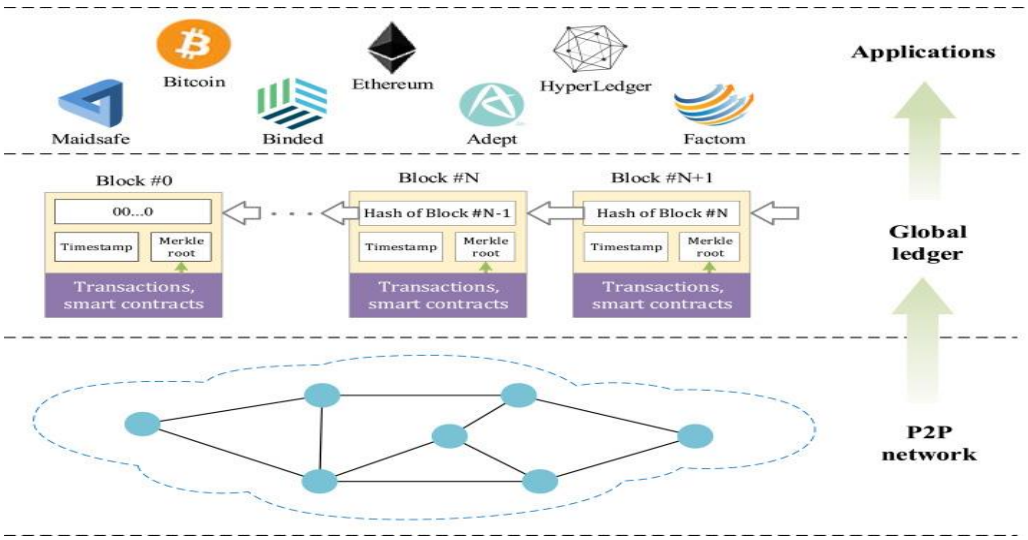
THE ESSENTIAL INTERCONNECTION BETWEEN BLOCKCHAIN AND ZERO-KNOWLEDGE PROOF

Introduction

Blockchain being a series of linked blocks/records cryptographically linked with each other ensuring decentralization, transparency, and immutability. However, this mushrooming technology is growing and making its mark in every field, be it in health care, real estate, agriculture, and food. The scope of improvement is vast, for example blockchain in agriculture and food sector is inviting both the producer and the purchaser in great numbers as it is simplifying the processes, bringing transparency, and accumulating quality production **(6)**. Many blockchain networks use public databases. So, anyone having an internet connection can view the list of the network's transaction history. They can see all the details associated with the transaction and your wallet details, but the name of the user will still be unknown to them. This put your anonymous cover blown; debunking the myth of Blockchain's anonymity and privacy, and makes one realize that –The user's sensitive information stored on a Blockchain network is only confidential, not anonymous **(7).** Zero-knowledge proof is an encryption scheme whereby one party (the prover) can prove the truth of specific information to another party (the verifier) without disclosing any additional information. While blockchain has brought us great advantages like transparency, immutability, and decentralization, it can lack the privacy needed for some transactions. However, combining zero-knowledge proofs (ZKP's) with blockchain technology has the power to provide users with a powerful mix of immutability and security **(8)**.

The need for extra privacy in blockchains

With blockchains and cryptocurrency taking over the world in all sectors and as a means of payment, there is an excruciating need for security over such a vast network. Even though various means such as the avalanche effect, proof of work and the concept of byzantine fault tolerance are present there is a need for more encryption and privacy on transactions. Transactions can be viewed by anyone with an internet connection and does not add up to the whole talk about 'blockchains being completely secure'. Users inevitably are made to agree to the blockchain system by providing personal data to banks/companies and trusting them with it. These same banks and companies have been using the concept of immutable ledger in blockchains for a long period along with making transactions with the consent you provide for. The awareness and education about cryptography is not brought in the light by said banks/companies and needs another step before reaching its utmost level of security.



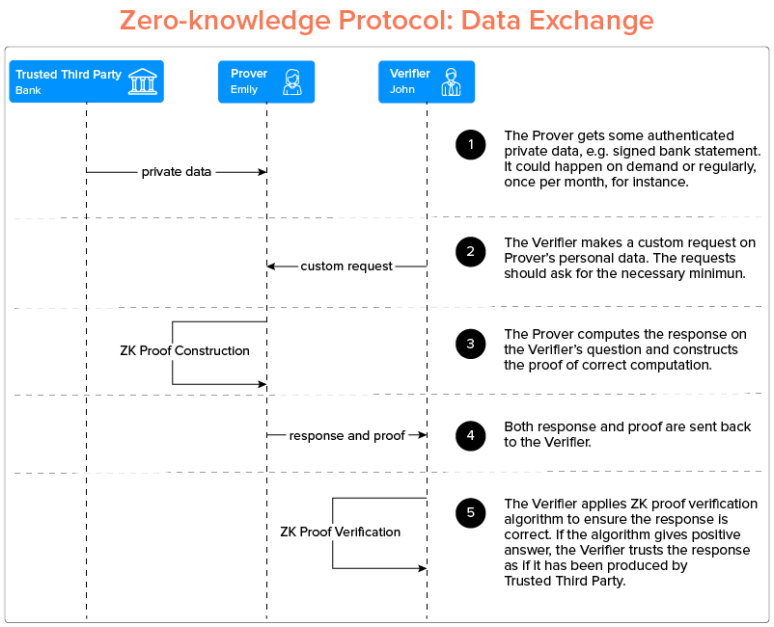
(2)

Figure 1: Journey of a transaction from the p2p network to being implemented in the blockchain

Why Zero Knowledge Proof can be used as a means of extra privacy

Consider a new applicant for a credit card who needs to convince the credit company that they have maintained sufficient average balance in their bank account over the last three months. The traditional way of doing this is for the applicant to share the bank statements over that period. But this reveals much more personal information than is necessary to the company. It not only reveals exact balance, but also the transaction details. Ideally, the applicant would like to convince the credit company that her private data satisfies the balance requirement without revealing either the exact balance or the transaction details. Zero knowledge proofs (ZKPs) is a technique by which an entity, or prover, with private data provides a verifiable proof to a verifier that certain property holds true for that data without revealing any additional information other than the truth of verified property. In our example, the credit applicant is the prover with the private data corresponding to the bank transactions and the verifier is the credit company which needs to verify only the monthly balance property **(9)**. The demand for privacy increased as cryptocurrency users understood that their transactions were easily traceable in the blockchain **(8)**.

This mode of security builds trusts between the sender and receiver in the digital network. Without such a mean the sender might be insecure about the transaction he is making due to the extra information being provided to the receiver, and there will be a bigger chance for hackers to intercept the information and gain enough knowledge to interrupt the blockchain causing various technical implications.



(1)

Figure 3: Process of data/transaction exchange using the Zero-knowledge Protocol

An important technique of ZKP- (zk-SNARKS)

One of the most popular techniques is zk-SNARKS (zero knowledge – Succinct Non-Interactive Argument of Knowledge). This technique can be used to define a quadratic equation which takes public data (known to all) and private data (only known to prover) and inputs to generate proof, which can then be validated by the verifier **(11)**.

A zk-SNARK consists of three algorithms G, P, V defined as follows:

The key generator G takes a secret parameter lambda and a program C, and generates two publicly available keys, a proving key pk, and a verification key vk. These keys are public parameters that only need to be generated once for a given program C.

The prover P takes as input the proving key pk, a public input x and a private witness w. The algorithm generates a proof prf = P(pk, x, w) that the prover knows a witness w and that the witness satisfies the program. The verifier V computes V(vk, x, prf) which returns true if the proof is correct, and false otherwise. Thus, this function returns true if the prover knows a witness w satisfying C(x,w) == true **(3)**.

An example program (3):

Suppose Bob is given a hash H of some value, and he wishes to have a proof that Alice knows the value s that hashes to H. Normally Alice would prove this by giving s to Bob, after which Bob would compute the hash and check that it equals H.
However, suppose Alice doesn't want to reveal the value s to Bob but instead she just wants to prove that she knows the value. She can use a zk-SNARK for this.

We can describe Alice's scenario using the following program, here written as a Javascript function:

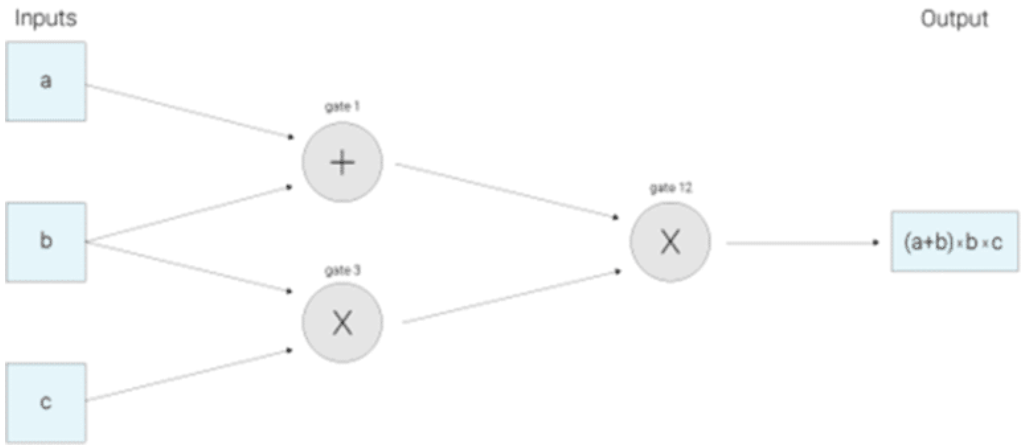
```
function C(x, w) {  return ( sha256(w) == x );}

Code language: JavaScript (javascript)
```

In other words: the program takes in a public hash x and a secret value w and returns true if the SHA–256 hash of w equals x. Translating Alice's problem using the function C(x,w) we see that Alice needs to create a proof that she possesses s such that C(H, s) == true, without having to reveal s. This is the general problem that zk-SNARKs solve.

How the cryptocurrency - ZCash uses zk-SNARKs

ZCash is a cryptocurrency with a decentralized blockchain that seeks to provide anonymity for its users and their transactions. ZCash increases user privacy by using zero-knowledge proofs (zk-SNARKs) to validate transactions without revealing information that could compromise a user's privacy **(11)**.
ZCash is one of the few coins using zk-SNARKs to ensure privacy required by users on their transactions. Blockchains heavily needed this extra layer to ensure the maximum confidentiality on the transactions taking place through the users all around the world on the network.

In order to have zero-knowledge privacy in Zcash, the function determining the validity of a transaction according to the network's consensus rules must return the answer of whether the transaction is valid or not, without revealing any of the information it performed the calculations on. This is done by encoding some of the network's consensus rules in zk-SNARKs. At a high level, zk-SNARKs work by first turning what you want to prove into an equivalent form about knowing a solution to some algebraic equations **(4)**.
The first step in turning our transaction validity function into a mathematical representation is to break down the logical steps into the smallest possible operations, creating an "arithmetic circuit". Similar to a Boolean circuit where a program is compiled down to discrete, single steps like AND, OR, NOT, when a program is converted to an arithmetic circuit, it's broken down into single steps consisting of the basic arithmetic operations of addition, subtraction, multiplication, and division **(4)**.



(4)

Figure 3: An example of what an arithmetic circuit looks like for computing the expression (a+b)*(b*c)

Our next step is to build what is called a Rank 1 Constraint System, or R1CS, to check that the values are "traveling correctly". In this example, the R1CS will confirm, for instance, that the value coming out of the multiplication gate where b and c went in is b*c **(4)**.

In this R1CS representation, the verifier has to check many constraints — one for almost every wire of the circuit. In a 2012 paper on the topic, Gennaro, Gentry, Parno and Raykova presented a nice way to "bundle all these constraints into one". This method uses a representation of the circuit called a Quadratic Arithmetic Program (QAP). The single constraint that needs to be checked is now between polynomials rather than between numbers. The polynomials can be quite large, but this is alright because when an identity does not hold between polynomials, it will fail to hold at most points. Therefore, you only have to check that the two polynomials match at one randomly chosen to point in order to correctly verify the proof with high probability. With zk-SNARKs, sophisticated mathematical techniques such as homomorphic encryption and pairings of elliptic curves are used to evaluate polynomials "blindly" – i.e. without knowing which point is being evaluated. The public parameters described above are used to determine which point will be checked, but in encrypted form so that neither the prover nor the verifier know what it is **(4)**.

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

Comparison between Bitcoin and Zcash

As a digital currency, ZCash is similar to Bitcoin. Like Bitcoin, ZCash also has an including its open-source code, but their major differences lie in the level of privacy and fungibility that each provides.

Bitcoin was a pioneer in the open financial system; ZCash seeks to maintain the same structure as Bitcoin but with privacy and fungibility as added feature. Bitcoin's solution to fraud and theft was to make all transactions totally transparent and one hundred percent traceable. Unfortunately, Bitcoin's deprecation of privacy is also a flaw that it has sought to solve. Some of Bitcoin's original users mistakenly believed that because wallet addresses were pseudonymous, that using Bitcoin was anonymous. However, legal action against darknet sites like the Silk Road proved that all it takes is a small amount of information in order to reveal the true identity behind a Bitcoin wallet. Zcash innovated by adopting Bitcoin's open ledger system and encrypting information about the ledger's users. This means that even though all ZCash transactions are recorded on a blockchain, the transactions are encrypted and can only be viewed by users that have been given access to them **(11)**.

***Author**: Vayk Mathrani*

REFERENCES

1. Blockchain: The Fundamentals of Decentralization {Infographic} By Chirag Bhardwaj November 15, 2019 7. min read [Available From: https://appinventiv.com/blog/basics-of-blockchain-infographic/]
2. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar, A survey on privacy protection in blockchain system, Journal of Network and Computer Applications, Volume 126, 2019, Pages 45-58, ISSN 1084-8045. [Available From: https://doi.org/10.1016/j.jnca.2018.10.020. (https://www.sciencedirect.com/science/article/pii/S1084804518303485)
3. Introduction to zk-SNARKs, An overview of zero-knowledge proofs and how to integrate zk-SNARKs into Ethereum. by ConsenSys March 27, 2017
4. [Available From: https://consensys.net/blog/developers/introduction-to-zk-snarks/]
5. What are zk-SNARKs? Zcash [Available From**:** https://z.cash/technology/zksnarks/]
6. Blockchain: The Fundamentals of Decentralization {Infographic} By Chirag Bhardwaj November 15, 2019 7. min read [Available From: https://appinventiv.com/blog/basics-of-blockchain-infographic/]
7. What is Zero-Knowledge Proof & its Role in the Blockchain World? By Chirag Bhardwaj January 9, 2020 8. min read [Available From: https://appinventiv.com/blog/zero-knowledge-proof-blockchain/]
8. Zero-knowledge proofs – a powerful addition to blockchain by Danielle Enwood | Jun 1, 2021 | [Available From: https://blockheadtechnologies.com/zero-knowledge-proofs-a-powerful-addition-to-blockchain/]
9. Privacy in blockchain collaboration with zero knowledge proofs. January 16, 2019 | Written by: Vinayaka Pandit and Pankaj Dayama [Available From: https://www.ibm.com/blogs/blockchain/2019/01/privacy-in-blockchain-collaboration-with-zero-knowledge-proofs/]
10. Establishing blockchain privacy through Zero Knowledge Proof June | 2019. Written by: Hitarshi Buch [Available From: https://www.wipro.com/blogs/hitarshi-buch/establishing-blockchain-privacy-through-zero-knowledge-proof/
11. ZCash By Jake Frankenfield April 30, 2020 [Available From: https://www.investopedia.com/terms/z/zcash.asp]