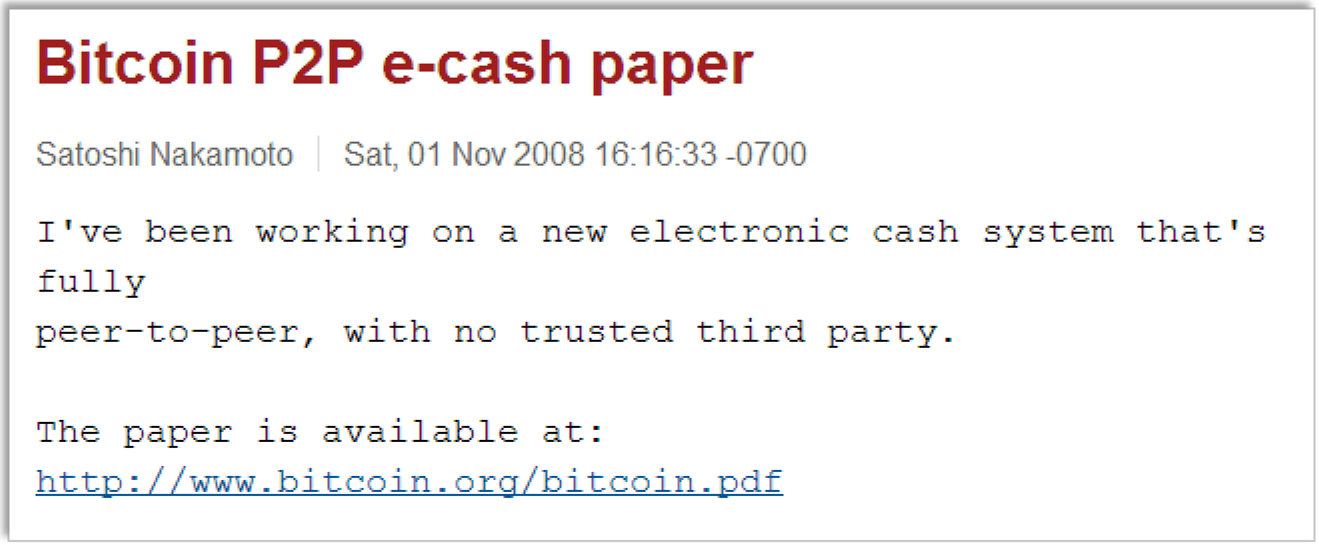
UNIVERSITY OF
NEW HAVEN

# Bitcoin

Satyendra Gurjar

- Bitcoin is decentralize digital or crypto currency.
- Peer-to-peer payment system.
- No central server and/or trusted parties.
- Messages are broadcast on a best effort basis
- Nodes can leave and rejoin the network at will.

- In 2008, anonymous person or group of people, call themselves **Satoshi Nakamoto**, published a 9 pages paper on The Cryptography Mailing list at metzdowd.com



**Bitcoin P2P e-cash paper**

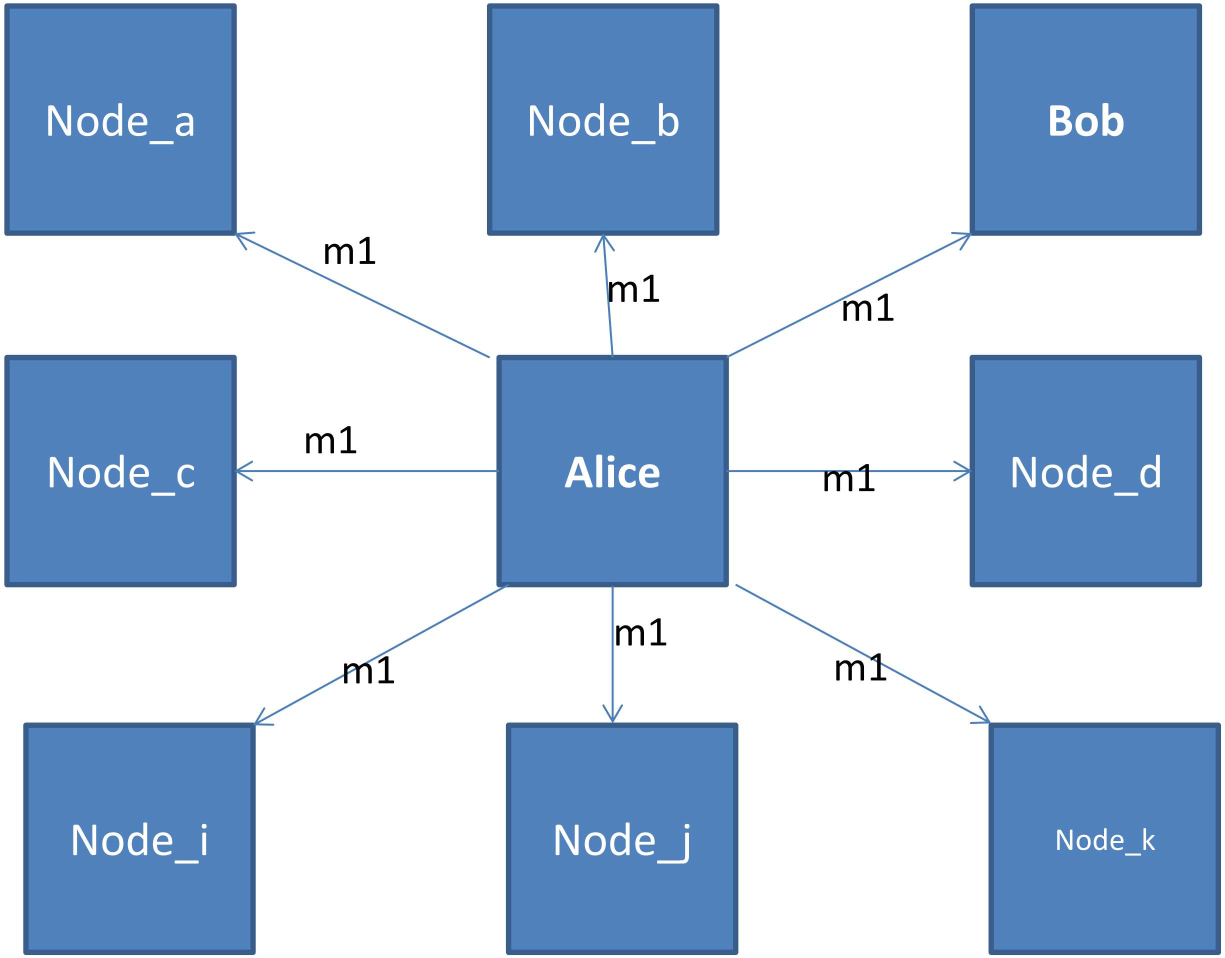
Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

```
I've been working on a new electronic cash system that's
fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf
```

- Public ledger, available on public websites – blockexplorer.com
- Every node in p2p network knows about every transaction happen in network.
- Majority of nodes in the network needs to agree on the state of the transaction, for it to be consider valid.

# Alice wants to send ‘x’ bitcoins to Bob



# Alice wants to send ‘x’ bitcoins to Bob

- Alice must have received at least ‘x’ bitcoins in the past.

- Alice broadcast the message, m1, on p2p network. That says she wants to move ‘x’ bitcoins from her account to Bob’s.

- She sign the message with her private key, identifies the sender. Other nodes can verify sender by using Alice’s public key.

- She puts Bob’s public key as payee, identifies receiver.

- Alice must use the past transactions, where she received at least ‘x’ bitcoins in order to pay Bob.

- Since Ledger is **public**, everyone can verify that if Alice has received ‘x’ bitcoins in the past.

- **Where are my bitcoins ?**
  Bitcoins are sent to a public key, owner of the private key of that public key is the owner of those bitcoins.

- **Don’t loose private key**
  If Alice looses her private key, she looses all the money, that was sent to her public key.

  Alice would also need her private key to use any bitcoins that was sent to her public key.

# Double Spending

- What if Alice broadcast sends same ‘x’ bitcoins, that is uses same transactions where she received ‘x’ bitcoins, to pay Bob and Charlie at same time.
- Some nodes in the network receive “Alice pay ‘x’ to Bob”, m1, while some receive “Alice pay ‘x’ to Charlie”, m2.
- Since nodes will see Alice has actually received ‘x’ bitcoins in the past and not used in any other transaction, some node in network will verify m1 while some will verify m2
- How do we stop it, without central authority or trusted parties ?

Alice can take advantage of network delay or induce delay or DoS attack to enable double spending.

# Proof of Work

- In addition to verify the transaction, nodes needs to solve a puzzle that takes significant amount of cpu cycles.

Adam Back's Hashcash 2002

**Flow of transaction verification**

1. New transactions are broadcasted to all nodes
2. Each node collects new transactions into a block
3. Each node work on finding a solution of puzzle for its block.
4. When a node finds a solution to puzzle, it broadcast 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 block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

- Puzzle: find a random string (nonce), when its added to the block being verified, SHA-256 hash of it begins with ‘n’ number of zero bits.

  $SHA\text{-}256(Block+Nonce)$ = starts with ‘n’ zero bits

- Block: List of unsolved transactions by a node.

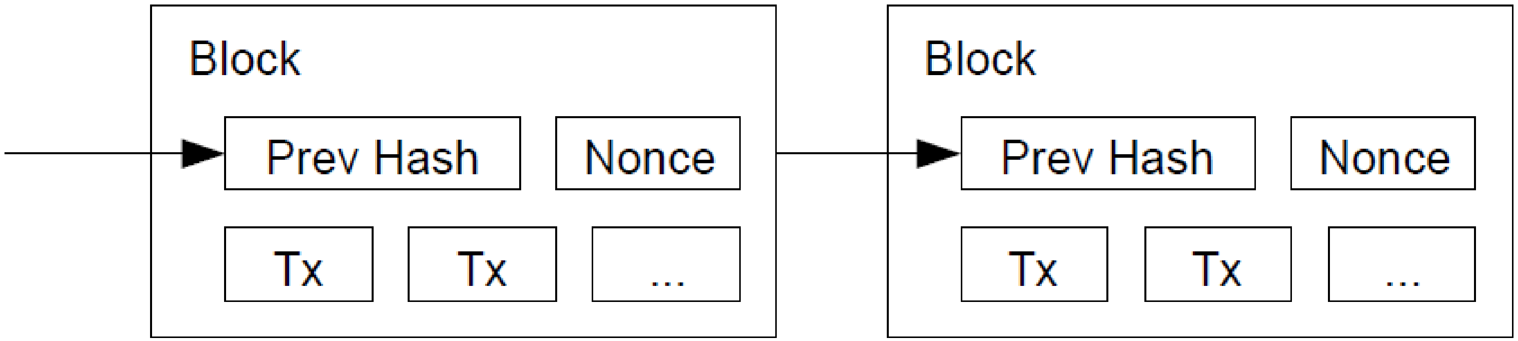
- The difficulty of the mathematical problem is automatically adjusted by the network, such that it targets a goal of solving an average of 6 blocks per hour.

- Every 2016 blocks (about two weeks), all Bitcoin clients compare the actual number created with this goal and modify the target by the percentage that it varied. This increases (or decreases) the difficulty of generating blocks.

# Block Chain

Block chains are formed by including hash of previous block.

Node on the network indicates that a block is being accepted by including hash of that block in their block.

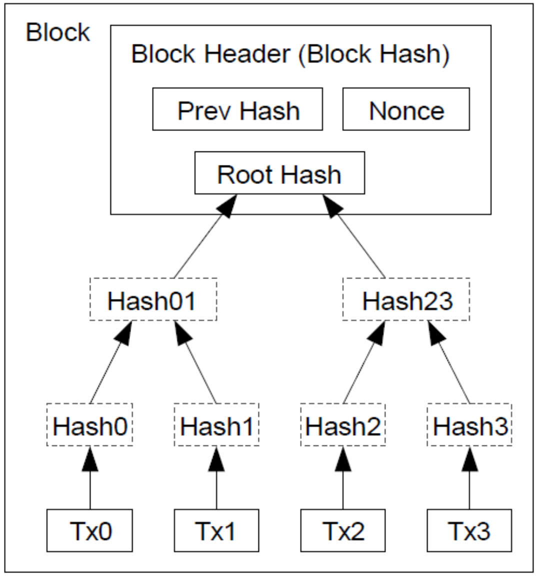


# Bitcoin miners

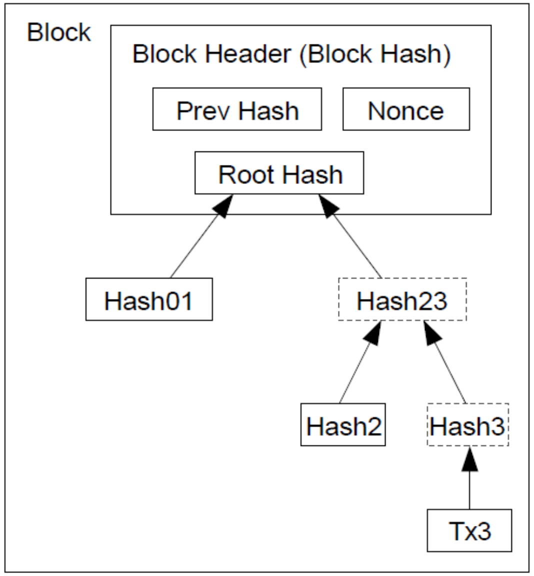
- Each block starts with a transaction that has no previous transaction, aka coinbase transaction.
- Coinbase transaction says to pay 1 bitcoin to public key of node creating the block.
- This also means each node in the p2p network is trying to solve a different block as first transaction in block is different for each node.
- When a block is accepted by nodes, then the creator of that block earns 1 bitcoin.

# Reclaiming Disk Space

- Blocks contains list hash of transactions, as block chain grows, it takes more and more diskspace.
- To preserve disk space, transactions are hashed in a Merkle Tree, with only the root included in the block's hash.
- Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

# Privacy

- Since bitcoins are send to public keys, identity of the bitcoin payer and payee is not revealed.
- If node in the bitcoin network uses Tor like network, it can remain unidentified.
- Market place like Silk Road, making use of bitcoins.

# 0x3F