory and compliance requirements to be met. This results in the four types of transactions supported by Zcash: private, shielding, deshielding and public (Figure 2). The variety in transaction types also works to fulfill the needs of a wide range of clients, which gives Zcash an edge above the competition.

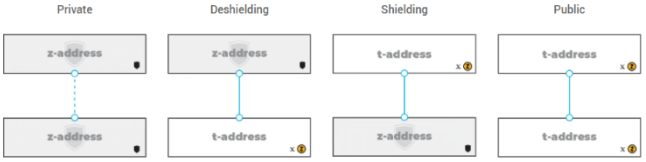

Figure 2.: Representation of the type of transactions supported by Zcash involving private (z-) and public (t-) addresses. The possibility for both parties to disclosure the information on their end gives way for audits and regulatory verifications to be met.

In addition, Zcash offers multiple features that distinguish their system from other similar networks, including the capacity to include encrypted memos in the transactions as a way for the sender to share

important information with the receiver, separate disclosure of addresses and payment volumes, the option to create transactions that require multiple signatures to be validated (multisignature transactions), and all while maintaining transaction fees of 0.0001 Zcash.

Given that Zcash is originally based on the same code base as Bitcoin, there are also many similarities that can be pointed between these two, including the same maximum total of tokens that can be mined (21 million), the same number of tokens given as a reward for the successful construction of a new block (6.25 ZEC and BTC, respectively). These similarities also work as a gateway for potential users to enter the network while not being completely unfamiliar with how it works in terms of availability and mining, while giving them the opportunity to test the functionalities that turn Zcash into a vast improvement regarding privacy.

IV. Long-term Possibilities

Despite the fact that Zcash is one of earliest applications of zk-SNARKs as a technology, this type of confidential validation of transactions could also be added to other distributed ledgers as an additional security layer, which could be useful for institutional clients or other high-level users with more strict confidentiality requirements.

It is still quite early in terms of computational power to think too far into the future of zk-SNARKs, but Zcash ensures that their team of scientists are among the most-knowledgeable in the subject, and that they will continuously work on new ways to implement this system, of which they have already revealed two examples:

IV.a. Private smart contracts

Smart contracts are the backbone of Ethereum and the source of its popularity. They allow for two distrustful parties to reach an agreement for a transaction that only becomes effective once certain conditions are met, while ensuring that each of the

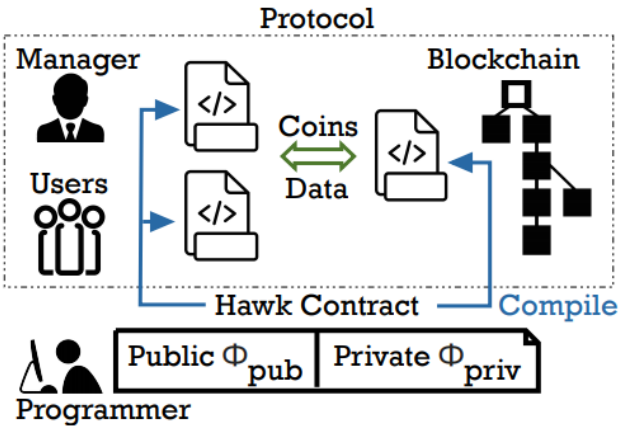

Figure 3.: Simplified diagram of the Hawk protocol. Note how all of the actors communicate with the blockchain through the contract instead of directly with each other, which allows them to keep their end of the transaction private.

parties is correctly compensated in case of breaches or aborts. However, much like transactions on Bitcoin, the details of the contracts are publicly available through the Ethereum Network.

Hawk[4] is a project aimed at implementing zero-knowledge proof mechanisms to similar contracts, where users can create the contracts in an intuitive way and their compiler takes care of the cryptographic protocol to communicate with the blockchain, and it also allows the parties to keep the details on their end of the contract private, while the conditions for the fulfillment of the transactions remain completely impervious to tampering either from the involved parties or external malicious actors.

IV.b. Private payment channels

Another potentially useful application of zero-knowledge proof mechanisms comes with their implementation into payment channels. Since transactions in public blockchains require time to be properly validated and added to the respective block, not only is the privacy of the transactions compromised, but scalability and latency issues are also added to the mix[5].

BOLT[6] (Blind Off-chain Lightweight Transactions), developed by Ian Miers and Matthew Green, takes inspiration from the Lightning Network to offer fast and scalable payment channels that take advantage of

Zcash's strong focus on privacy. They combine the use of payment channels set up by the merchant, which allow for multiple small transactions to take place in milliseconds (without block confirmation), and the ability to route the payments through third parties, avoiding the need to maintain a direct channel between the merchant and each customer.

Even if this project was born from the idea to combine Zcash and the Lightning Network, the developers claim that it is possible to set up BOLT to work with most tokens if the primitives can be added to the network, since the privacy provided by BOLT is not inherently provided by the blockchain but by the way they anonymously establish and close the channels.

V. Conclusion

As cryptocurrencies become more relevant in our society, it is important to keep focusing on the issues that are deeply associated with its current functionalities and to keep an open mind on how to solve them, since their adoption depends on improving the image the general population has about them.

Projects like Zcash, Hawk and BOLT work towards a similar goal through different paths: to convince those interested in cryptocurrency that their data can be protected, without needing to trust in any centralized datacenter or safekeep mechanism. They stand as proof that when creativity meets vision, almost everything can be accomplished, and that paints a brighter picture of the future not only the cryptocurrency market, but also the entire sector of digital personal finances.

VI. References

1. Conti, Mauro et al (2017). "A Survey on Security and Privacy Issues of Bitcoin" Retrieved from: https://arxiv.org/pdf/1706.00916.pdf?utm_source=securitydailynews.com
2. Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" Retrieved from: https://bitcoin.org/bitcoin.pdf
3. Gennaro, Rosario et al (2012). "Quadratic Span Programs and Succinct NIZKs without PCPs" Retrieved from: https://eprint.iacr.org/2012/215.pdf
4. Kosba, Ahmed et al (2015). "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts" Retrieved from: https://eprint.iacr.org/2015/675.pdf
5. Chauhan, Anamika et al (2018). "Blockchain and Scalability". 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, 2018, pp. 122-128. Retrieved from https://ieeexplore.ieee.org/abstract/document/8431962
6. Miers, Ian (2016). "BOLT: Private Payment Channels". Retrieved from: https://electriccoin.co/blog/bolt-private-payment-channels/