International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

An Introduction to ZCash-How ZCash a better Cryptocurrency than Bitcoin

Sruthi Krishna.U[1], Dr. Anil G. N[2]

[1]M. Tech Student, BMS Institute of technology & Management, Yelahanka, Bangalore-560064
[2]Associate Professor, BMS Institute of technology & Management, Yelahanka, Bangalore, Karnataka, India

---

Abstract - *Cryptocurrency have emerged as important financial software in the field of finance and technology. Bitcoin is the first digital software evolved to achieve a wide spread adoption. These cryptocurrencies rely on a secure distributed ledger data structure i.e., blockchain, mining is also an integral part of such systems. Bitcoin fails to offer privacy for payment systems. To overcome this drawback, Zcash was developed. Zcash is developed to fix the security issues of bitcoin. It bridges the existing payment scheme used by the bitcoin system with a shielded payment scheme secured by zero-knowledge succinct non-interactive arguments of knowledge(zk-SNARKs). It attempts to address the problem of mining centralization by use of Equihash memory-hard proof-of-work algorithm. This specification defines the Zcash consensus protocol and explains its differences from Zero cash and Bitcoin.*

Key Words*: *Cryptocurrency, block Chain, Mining Bitcoin, Zcash, zk-SNARKs

1. INTRODUCTION

As technology is growing day by day, Cryptocurrencies have played a major impact in the field of finance. The cryptocurrencies make use of cryptography to make coins as well as for the secure transactions. There are many cryptocurrencies available in the market worldwide. Some examples of them are Bitcoins, Lite coins, Ethereum's Ether are the popular cryptocurrencies.

In some countries, Cryptocurrencies are legalized. Bitcoin is the first ever digital software developed as cryptocurrency. It was developed by Satoshi Nakamoto and released in 2009.It was the first widely adopted digital currency.it enables the payment between the two bitcoin users anywhere in the world, with negligible fees and no risk of reverted transaction. It requires no trusted parties. Bitcoins uses a distributed ledger known as blockchain to store the transactions made by the user, Mining is a central theme of the bitcoin software. The major drawback of this was, it fails to offer privacy for the Bitcoin transactions, as a result Zcash came into existence.

Zcash is the latest kind of cryptocurrencies. It is decentralized open source cryptocurrency. The transactions are recorded and published on blockchain but details such as the sender, recipient and amount remain private. It was developed by Zooko Wilcox O-Hearn and Matthew DGreen. It was released in 2016.Zcash offers its user the choice of shielded transactions, which allow for content to be encrypted using advanced cryptographic technique such as zero-knowledge proof construction called as zk-SNARKs developed by its team. Thus, Zcash Offers an added feature over bitcoin, while ensuring privacy.

2. OVERVIEW

ZCash is a privacy driven cryptocurrency. The algorithm used is Equihash algorithm, which is an asymmetric memory-hard Proof of Work algorithm based on the generalized birthday problem. It relies on high RAM requirements to bottleneck the generation of proofs and making ASIC development unfeasible. The zero-learning Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) [2] methods is utilized to guarantee that all data (sender, collector, sum) is encoded, without the likelihood of twofold spending. The main data that is uncovered with respect to exchanges is the time in which they occur.

3. BITCOIN

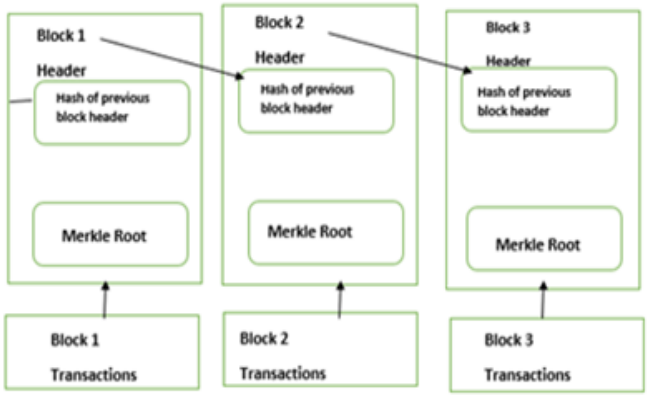
Bitcoin is the principal generally embraced advanced cash. It empowers close quick installments between any two Bitcoin clients anyplace on the planet, with unimportant expenses and no danger of returned exchanges. Like all electronic installment frameworks, Bitcoin needs an instrument to guarantee the respectability of the exchanges (e.g., to keep a maverick client from paying the same computerized "coin" to different traders). Customary electronic installment frameworks accomplish this by depending on a trusted focal gathering, for example, a bank. Bitcoin dodges such unified trust (and the Overhead connected with it); rather, Bitcoin utilizes a circulated record, known as the block chain to store clients' exchanges. The piece chain is kept up and refreshed by agreement over the pool of (commonly doubtful) members, utilizing an Internet convention that is difficult to subvert. Any client can, whenever, specifically pay some other client, by communicating an installment exchange in the Bitcoin organize. The beneficiary checks this exchange against earlier ones in the piece chain, to confirm that the sent assets have a substantial provenance and are not copied (i.e., spent numerous circumstances).

3.1 BLOCK CHAIN METHODOLOGY

A block chain is a general public ledger of all Bitcoin transactions. It is continuously growing as new completed blocks are added to it with new recordings. The blocks are

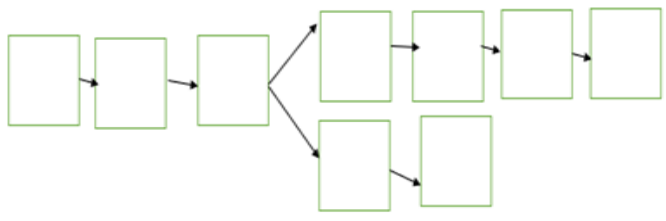
added to the blockchain in a chronological order. Each node gets a copy of blockchain automatically while joining the bitcoin network. The blockchain maintains the complete transaction details regarding the addresses and their balances right from the genesis or the first block to the last used block. The blockchain is the main technological innovation of Bitcoin.

A simplified representation of Blockchain can be illustrated as in the figure.



Simplified Block Chain

The first block contains the first transactions of a given cryptocurrency i.e. bitcoin. The hash of the first block is passed forward to the miner, which uses it and generates a nonce to create the hash for the second block and cycle repeats. Thus, forming a chronological order. When two blocks are created fork occurs for the creation of block at the same time, a timestamp is generated and subsequent block links are accepted. The forking can be represented by below figure.



Forking in a Block Chain

3.2 MINING METHODOLOGY

Every cryptocurrency includes a distributed general public ledger known as the Block Chain. A transaction is created when a user sends some currency to the receiver. Mining tests the transactions and adds them to this general public ledger. When a new transaction takes place, the miner verifies the currency whether it belong to the user or not, or if the user is trying to double spend. The original ownership of the currency can be tracked from the blockchain [3][1]. A malicious user would create multiple nodes and attempts to make a invalid transactions. In order to prevent such attacks miners are required to perform a resource intensive task. The resource intensive task [3] includes the following:

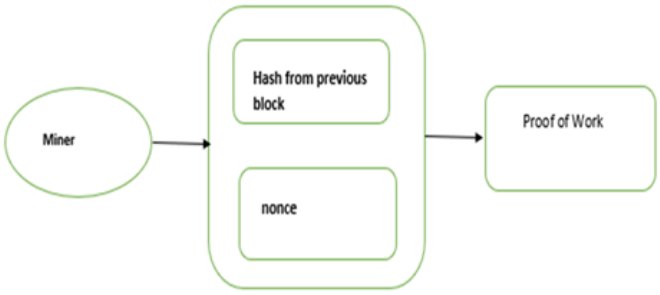
a. Proof of work- it is easily verifiable result of a resource intensive task that confirms that particular task has been performed.

b. Proof of Stake- it requires the miner to show how much amount of currency, miner owns in particular system.

c. Proof of Retrievability: it requires the miner to show that the data was given to store is intact and can be recovered

The Proof Constructions requires intensive use of the memory or any related resources. It restricts the number of transactions which is validated in the given amount of time period.

The simplified Proof of Work mining is depicted in the figure.



Simplified view of Proof of Work Mining

Mining uses brute-force algorithm and it is designed so that the number of blocks mined per day remains approximately constant in order to control the rate of introduction of new currencies, which are unlocked when a block is mined. The first miner is to compute the proof and to test the block and it earns the reward, which is a fraction of unlocked currency. This testing should be done at a high speed and at a ease.

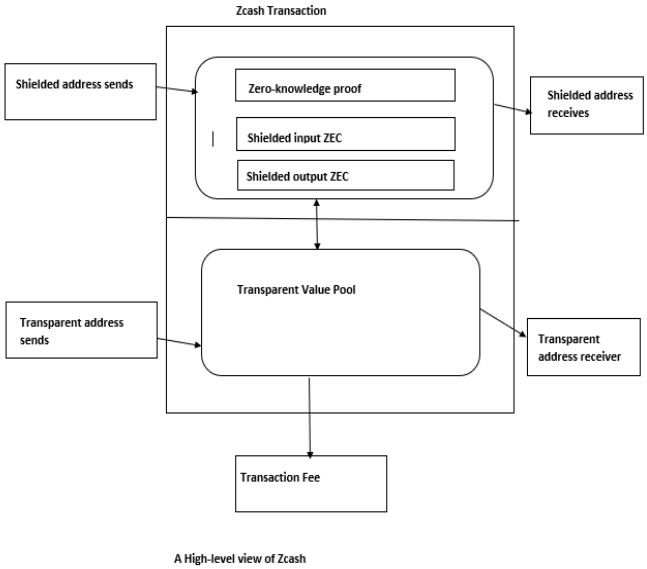
4. ZCASH

Zcash is a decentralized and open-source cryptographic money that offers security and specific straightforwardness of exchanges.Zcash installments are made accessible on an overall population record known as blockchain yet the sender, recipient and measure of exchanges stays private [5].

4.1 ZCASH METHODOLOGY

Zcash encrypts the information of protected exchanges. Since the installment data is secured, the convention utilizes a cryptographic strategy to test its legitimacy.

Zcash uses a zero-knowledge proof construction called **zk-SNARKS** developed by its team of cryptographers based on recent cryptographic technologies. These developments enable the system to keep up secure record adjust without unveiling it to outsiders or sum involved. Instead of openly exhibiting spend specialist and exchange values, the metadata is encoded and thus proves that no one is stealing.



A High-level view of Zcash

Zcash functionality is realized in two types of transactions: mint transactions and pour transactions which are appended to ledger.

Mint transactions: It allows a user to convert the user to convert a user specified base coins to Same number of zero coins, this transaction consists of cryptographic commitment to a new coin which specifies its values and owner address.

Pour transactions: It allows the user to make a private payment by consuming some number of coins in order to produce new coins, the user inputs two coins, each one of the coin appears in some mint transactions or the output of pour transactions, the total value of the input coins equals the total value of the output coins.

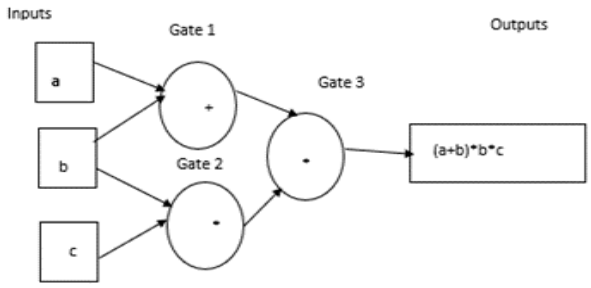
4.2 IMPLEMENTATION OF zk-SNARKS IN ZCASH

Keeping in mind the end goal to have zero-learning protection in Zcash, the capacity deciding the legitimacy of an exchange as per the system's accord rules must restore the appropriate response of whether the exchange is substantial or not, without uncovering any of the data it played out the estimations on. This is finished by encoding a portion of the system's accord administers in zk-SNARKs. At an abnormal state, zk-SNARKs work by first transforming what you need to demonstrate into a comparable frame about knowing an answer for some logarithmic conditions. In the accompanying segment, we give a concise review of how the guidelines for deciding a legitimate exchange get changed into conditions that would then be able to be assessed on a hopeful arrangement without uncovering any delicate data to the gatherings checking the conditions.

Calculation → Arithmetic Circuit → R1CS → QAP → zk-SNARK

The initial phase in transforming our exchange legitimacy work into a numerical portrayal is to separate the consistent strides into the littlest conceivable operations, making a "math circuit". Like a boolean circuit where a program is incorporated down to discrete, single steps like AND, OR, NOT, when a program is changed over to a number juggling circuit, it's separated into single steps comprising of the fundamental number-crunching operations of expansion, subtraction, augmentation, and division (despite the fact that in our specific case, we will abstain from utilizing division).

Here is a case of what a circuit looks like for figuring the expression (a+b)*(b*c):



Taking a look, at such a circuit, we can think about the info esteems a, b, c as "voyaging" left-to-appropriate on the wires towards the yield wire. Our subsequent stage is to assemble what is known as a Rank 1 Constraint System, or R1CS, to watch that the qualities are "voyaging accurately". In this illustration, the R1CS will affirm, for example, that the esteem leaving the augmentation door where b and c went in is b*c.

In this R1CS portrayal, the verifier needs to check numerous imperatives — one for relatively every wire of the circuit. (For specialized reasons, it turns out we just have a limitation for wires leaving augmentation entryways.) In a 2012 paper on the subject, Gennaro, Gentry, Parno and Raykova introduced a pleasant method to "package every one of these imperatives into one". This strategy utilizes a portrayal of the circuit called a Quadratic Arithmetic Program (QAP). The single requirement that should be checked is currently between polynomials as opposed to between numbers. The polynomials can be very huge, yet this is okay since when a personality does not hold between polynomials, it will neglect to hold at generally focuses. Hence, you just need to watch that the two polynomials coordinate at one arbitrarily picked point keeping in mind the end goal to effectively confirm the confirmation with high likelihood.

On the off chance that the prover knew ahead of time which point the verifier would check, they may have the capacity to make polynomials that are invalid, yet fulfill the personality by then. With zk-SNARKs, refined numerical methods, for example, homomorphic encryption and pairings of elliptic bends are utilized to assess polynomials "aimlessly" - i.e. without knowing which point is being assessed. People in general parameters portrayed above are utilized to figure out which point will be checked, yet in encoded shape with the goal that neither the prover nor the verifier recognize what it is.

The depiction so far has chiefly tended to how to get the S and N in "SNARKs" — how to get a short, non-intelligent, single message evidence — however hasn't tended to the "zk" (zero-information) part which permits the prover to keep up the classification of their mystery inputs. Things being what they are at this stage, the "zk" part can be effectively included by having the prover utilize "arbitrary movements" of the first polynomials that still fulfill the required character.

4.3 MINING IN ZCASH

It uses Equihash as an algorithm for hashing which is asymmetric memory-hard proof of work algorithm based on generalized Birthday problem. It was developed by Alex Biryou and Dmitry Khovratovich. It relies on high RAM requirements to bottleneck the generation of proofs and ASIC development unfeasible.

5. CONCLUSION

Decentralized currencies should ensure privacy to its user when conducting financial transactions. Zcash provides such privacy protection by hiding user identities, exchange sums and records from public view. The underlying zk-SNARKs technique i.e., cryptographic proof is enough to support a wide range of policies. It can, for instance, let a client demonstrate that he paid his duty charges on all exchanges without uncovering those exchanges, their sums, or even the measure of expenses paid. For whatever length of time that the strategy can be determined by proficient nondeterministic calculation utilizing NP proclamations, it can (on a fundamental level) be implemented utilizing zk-SNARKs, and added to Zcash. This can empower security saving confirmation and implementation of an extensive variety of consistence and administrative approaches that would some way or another be obtrusive to check specifically or may be avoided by degenerate experts. This raises research, arrangement, and designing inquiries over what strategies are alluring and for all intents and purposes feasible. Another examination question is the thing that new usefulness can be acknowledged by increasing the capacities effectively display in Bitcoin's scripting dialect with zk-SNARKs that permit quick check of expressive proclamations.

6. REFERENCES

[1]. Israa Alqassem, Davor Svetinovic, Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural Analysis. 2014 IEEE International Conference on Internet of Things (iThings 2014), Green Computing and Communications (GreenCom 2014), and Cyber-Physical-Social Computing (CPSCom 2014)

[2]. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic CashSystem,2009[online]. Available: http://www.bitcoin.org/bitcoin.pdf

[3]. Eli Ben-Sasson,, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza, Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy.

[4]. Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu and Richard Brooks, A Brief Survey of Cryptocurrency Systems.

[5]. Daira Hopwood Sean Bowe† — Taylor Hornby — Nathan Wilcox Zcash Protocol Specification Version 2017.0-beta-2.5 March 7, 2017