Democracy Enhancing Technologies

Jeremy Clark

A Thesis in
The Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy
(Information and Systems Engineering)
at
Concordia University
Montréal, Québec, Canada Test

September 2023

Abstract

Name: **Jeremy Clark**

Title: **Democracy Enhancing Technologies**

Hello. No more than 250 words.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Diam donec adipiscing tristique risus nec feugiat in fermentum posuere. Et netus et malesuada fames ac turpis. Nullam non nisi est sit. Felis eget velit aliquet sagittis id. Mauris commodo quis imperdiet massa tincidunt. Tellus molestie nunc non blandit massa enim nec. Facilisis mauris sit amet massa. Et molestie ac feugiat sed. Metus vulputate eu scelerisque felis imperdiet proin.

Acknowledgments

Hello.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Diam donec adipiscing tristique risus nec feugiat in fermentum posuere. Et netus et malesuada fames ac turpis. Nullam non nisi est sit. Felis eget velit aliquet sagittis id. Mauris commodo quis imperdiet massa tincidunt. Tellus molestie nunc non blandit massa enim nec. Facilisis mauris sit amet massa. Et molestie ac feugiat sed. Metus vulputate eu scelerisque felis imperdiet proin.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Focus on making proof of liabilities for the real world that can be used by marketplaces.

Scope. Blah blah blah.

Contributions. Our primary contributions are as follows.

1. Blah blah blah.

2. Blah blah blah.

3. Blah blah blah.

Chapter 2

Background

In this chapter, we dive into the realms of Bitcoin, cryptocurrency markets, and digital exchanges. We explore the concepts of zero-knowledge proofs and succinct non-interactive arguments of knowledge (zk-SNARKs), shedding light on their significance within the cryptographic landscape. Subsequently, we transition to discussing proof of solvency, elucidating its evolution and assessing its present state within financial frameworks.

2.1 Bitcoin

Bitcoin is recognized as the world's first successful cryptocurrency and decentralized digital currency. The goal of Bitcoin is to allow financial transactions to be settled on its own, without the need of a middleman, typically financial institutions. Bitcoin is built on a peer-to-peer network, which means that every participant helps in safe keeping the transactions history, and propagading the new transactions. There is no single point of failure. This allows for transactions to occur in real time, in contrast to the delays encountered in the traditional finance world. Bitcoin defines two different concepts: Bitcoin the cryptocurrency, and Bitcoin the blockchain. The cryptocurrency resides on the blockchain. The Bitcoin blockchain is a decentralized ledger that records all Bitcoin (the cryptocurrency) transactions immutably and transparently. This blockchain serves as a verifiable record of all Bitcoin transactions, accessible to every participant in the network. The transparency afforded by the public blockchain engenders trust and accountability.

2.1.1 Transactions

For every participant of the network, there is a public key, a private key and a wallet address associated with the participant. The public key is derived from the private key using elliptic curve multiplication, and the wallet address is derived from the public key using a hashing function. Both are one way function, meaning you cannot derived the other way around. The public key serves as the unique identifier in the network, but it is the wallet address that typically defines a participant. The wallet address can be seen as a bank account number. When you send bitcoin to someone, you send it to their wallet address. To be able to send some bitcoin, you need to create a transaction and send it to the network. When transactions are sent on the network, there is no way of knowing who propagaded the transaction first. We need to make sure a transaction originates from the sender. The way to do that is to sign your transaction. The digital signature is created from the transaction data and the private key, which is only known by the owner of the address. The public key is then used to verify the authenticity of the signature. Sending a transaction is the easiest problem to solve. The real challenge is to keep track of who owns what, and to avoid the double spending problem. The methodology for managing this is to keep the history of every single transactions. The transactions are bundled up into blocks, and the chain of blocks create the blockchain.

2.1.2 Network

The challenge of the network, is to have every single node achieve consensus on the transaction history. Nodes are computers connected to the network, working on publishing new blocks. The nodes work collectively to establish order of transactions (sequencing). Every new transaction is broadcaseed to all nodes. The nodes puts the transactions into a block, and try to publish that block. In order to publish a block, each node needs to solve a proof-of-work challenge. When a node solves the challenge, it broadcasts the block to every nodes. The nodes accepts the block if all transactions are valid. There is no formal way of approving a new block. A node show its acceptance by starting to work on a new block using the hash of the accepted block as previous hash. Some nodes might accept different blocks, if multiple blocks are propagaded at the same time. This would create mutliple chains. To solve this issue, the longest chain is considered to be the correct one. If two chains have the same length, nodes keep working on their respective chains untill one of the chains receives a new block, breaking the tie.

2.1.3 Proof-of-work

In order to submit a new block, a node have to find a hash with a specific number of leading zero bits. It is exponentially more difficult for every zero bit. This cryptographic puzzle serves as a barrier to entry, ensuring that a lot of computational power was spent on creating the block. The way to test different hash values, is to change the block timestamp, and the nonce value. The nonce value is there solely for that purpose. Once a block is published, you cannot change any value inside of it because the hash value would change. The immutability of the older blocks is what makes Bitcoin secure. To modify a block in the middle of the chain, you would need to redo the work of every single blocks made after that. The longest chanin is determined by the cumulative proof-of-work invest in it. This is why we say that Bitcoin is secured as long as 51 pourcent of the nodes are honnest. The chain with the majority of nodes working on it will grow up the fastest, thus will be the accepted chain. The difficulty of the new block is determined by an average, in order to generate blocks at a steady pace. There is also a bitcoin reward associated with mining (publishing) a block.

2.1.4 Merkle Tree

In the architecture of the blockchain, only the merkle root is stored in the block header. Nodes only keep the recent blocks in memory. For the older blocks, they keep only the block header in memory. This storage ensures the integrity of the blockchain, while decreasing the memory required to have the full blockchain history. Since the hash of a block is the hash of the block header, this strategy does not impact the integrity checks of the blockchain. The merkle root is the top of the Merkle Tree, and is a unique identifier of the full tree. A merkle tree is a tree where the parent node is the hash of the child nodes. The tree is immutable because changing a single node would have an impact on the merkle root. For instance, in figure 2.1 chaning the transaction 0 whould change the hash 0, which in turn would change the hash 01, subsequently changing the root hash.

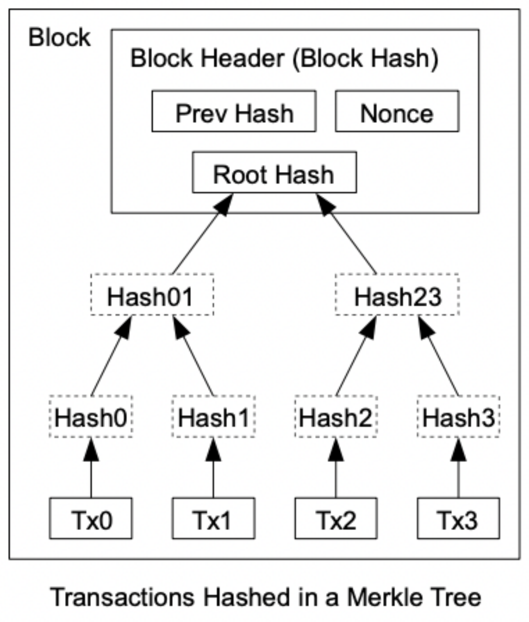


Figure 2.1: Bitcoin Merkle Tree [1]

For individuals new to the realm of Bitcoin, marketplaces stand out as the optimal avenue for purchasing this digital asset. These platforms facilitate the seamless exchange of traditional currency for Bitcoin, offering an accessible entry point into the world of cryptocurrencies. However, it's crucial to understand that the Bitcoin obtained through these marketplaces initially remains under the custody of the platform itself, rather than being directly linked to a personal wallet address.

While marketplaces provide a convenient avenue for acquiring Bitcoin, the initial custody arrangement may raise concerns about transparency and control. Nevertheless, once the Bitcoin is securely stored in a personal wallet, users can enjoy the benefits of decentralized transactions without the need for continuous reliance on intermediaries. This newfound financial autonomy empowers individuals to engage with the Bitcoin network on their own terms, fostering a deeper understanding of and participation in the world of cryptocurrencies.

2.2 Marketplaces

The best way to buy bitcoin for the first time is through marketplaces. Marketplaces facilitate the exchange of traditional currency for bitcoin. However, it is crucial to understand that the Bitcoin obtained remain into the custody of the platform, rather than being deposited to a personnal wallet address. In order to gain custody of your bitcoins in your wallet, you need to enter a transfer request. This is similar to tradinitonal finance, where you trust the bank (marketplace), to go ahead with your transaction. Once you have bitcoins in your wallet, you can transact on the network without needing a 3rd party. Unless you are running a node, you will need to trust a 3rd party, wheter it is a marketplace, or over the counter, to first acquire bitcoin.

When the bitcoin you own is in custody of the marketplace, there is no way to see your bitcoin onchain. Marketplaces have many wallets, some are made public and some are not. While this allo for the privacy of your marketplace deposits and withdraws, it represent an fondamental contradiction. Bitcoin was designed to be transparent and public, without the need of a 3rd party to do a transaction. Not being able to track your bitcoin in the marketplace pauses a significant challenge. A user has no proof that the marketplace solvency to reimburse every client. However, this problem is being actively worked on. Marketplaces have begin to use proof of solvency (or proof of reserve) to demonstrate that they are solvent. While this is a step in the right direction, the current proof of solvency used by the marketplaces have many default, and they are not sufficient to prove that they are solvent.

2.3 Zero Knowledge

Zero-knowledge proofs is a cryptographic technique to prove some knowledge without divulging any informations.For instance, the classic way of proving that you know the solution to an equation, is to reveal the solution to the equation itself. However, with zero knoledge you are able to prove that you know the solution, without discolsing the solution. To construct a zero knowledge proof, you need to construct a proof that is sound and complete. You also need your proof to be zero knowledge[3].

- **Completeness**: If the statement is true, an honest verifier will be convinced by an honest prover.
- **Soundness**: If the statement is false, no dishonest prover can convince the

honest verifier (except with some infinitysimal probability).

- **Zero-Knowledge**: If the statement is true, a verifier learns nothing other than the fact that the statement is true. [4]

2.3.1 Non interactive proofs

Zero knowledge proofs were originaly designed as interactive, that is multiple rounds of interaction between the prover and the verifier [5]. leading to what are called interactive zero-knowledge proofs. This interaction allos the prover to demonstrate knowledge of the solution without revelaing any additionnal information. An alternative model was then proposed where the verifier and prover use a reference string that is shared during a trusted setup. Once we have the reference string, a single message is needed between the prover and the verifier. The elimination of multiple rounds of interaction simplifies the verification process and reduces the computational power required. Therefore, noninteractive zero-knowledge proofs offer enhanced efficiency and scalability, which will be needed later on. [6] [7]

2.3.2 SNARKS

One of the recent advancement for non-interactive proofs is what is known as SNARK (non-interactive argument of knowledge). This means a proof that is:

- **Succinct**: the size of the proof is very small compared to the size of the witness.

- **Non-interactive**: No rounds of interactions between the prover and the verifier.

- **Argument**: Secured only for provers with bounded computational ressources, that is a dishonest prover with unlimited computational power could prove a wrong statement.

- **Knowledge-sound**: If the statement is true, a verifier learns nothing other than the fact that the statement is true. [9]

Moreover, a SNARK can also be zero-knowedge, where the prover demonstrate knowledge without revelaing any additionnal information about the witness. We call such proof a zk-SNARK.

2.3.3 Arithmetic circuit

Arithmetic circuits are a core component of SNARKS. An arithmetic circuit is a set gates, each assigned a distinct set of inputs corresponding to the numbers to be processed in the operation. These gates are configured to execute arithmetic operations such as addition, subtraction, multiplication, or division. The outputs of the gate circuit represent the digits of the resulting computation. This structure allows SNARKs to efficiently verify complex mathematical computations while preserving succinctness and scalability.

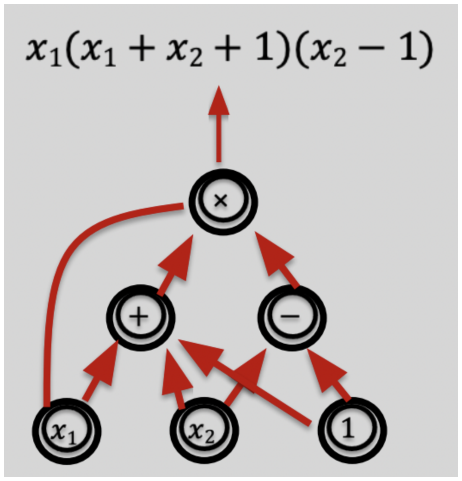
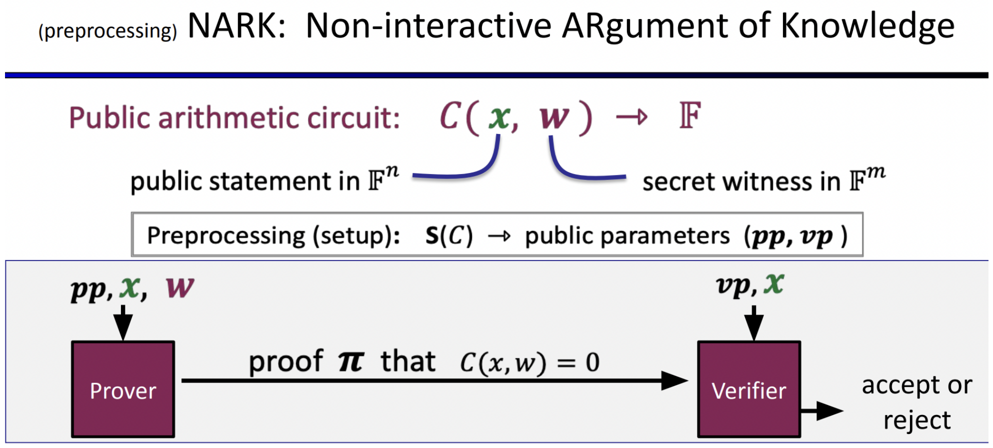


Figure 2.2: General Arithmetic circuit [8]

The prover's process in SNARKs is to create a proof using the setup parameter, a private witness, and public input. Thr proof shows that the arithmetic circuit is equal to 0. Using the same setup parameter and the public input, the verifier confirms the accuracy of the proof by making sure it aligns with the parameters.



(preprocessing) NARK: Non-interactive ARgument of Knowledge
Public arithmetic circuit: $C(x, w) \rightarrow \mathbb{F}$
public statement in $\mathbb{F}^n$
secret witness in $\mathbb{F}^m$
Preprocessing (setup): S(C) → public parameters (pp, vp)
pp, x, w
vp, x
Prover
proof π that $C(x,w) = 0$
Verifier
accept or reject

Figure 2.3: Arithmetic circuit for SNARK [8]

- **S(C)**: Public parameters (pp,vp) for prover and verifier

- **P(pp,x,w)**: Proof π
- **V(vp,x,π)**: Accept or reject
- **C(x,w)**: Arithmetic circuit
- **w**: Private witness
- **x**: Public input

2.4 Proof of solvency

A proof of solvency is a system where we prove that someone, in most cases an exchange, hold enough assets to cover the balance of every customers. In traditional finance, this would be done thourgh an audit. While an audit can be usefell, it has many downfalls. Obviously it requires the trust of another 3rd party, but it poses also a time constraint. You cannot hold an audit every single day, and in the bitcoin world things move fast. It is essential to be able to fill a prove of solvency every single day.

A proof of solvency is composed by a proof of assets, where we prove what assets the marketplace owns, and the proof of liabilities, where we prove what the total amount of user deposits.

The first paper about a proof of solvency focuses only on the proof of liabilities. In his paper Gregory Maxwell addresses the issue of verifying the solvency of Bitcoin exchanges. [11] Maxwell's system ensures user privacy by maintaining confidentiality of individual account balances, while only revealing aggregate information in the proof of liabilities. This is achieved through the application of Merkle trees.

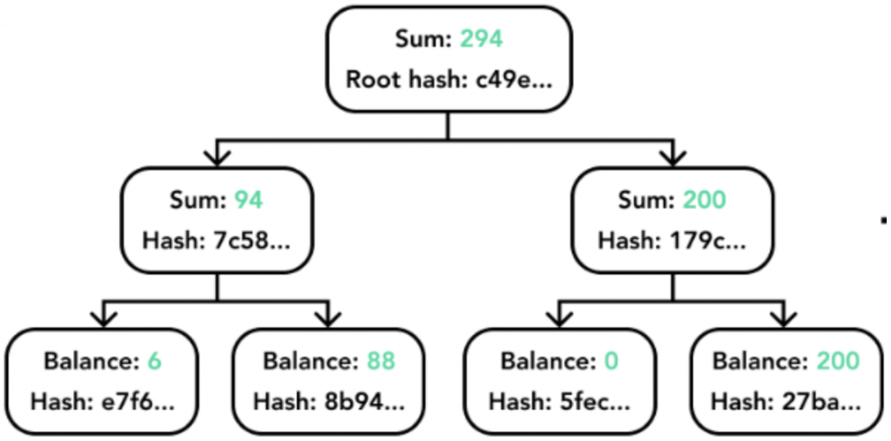


Figure 2.4: Merkle tree for proof of liabilities

In the Merkle tree, every node contains a user's balance along with a hash-based commitment incorporating the customer ID and a nonce. The root of the tree is the sum of the balances. To verify their inclusion in the total liabilities, users receive a subset of the hash tree from the exchange. This subset includes the user's nonce and the sibling nodes along the unique path from the user's leaf node to the root. By comparing the received information to the exchange's broadcasted root node, users can confirm the inclusion of their balance. While elegant, the protocol does have privacy implications. The exact value of the exchange's total liabilities, published in the root node, may be sensitive data. Additionally, the proof of inclusion reveals the neighbor's balance, and the subtree's balance along the Merkle path.

The proof of liabilities is only part of the proof of solvency. A complete proof of solvency needs a proof of asset as well. Provision describes the first preserving privacy proof of asset [10].

In Provisions, the focus shifts towards preserving privacy while still proving ownership of assets. Instead of publicly demonstrating control over specific addresses, Provisions enables exchanges to prove ownership of an anonymous subset of addresses sourced from the blockchain.

Since these 2 papers, a lot of work was done to make the proof of solvency evolve. However, marketplaces still do not use proof of solvency, or implement a proof of solvency with some flaws.

2.4.1 Real world proof of solvency

Binance has taken the first step in the right directions by having a proof of reserves[2]. Every month, they publish a merkle tree with the sum of their liabilities. They also publish a list of the assets they possess. However there is many thing wrong with there proof of reserves. They do not show that they have control over the wallets. They only pusblish a proof every month, which leaves them plenty of time to be unsolvent, since the crypto market is quite fast.

Crypto.com did a 1 time audit as a proof of reserve[12]. Kraken also does a proof of liabilities every few months, but no proof of assets[13].

Overall, here is all the reasons that the current proof of solvencies are insufficient. Proof of liabilities every month is not enough. No proof of assets, so they could lie their assets, pusblish a list of wallets that they do not have control over.

Chapter 3

Recursion proofs

Chapter 4

Proof of liabilities

Bibliography

[1] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report, Bitcoin.org, 2008.

[2] Binance. Proof of Reserves. `https://www.binance.com/en/proof-of-reserves`.

[3] Boaz Barak. Lecture 14: Zero knowledge proofs. `https://www.boazbarak.org/cs127spring16/chap14_zero_knowledge.html`.

[4] LCX Team. Introduction to Zero-Knowledge Proofs. November 3, 2023. `https://www.lcx.com/introduction-to-zero-knowledge-proofs/`.

[5] Goldwasser, S., Micali, S., Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1), 186–208. 1989.

[6] Blum, M., Feldman, P., Micali, S. Non-Interactive Zero-Knowledge and Its Applications. *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, 103–112. 1988.

[7] Goldreich, O., Micali, S., Wigderson, A. Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model? *STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing*, 113–131. 1991.

[8] Dan Boneh, Shafi Goldwasser, Dawn Song, Justin Thaler, Yupeng Zhang. Zero Knowledge Proofs: Introduction to Modern SNARKs. 2023.

[9] Nitulescu, Anca. *zk-SNARKs: A Gentle Introduction.* 2020.

[10] Dagher, Gaby G., Bunz, Benedikt, Bonneau, Joseph, Clark, Jeremy, and Boneh, Dan. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. October 26, 2015.

[11] Malkhi, Dahlia. Exploring Proof of Solvency and Liability Verification Systems. Published January 5, 2023. Updated November 27, 2023. `https://blog.chain.link/proof-of-solvency/`.

[12] Mazars. Proof of Reserve Report. December 9, 2022. `https://www.crypto.com/proof-of-reserve`.

[13] Kraken. Proof of Reserves. `https://www.kraken.com/proof-of-reserves`.