Bitcoin – A Distributed Digital Currency

CALIFORNIA STATE UNIVERSITY EAST BAY

Prajna Prabhakara

Image Source: Free for Commercial Use Images at https://pixabay.com

Bitcoin: Motivation

- Bitcoin: replace bank & financial institution services with cryptography and code.
- Replace background agreements and transactions with software. Eg:Mortgage
- A completely decentralized, distributed and secure database called a blockchain.
- In 2009, Satoshi Nakamoto unveiled the first entirely digital currency.
- The technology worked on the principle : money is just an accounting tool—a method for abstracting value, assigning ownership, and providing a means for transacting. Eg: 50$ Bill, Tabulation
- Banks have partially sublimated physical currencies within closed systems.
- First decentralized cryptocurrency.

Reference: IEEE Spectrum, October 2017

Currency

- **Physical Form**: Cash or Dollars
  - Possessing the physical token equals ownership
  - MUST be very difficult to replicate
- **Digital Form:** Ledger of transactions

Banks

- Single centralized hidden ledger of transactions
- Bank keeps record of who owns or owes money

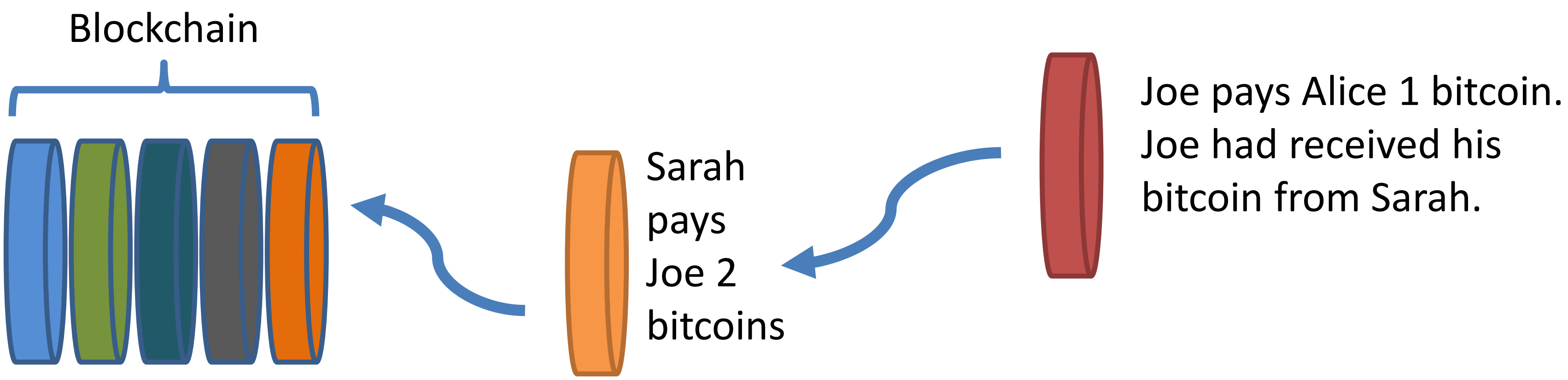
Bitcoin

- Universally accessible distributed ledger of transactions
- Miners verify ownership and transfer of money

Reference: IEEE Spectrum, October 2017

Bitcoin Blockchain

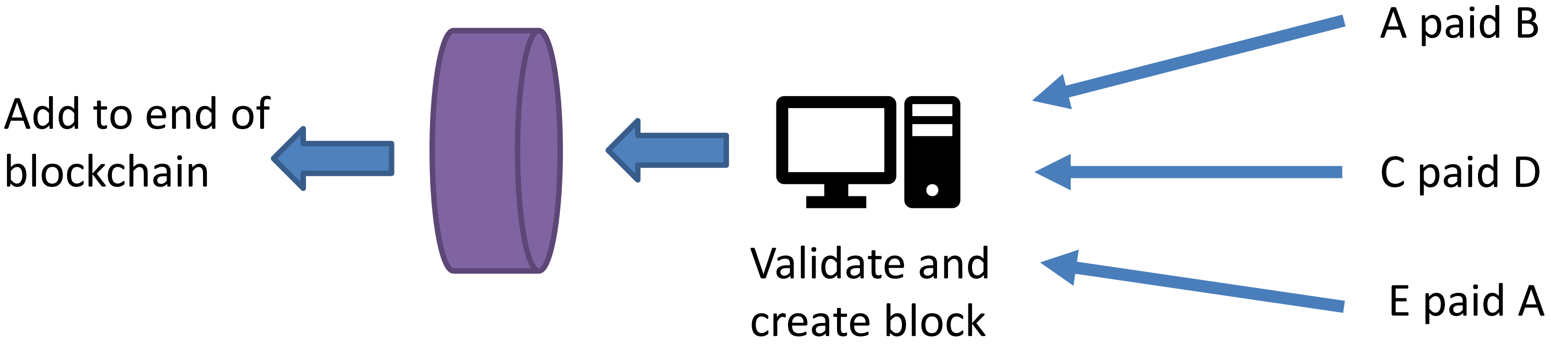
- **Blockchain**: Single universally accessible digital ledger of all transactions
  - Changes can be made only by adding new information to the end.
  - Each new addition, or block, contains a set of new transactions that reference previous transactions in the chain.
  - Replicated on networked computers around the world
  - Accessible to anyone with a computer and an Internet connection.


Blockchain
Sarah pays Joe 2 bitcoins
Joe pays Alice 1 bitcoin. Joe had received his bitcoin from Sarah.

Reference: IEEE Spectrum, October 2017

Bitcoin Miners

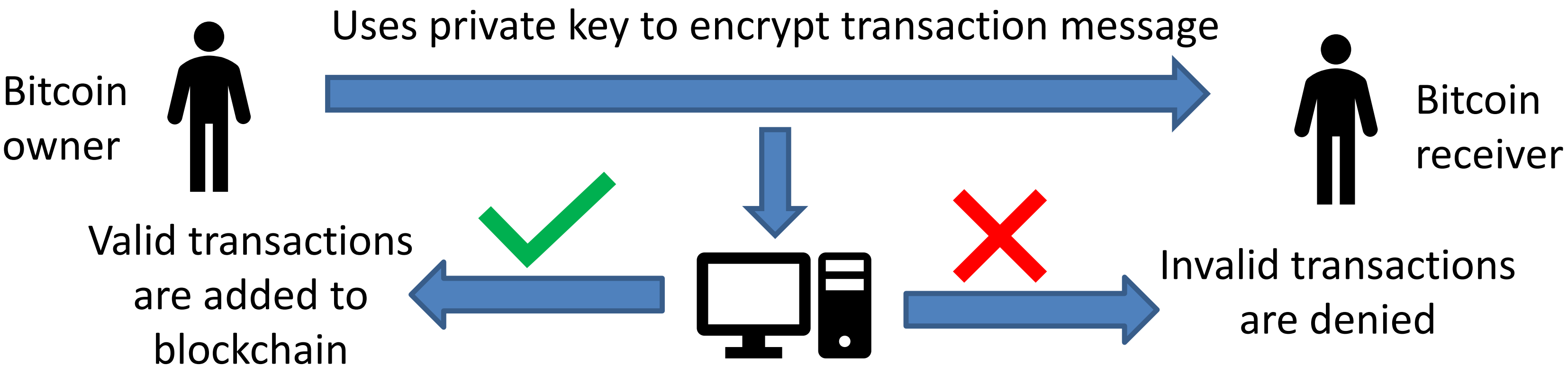
- **Miners:** Network participants who detect bitcoin transaction requests, validate them, and add them to the blockchain.
  - Miners are paid through bitcoin for their verification efforts
  - Miners can be anyone with a computer around the world
- **Validation**:
  - Ownership Problem: Verify the sender owns the bitcoin he is sending
  - Avoid Double Spending: Make sure sender hasn't used his bitcoin elsewhere
  - Irreversibility: Ensure transactions cannot be reversed



Reference: IEEE Spectrum, October 2017

Transaction Validation

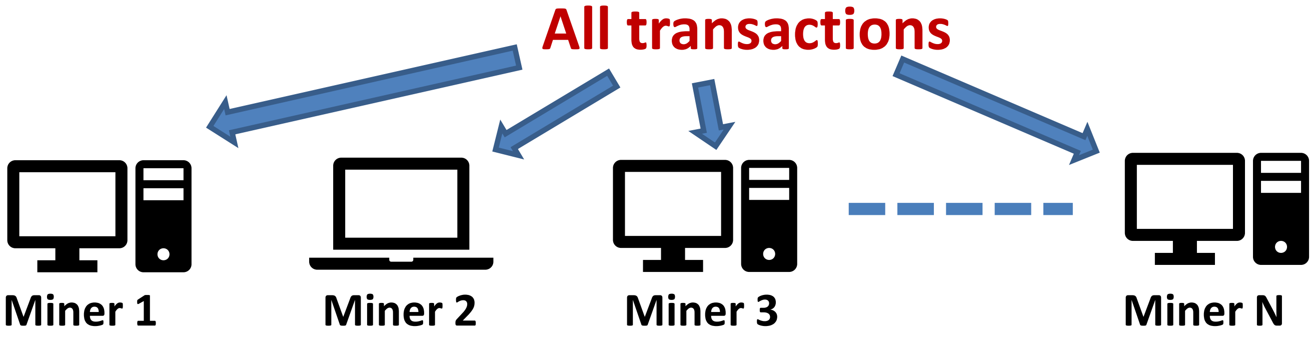
- Bitcoin owner has a public key and private key
  - Public key resides in the blockchain for anyone to see
  - Private key is kept safe from view by the owner
  - A new public/private key is generated when the bitcoin is transferred


Uses private key to encrypt transaction message
Bitcoin owner
Bitcoin receiver
Valid transactions are added to blockchain
Invalid transactions are denied

Miner uses the public key to verify if the message was encrypted using the corresponding private key. Also, check blockchain if bitcoin was already used for an earlier transaction.

Reference: IEEE Spectrum, October 2017

Miner’s Integrity



- Miner could modify the blockchain for his benefit. Example –
  - Miner uses bitcoin to buy a coffee
  - He deletes the transaction from his blockchain
  - Broadcasts his version of blockchain to all miners

Reference: IEEE Spectrum, October 2017

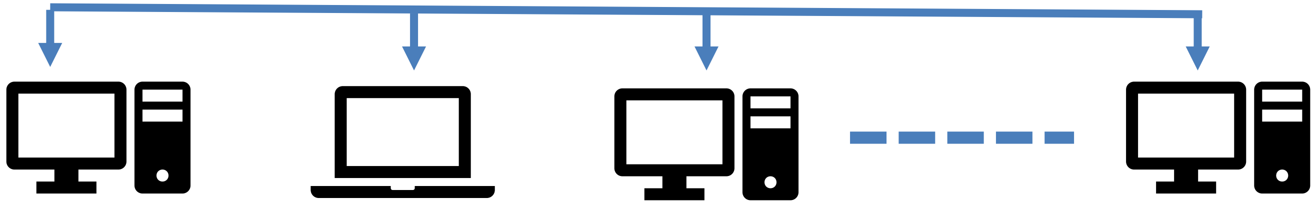
Ensuring Irreversibility

- Irreversibility in dollar transactions
  - Banks ensure money spent from an account or credit card cannot be spent again
  - A dollar is spent only when it physically changes hands
- Irreversibility for bitcoin transactions
  - Satoshi Nakamoto’s significant contribution to computer science
  - Bitcoin’s method is called Proof-of-work
  - Proof-of-stake is an alternate method
- Required since miners can be anyone in the world and there is no central authority to enforce legal modifications to blockchain. All legality must be ensured by the bitcoin code.

Reference: IEEE Spectrum, October 2017

Proof of Work Principle

A block of transactions



Miner 1 **Miner 2** **Miner 3** **Miner N**

Each miner hashes the sum combination of previous hash value from blockchain and the current block using different random seeds until the hash value starts with a predefined number of zeros

First miner to solve the hash problem

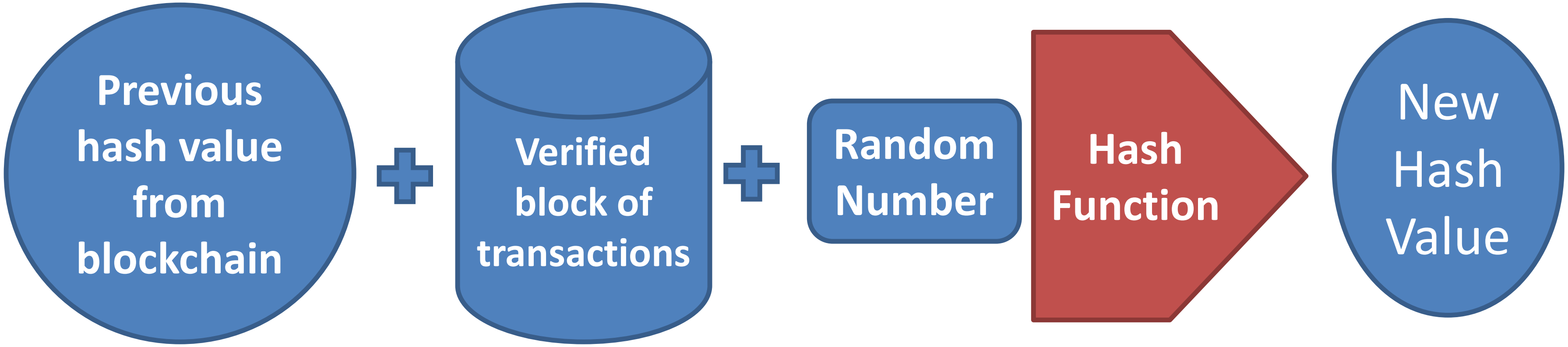
- Rewarded by bitcoins
- Bitcoins are generated during this verification process

Broadcasts the verified block and the zero prefixed hash value to all miners on the network. All miners cross-check the winning solution and update their copy of blockchain.

Reference: IEEE Spectrum, October 2017

Computational Cost of Proof Of Work

- Bitcoin mining software makes it very expensive in terms of computing power and electricity to add new blocks and even more expensive to change blocks further back in the record.
- Each miner needs to repeatedly run the following with different random seed numbers until the new hash value has a predefined number of zeros.(Can only be solved by Brute Force, Hence Expensive)


Previous hash value from blockchain
+
Verified block of transactions
+
Random Number
Hash Function
New Hash Value

Reference: IEEE Spectrum, October 2017

Impact of Proof-of-Work

- Proof-of-work makes it hard to reverse transactions
  - If a miner modifies one of the older blocks, all subsequent blocks will become invalid since block N uses hash value from block N-1.
  - The computational expense of modifying a block increases dramatically as new blocks are added in front of it.
- Miners invest hardware/electricity to mine bitcoins. Hence, it is in their interest to prevent the collapse of bitcoin and its blockchain.

Reference: IEEE Spectrum, October 2017

Beyond Currency

- Smart Contracts, Decentralized Notary
  - Slock, an Ethereum-enabled internet-of-things platform, stampd.io.
- Blockchain Healthcare
  - MIT Media Lab Research and multiple startups all over the world
- Personal Identification
  - Accenture, Microsoft and United Nations group are collaborating to build a blockchain for digital identity.
- IBM, Airbus, American Express, Intel are few of the many companies betting heavily on blockchain technology.

References:
https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/