Bitcoin: A Peer-to-Peer Electronic Cash System - A Walkthrough

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Agenda

- Introduction
- Transactions
- Timestamp server
- Proof-of-Work
- Network
- Incentive
- Reclaiming Disk Space
- Simplified Payment Verification
- Combining and Splitting Value
- Privacy
- Calculations

Introduction

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Introduction

- “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto

- A purely **peer-to-peer** (p2p) version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

- Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes.

Introduction (Cont'd)

Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

This paper proposes a solution to the **double-spending** problem using a p2p network.

- No mechanism exists to make payments p2p without a trusted party.

Transactions

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Transactions

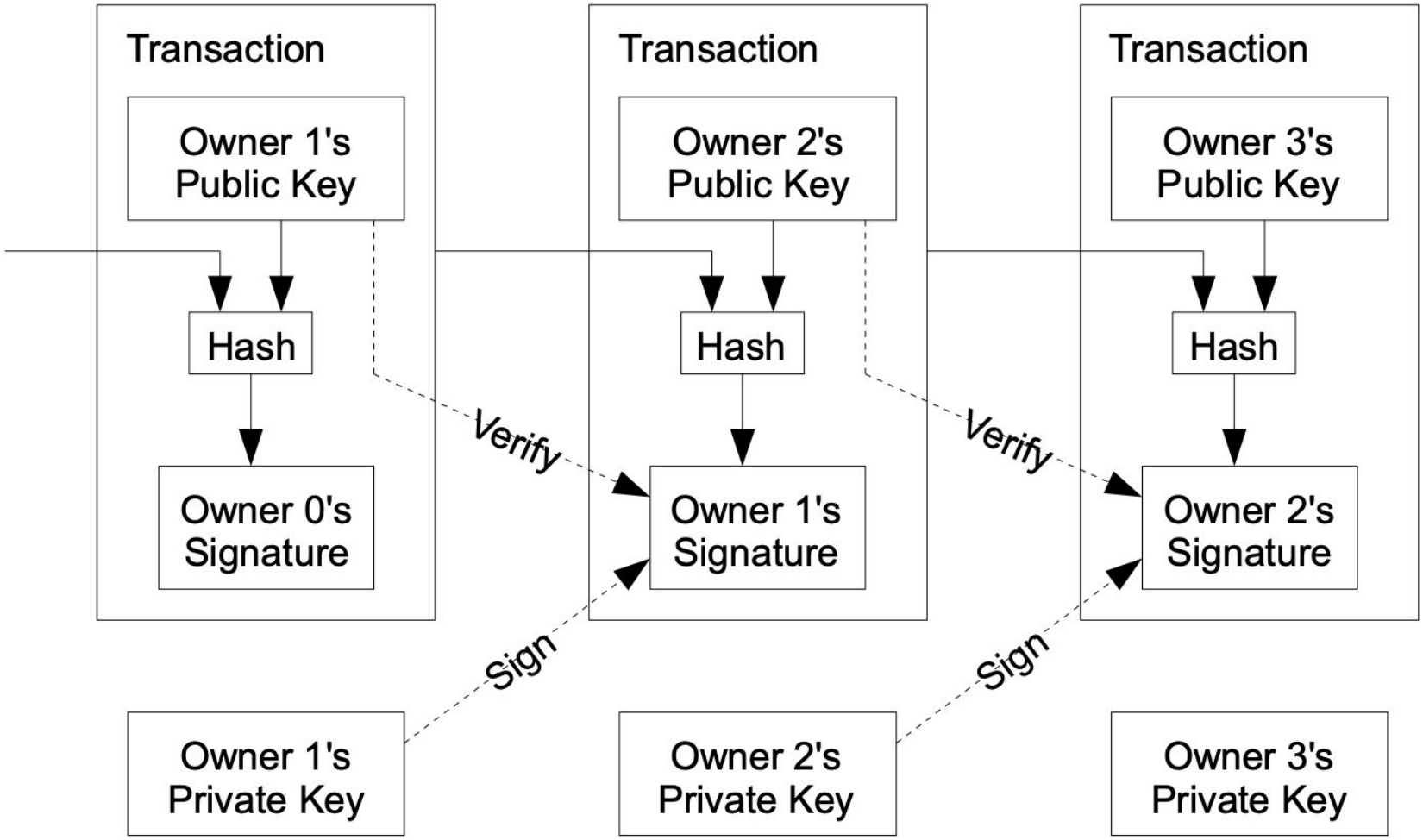


Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Transactions (Cont'd)

- Bitcoin owners want to transact.
  - The network broadcasts the bitcoin value when the owner transfers the currency.

- The owner digitally signs and encrypts the hash of the previous transaction to transfer the currency to the next owner.
  - Two mathematically linked keys—public and private—encrypt Bitcoin.

Transactions (Cont'd)

- The **public key**, such a bank account number, is used to encrypt the transaction with the owner's private key to form a digital signature. Thus, the public key is the recipient's address.

- Naturally, the next owner, the receiver, wants to make sure the sum provided to them has not been spent before. Only by agreeing on all previous transactions in sequence can the network guarantee this.

Transactions (Cont'd)

- The network has to agree on rules to publicly disclose the valid order of all transactions.

- Each transaction receiver seeks verification that the majority of the network agrees that they were the first to get this transaction and no other recipients have gotten it before.

Timestamp Server

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Timestamp Server

- Works by taking a hash of a block of items to be time-stamped and widely publishing the hash, such as in a newspaper.

- The timestamp proves that the data must have existed at the time, in order to get into the hash.

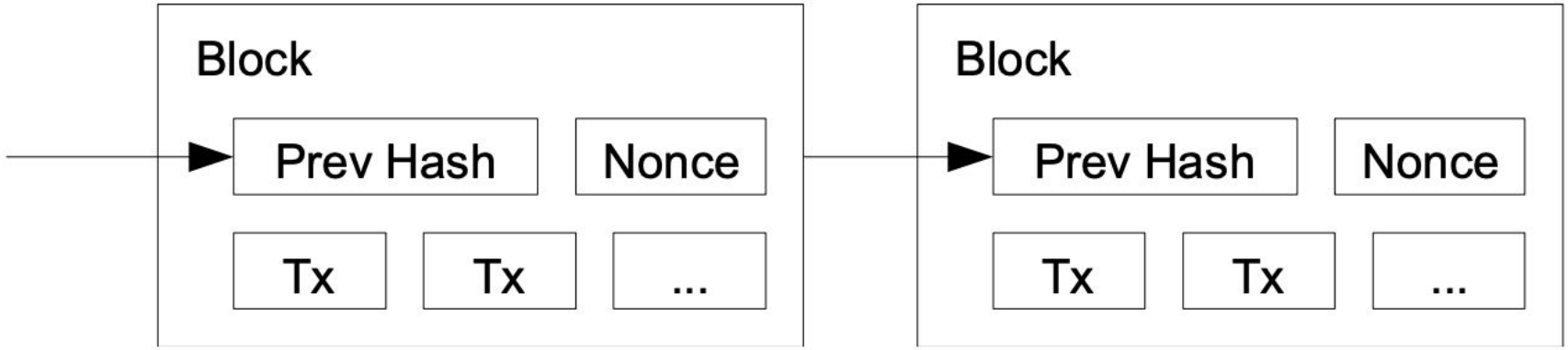
- Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

Proof-of-Work

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

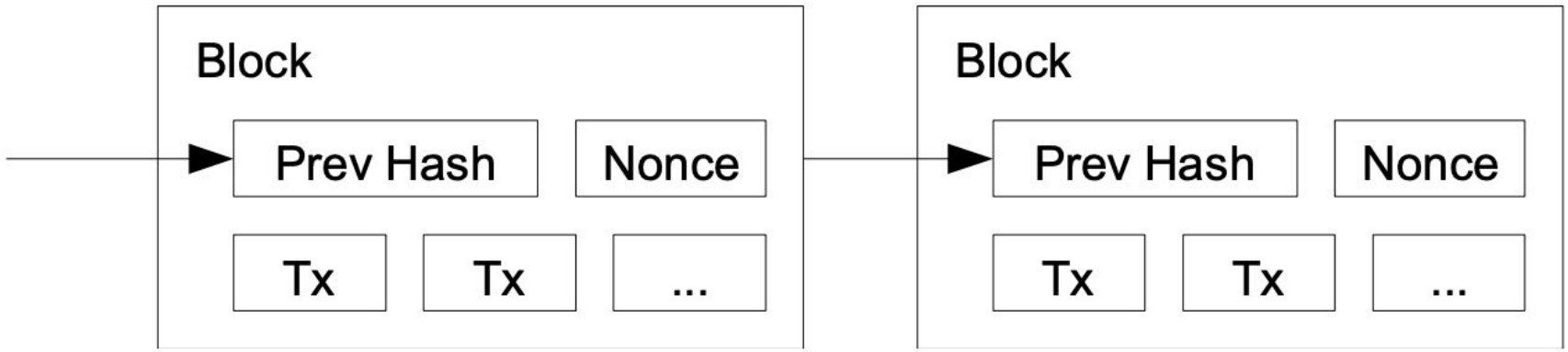
Proof-of-Work



A **block** contains data - Nonce, the timestamp, number of the transactions, the hash of the previous block and further information.

Image Source: [1] S. Nakamoto, “A peer-to-peer electronic cash system,” *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

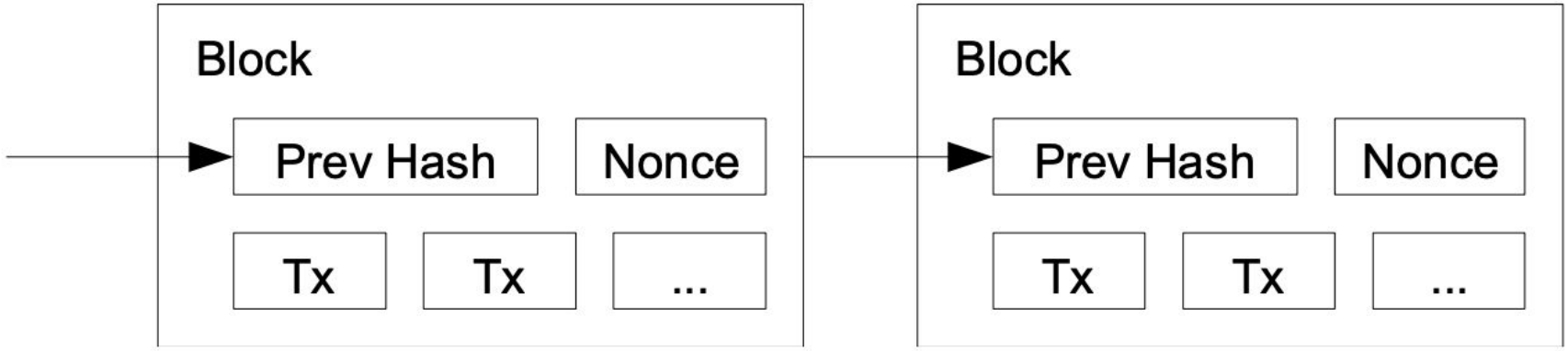
Proof-of-Work (Cont'd)



- Pick a **nonce** such that H(prev hash, nounce, Tx) < E.
  - E is a variable that the system specifies.
- Basically, this amounts to finding a **hash value** whose leading bits are zero (0).
  - The work required is exponential in the number of zero (0) bits required.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Proof-of-Work (Cont'd)



Proof-of-work (POW) is **hard**…

- Difficult
- Costly
- Time-consuming to create

…but **easy** to verify.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Network

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Network

Steps to run the network:

1. New transactions are broadcast to all nodes.

2. Each node collects new transactions into a block.

3. Each node works on finding a difficult POW for its block.

Network (Cont'd)

4. When a node finds a proof-of-work, it broadcasts the block to all nodes.

5. Nodes accept the block only if all transactions in it are valid and not already spent.

6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Incentive

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Incentive

A block's initial transaction is a unique transaction that launches a new coin held by the block's inventor.

- Since there is no central authority to produce money, this gives nodes an added motivation to promote the network and offers a mechanism to initially disperse funds into circulation.

The continuous creation of a fixed number of new coins is comparable to gold miners investing resources to increase the quantity of gold in circulation.

- In our situation, the resources used are CPU time and power.

Incentive (Cont'd)

- Once the majority of bitcoins have been mined, the block reward will become an insignificant percentage of miners' overall earnings.

- The incentive can also be funded with transaction fees.
  - Fees incentivize miners to include transactions in a block.

Incentive (Cont'd)

If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction.

Currently, if a miner is able to successfully add a block to the blockchain, they will receive 6.25 bitcoins as a reward.

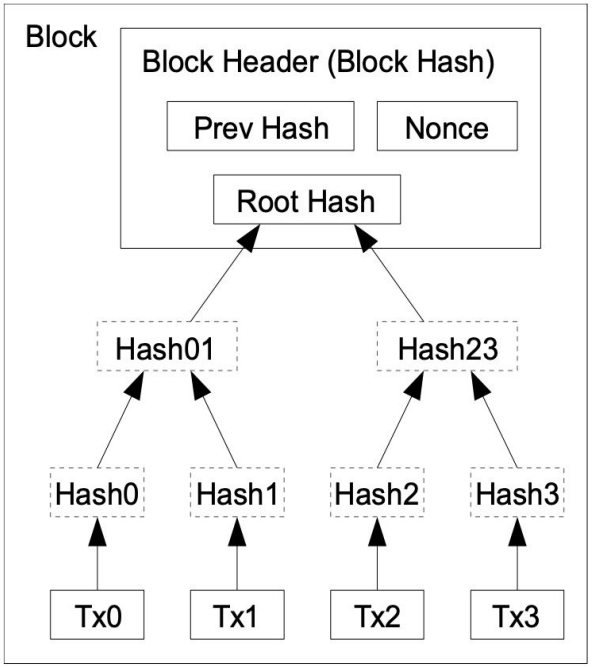
- The reward amount is cut in half roughly every four years, or every 210,000 blocks.

Reclaiming Disk Space

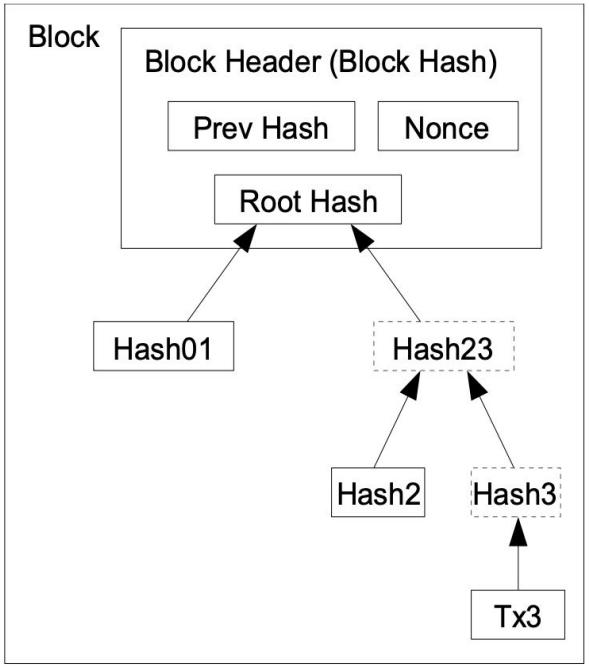
Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Reclaiming Disk Space



Transactions Hashed in a Merkle Tree

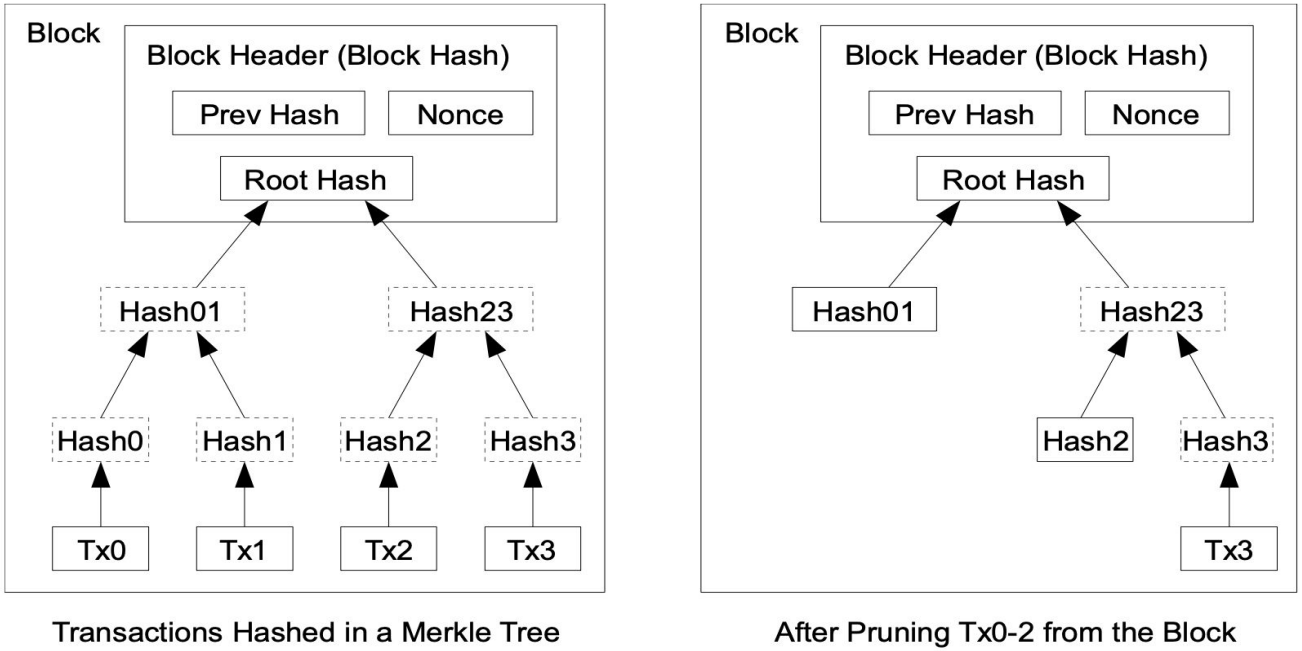


After Pruning Tx0-2 from the Block

Since the Bitcoin blockchain is immutable, it was inevitable that it would take a lot of memory to store. The Bitcoin Whitepaper assumes an 80-byte block header without transactions.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Reclaiming Disk Space



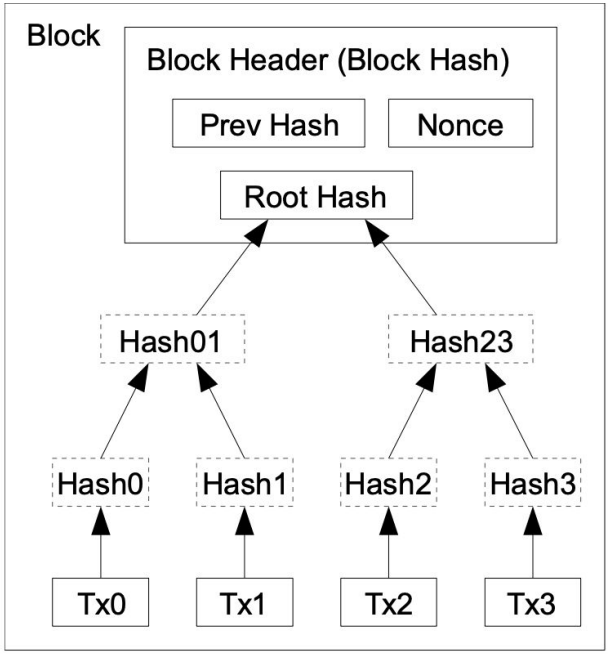
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

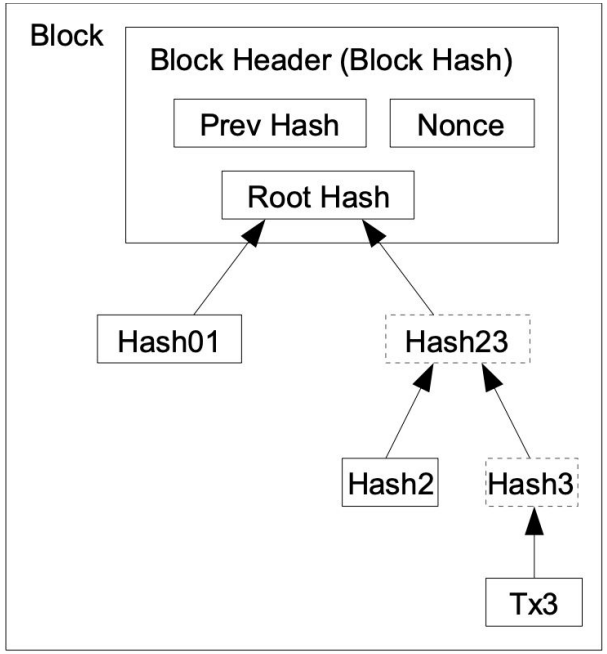
- Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Reclaiming Disk Space (Cont'd)



Transactions Hashed in a Merkle Tree

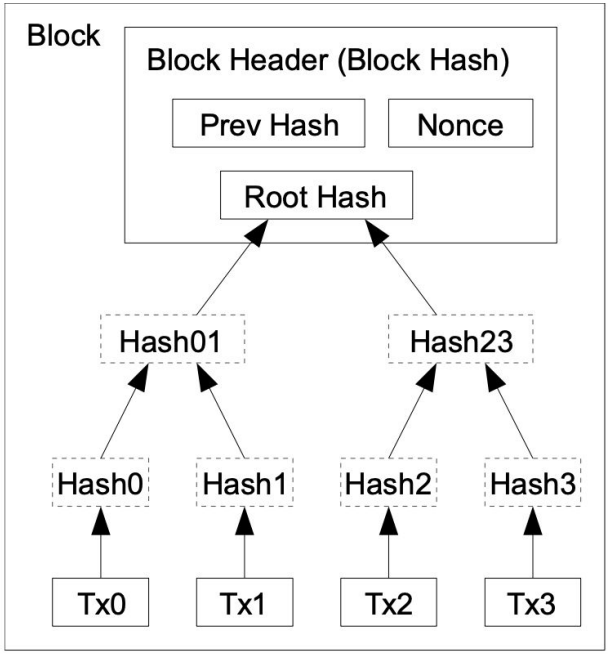


After Pruning Tx0-2 from the Block

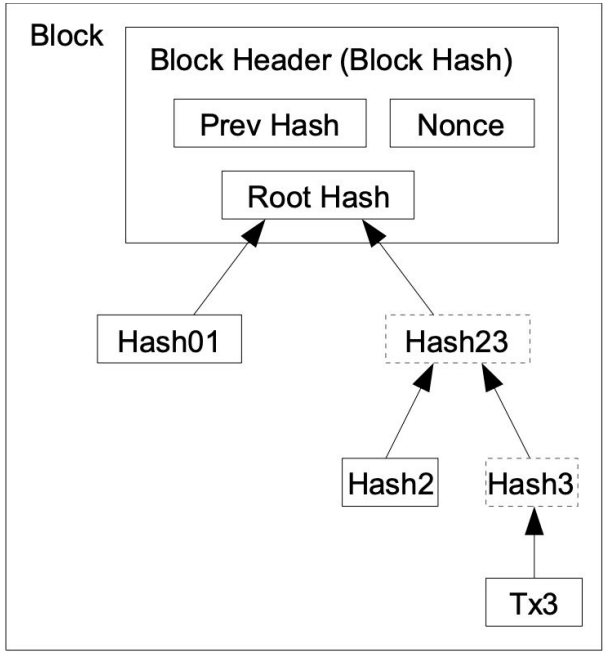
To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree, with only the root included in the block's hash.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Reclaiming Disk Space (Cont'd)



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Simplified Payment Verification

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Simplified Payment Verification

- User only needs to keep a copy of block headers of the longest POW chain, and obtain the Merkle branch linking to its transaction, he can see that a network node has accepted it.

- Transaction contain multiple inputs and outputs.

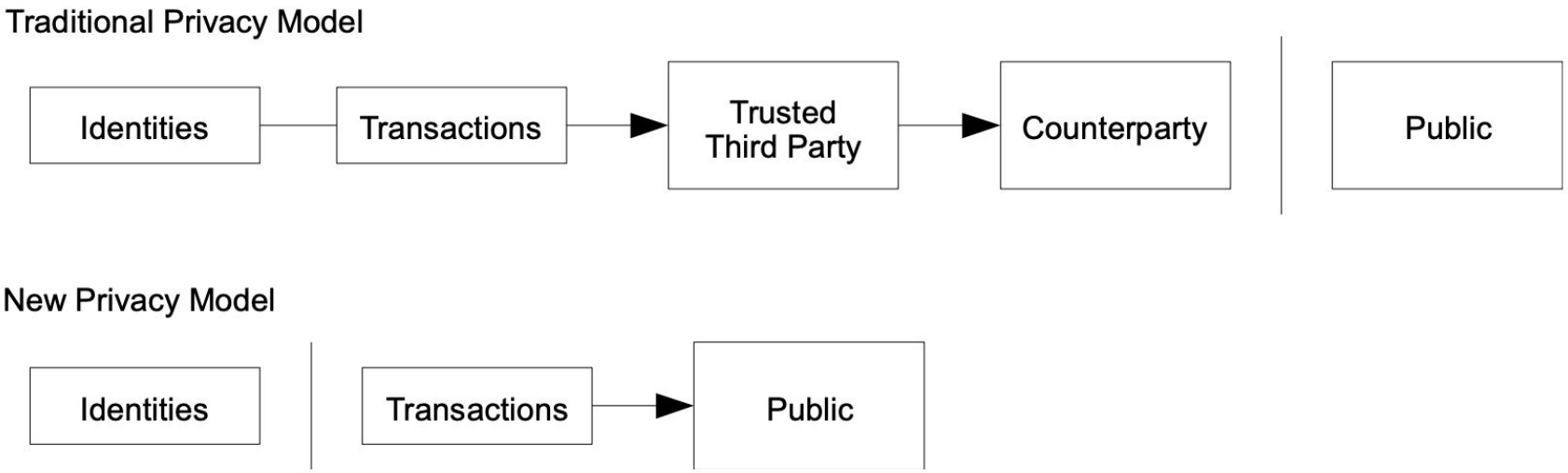
- Normally with a single input from a larger previous transaction or multiple inputs combining smaller amounts, and two outputs: one for payment and one for returning.

Privacy

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

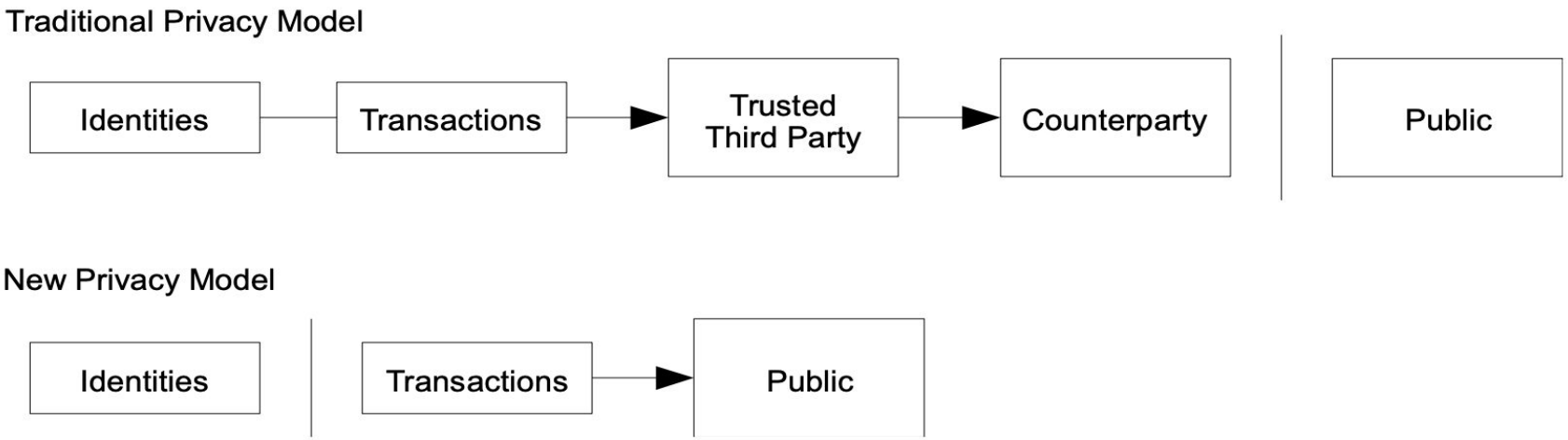
Privacy



The traditional banking model achieves a level of privacy by limiting access to information to the parties involved.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

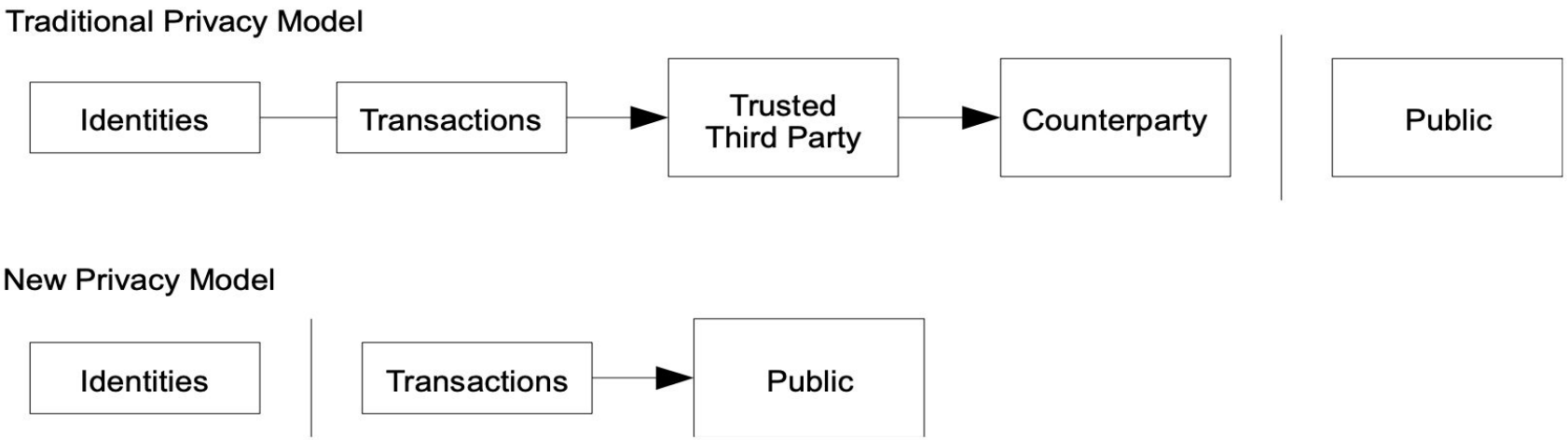
Privacy (Cont'd)



On the other side, the Bitcoin network makes all transactions public. Even if everyone can see that a transaction is being sent, no one can be connected to it since no one is aware of who the people are who are really acting.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

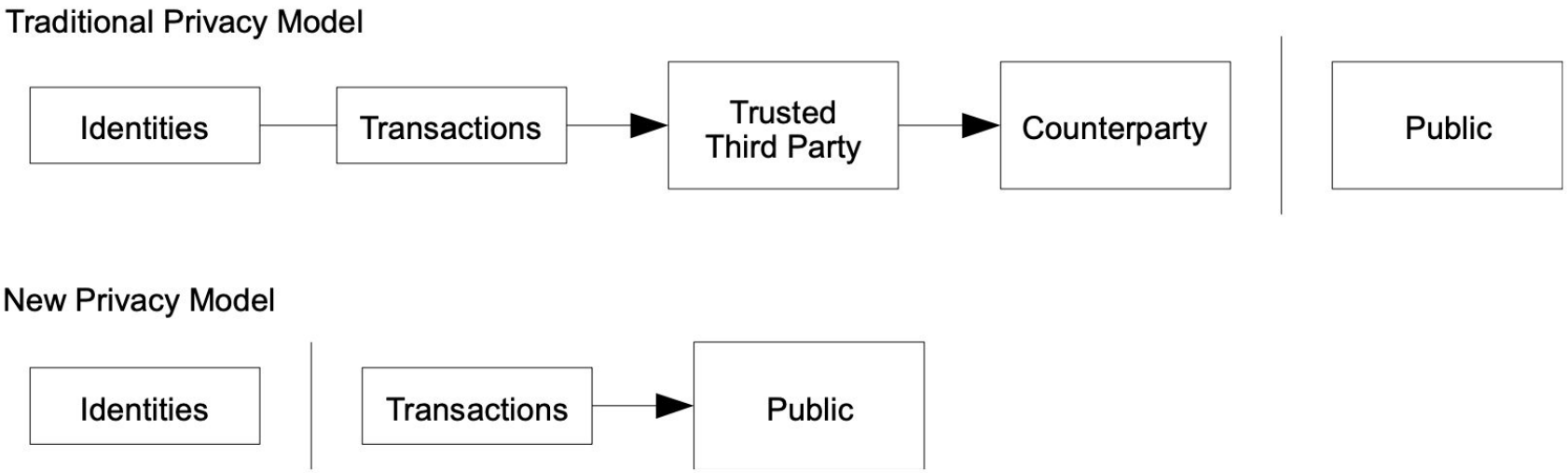
Privacy (Cont'd)



- But privacy can still be maintained by keeping public keys anonymous.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

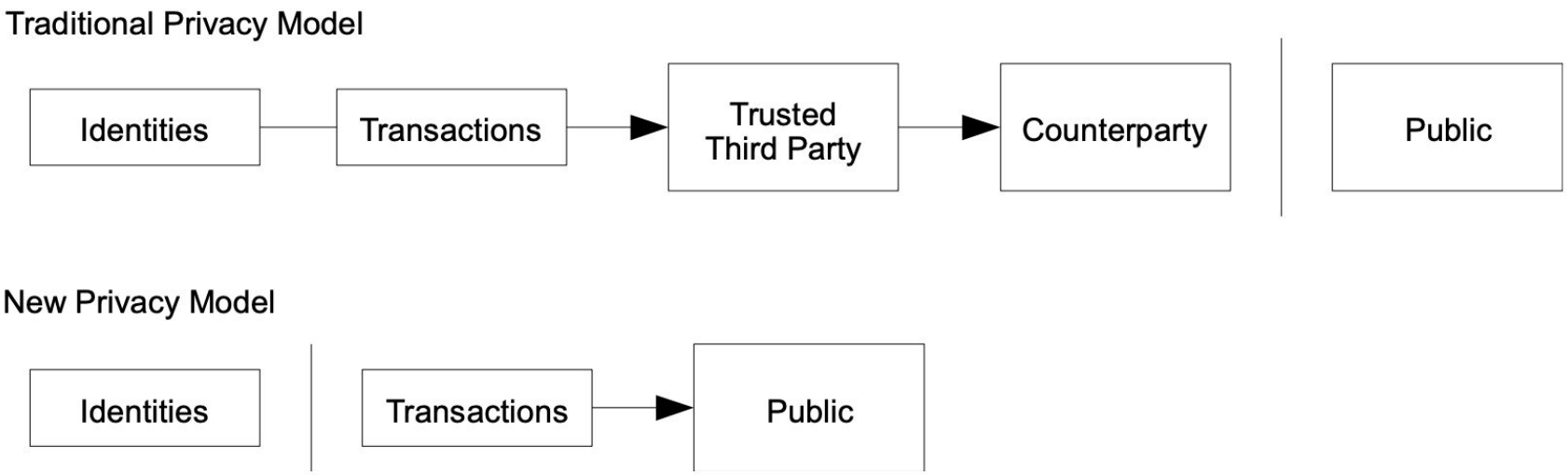
Privacy (Cont'd)



- Public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone (e.g., stock exchanges).

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Privacy (Cont'd)



- Additional firewall: address is created for each transaction to keep them from being linked to a common owner.

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Calculation

Swathi Punathumkandi, PhD

Ira A. Fulton Schools of Engineering
Arizona State University

Calculation

- An attacker generates an alternative chain quicker than the honest chain.
  - Even if this is done, it does not expose the system to arbitrary alterations like producing value from nothing or stealing money that never belonged to the attacker.

- Honest nodes will never accept a block with incorrect transactions as payment.
  - An attacker can only attempt to reverse a transaction he made.

Calculation (Cont'd)

- The honest chain and attacker chain race is a Binomial Random Walk.
  - The honest chain extends by one block and gains +1, whereas the attacker's chain extends by one block and loses -1.
- Gambler's Ruin applies to an attacker's chance of catching up.
  - A gambler with limitless credit begins at a loss and plays possibly endless trials to breakeven.

Calculation (Cont'd)

Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows:

p = probability an honest node finds the next block

q = probability the attacker finds the next block

q_z = probability the attacker will ever catch up for the z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Calculation (Cont'd)

The recipient waits until the transaction has been added to a block and z blocks have been linked after it.

- He does not know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Calculation (Cont'd)

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Calculation (Cont'd)

- Rearranging to avoid summing the infinite tail of the distribution…

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper

Calculation (Cont'd)

Running some results, we can see the probability drop off exponentially with z.

Table 1: Probability drop off for different values of q with z

q=0.1	
z=0	P=1.0000000
z=1	P=0.2045873
z=2	P=0.0509779
z=3	P=0.0131722
z=4	P=0.0034552
z=5	P=0.0009137
z=6	P=0.0002428
z=7	P=0.0000647
z=8	P=0.0000173
z=9	P=0.0000046
z=10	P=0.0000012

Table 2: Probability drop off for different values of q with z

q=0.3	
z=0	P=1.0000000
z=5	P=0.1773523
z=10	P=0.0416605
z=15	P=0.0101008
z=20	P=0.0024804
z=25	P=0.0006132
z=30	P=0.0001522
z=35	P=0.0000379
z=40	P=0.0000095
z=45	P=0.0000024
z=50	P=0.0000006

Image Source: [1] S. Nakamoto, "A peer-to-peer electronic cash system," *Bitcoin*, October 2008, Accessed: Jun. 9, 2023. [Online]. Available: https://bitcoin.org/en/bitcoin-paper