Bitcoin Technical Overview

Frank W. Miller, Ph.D.
Dept. of Computer Science
University of Colorado

We’re Not Going to Talk About This

Sources

Badev, A. and Chen, M., *Bitcoin: Technical Background and Data Analysis*, 2014-104, Federal Reserve Board, Washington D.C.

Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org

Who is Satoshi Nakamoto?

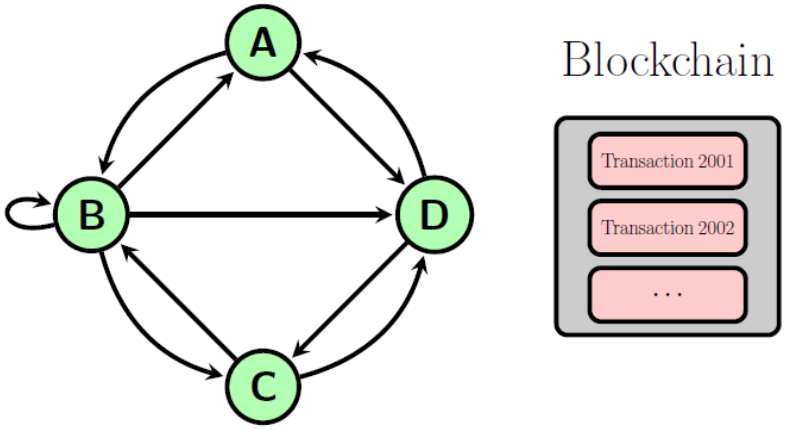
Satoshi Nakamoto is the name used by the unknown person or people who designed bitcoin and created its original reference implementation

What is It?

- Scheme for transferring value between parties
- Has some attributes of a payment system
  - Payment systems typically denominated in sovereign currency units
  - Bitcoin has its own unit called the *bitcoin*
  - Not tied to another unit of value
- Bitcoins have no intrinsic value
  - Like physical currency, e.g. dollar bill
- Value of bitcoins wrt other assets can fluctuate
  - Like an asset, e.g. stocks, commodities, precious metals, etc.

A Distributed Peer-to-Peer Network

- Participants transact directly with each other
- All transactions are chronologically ordered in a distributed, public ledger called a blockchain
- Each participant keeps a copy of the ledger
- No central management or administration
- Consensus based protocols used to approve incremental changes



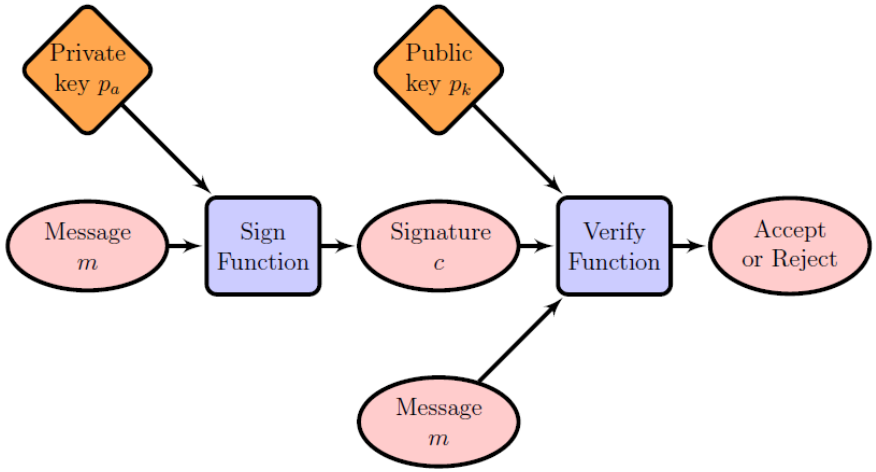
Mining

- Reward for recording transactions in blockchain
  - Participant systems *compete* to finish computationally intensive cryptographic problems
  - Result is new bitcoins
  - Process is referred to as “mining”

- Total number of bitcoins ever will be ~21 million
  - This makes Bitcoins scarce
  - Their unit “value” should increase over time

Transactions

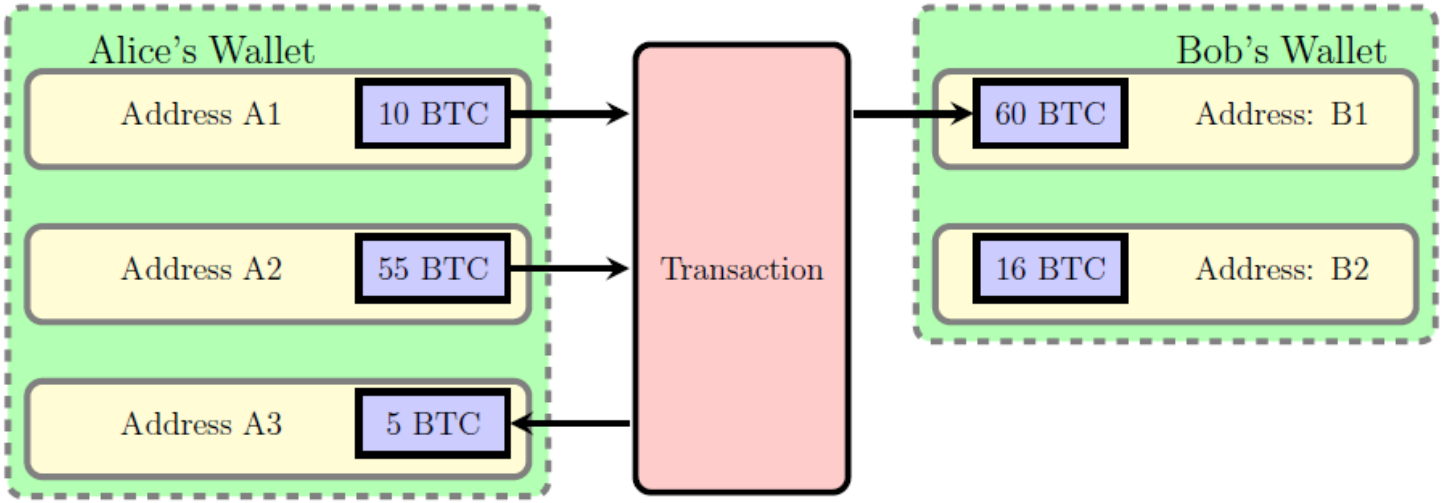
- Completed using cryptographic verification
  - Digital signatures
  - Cryptographic hash functions
- Participants use a “sign function” to indicate approval or rejection of messages
- Once consensus using a “verify function” is reached, transaction is accepted or rejected in the blockchain



Ownership

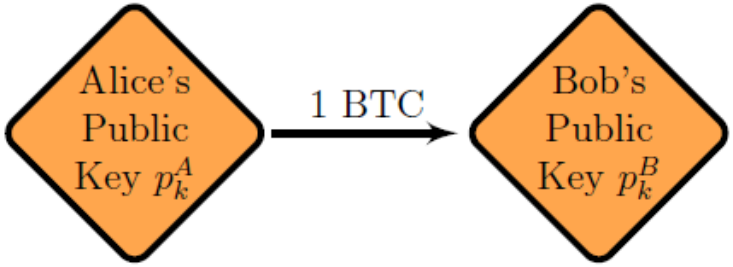
- Bitcoins reside at bitcoin addresses
  - Ownership is transferred by moving bitcoins from one address to another
- Each bitcoin address has a digital signature
  - Public part is a key string that provides an index to the address
    - Losing this part of the key means the bitcoins are gone forever
  - Private part allows operations on the bitcoins at that address
- Each address has a “balance” associated with it
- Collection of addresses is a “wallet”

Transaction Example



Initiating a Transaction

- Alice wants to send Bob 1 bitcoin
- Alice and Bob each have a wallet
- Alice then issues a digitally signed message
- If verified and completed, this has the following affect:



Verifying a Transaction

- Verify two things:

1. Did Alice send the message?

   Digital signature takes care of this

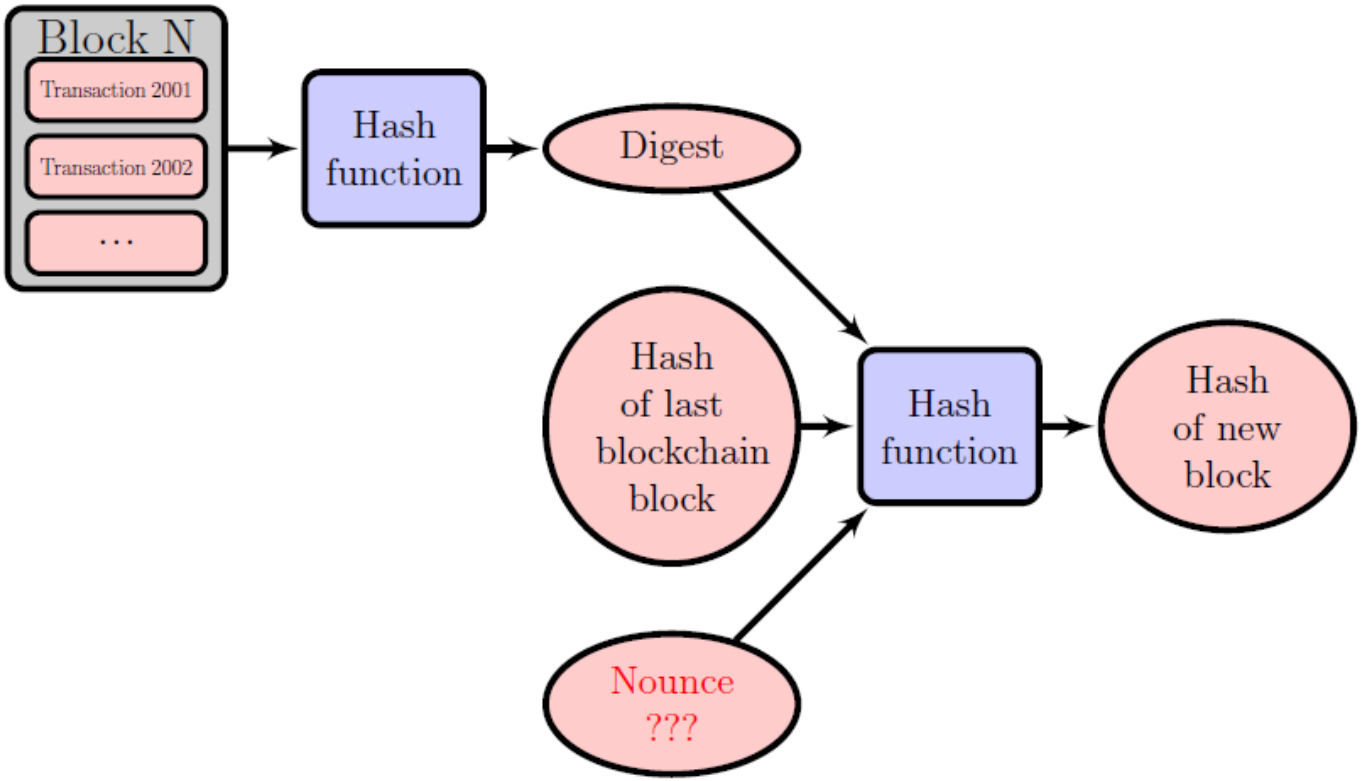
2. Are there enough funds at the sending address to complete the transactions?

   Records of all transactions are kept at each node so this is just a “lookup”

Blockchain Update

- The race is on!
  - The race gets harder as time goes on
- After verification, nodes compete to update the blockchain
  - Need to solve a hash based cryptograhic problem
  - Winner updates the record and collect a reward
- This process is called proof-of-work
- Nodes doing proof-of-work are miners

Proof of Work



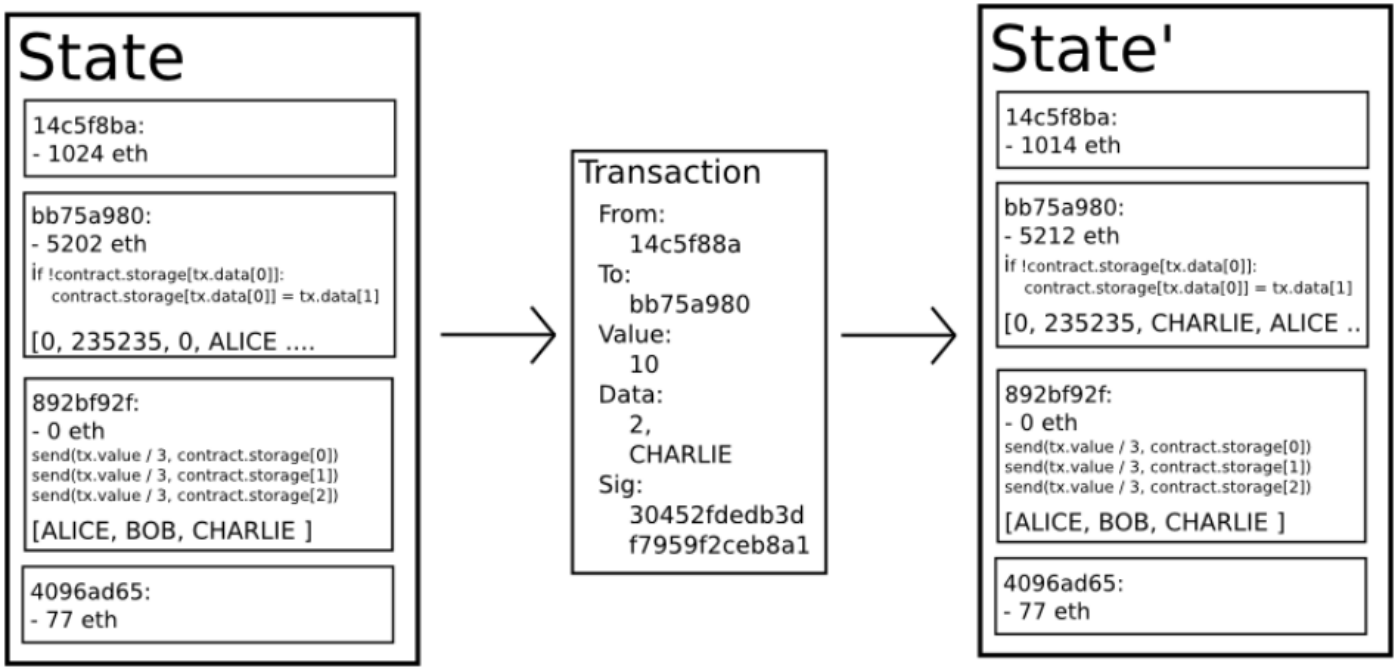
The Code

- https://github.com/bitcoin/bitcoin
- Written in C++
- MIT license

Ethereum

- Bitcoin's underlying blockchain technology as a tool for distributed consensus
- Ethereum is alternative protocol for building decentralized applications
- Implements a blockchain with a built-in Turing-complete programming language available during transactions
  - They call this "Smart Contracts"

Example Transaction



Applications

- Token systems (like Bitcoin)
- Financial derivatives and stable value currencies
- Identity and reputation
- File storage
- Autonomous organizations
- Contract situations: insurance, escrow, gambling

Conclusion

- Bitcoin and Ethereum represent interesting combinations of design choices for fully distributed applications

- Fully distributed “value transfer” is a novel application finding surprising traction, at least recently…