Distributed System : BitCoin & BlockChain

Houmin Wei

Electronics Engineering & Computer Science
Peking University

北京大学
PEKING UNIVERSITY

December 15, 2017

Bitcoin Overview

Buying a cup of coffee

Bitcoin: Challenges

- **Creation of a virtual coin**
  - How is it created in the first place?
  - How do you prevent inflation?
- **Validation**
  - Is the coin legit? (Proof-Of-Work)
  - How do you prevent a coin from double-spending?
- **Buyer and seller protection in online transactions**
  - Buyer pays, but the seller doesn't deliver
  - Seller delivers, buyer pays, but the buyer makes a claim
- **Trust on third party**
  - Rely on proof instead of trust
  - Verifiable by everyone
  - No central bank

What is Money

- **Medium of exchange**
  - Standard object used in exchanging goods and services
- **Unit of account**
  - Standard unit used for quoting prices
- **Store of value**
  - Store wealth from one point in time to another

Security in Bitcoin

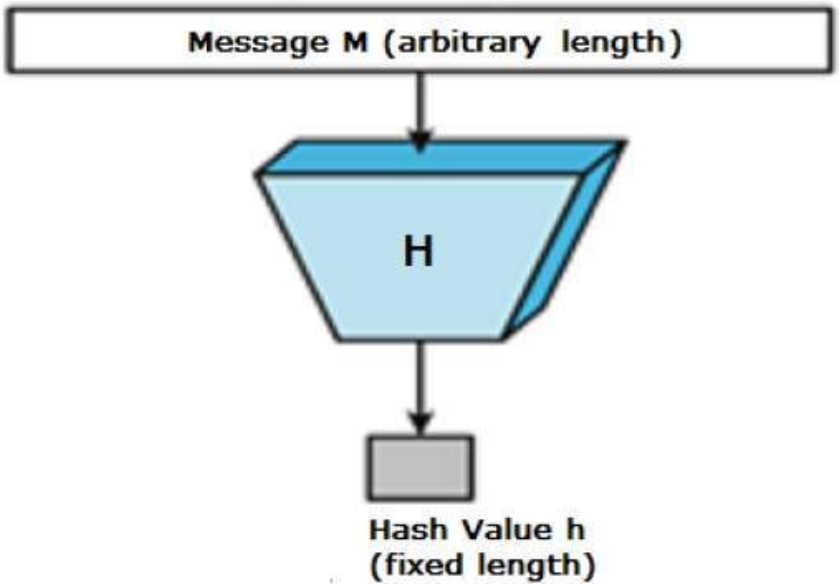
- **Authentication**
  - Am I paying the right person?
- **Integrity**
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- **Availability**
  - Can I make a transactions anytime I want?
- **Confidentiality**
  - Are my transactions private? Anonymous?

Security in Bitcoin

- **Authentication** -> **Public Key Crypto: Digital Signatures**
  - Am I paying the right person?
- **Integrity** -> **Digital Signatures and Cryptographic Hash**
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- **Availability** -> **Broadcast messages to the P2P network**
  - Can I make a transactions anytime I want?
- **Confidentiality** -> **Pesudonymity**
  - Are my transactions private? Anonymous?

Cryptographic Hash Function

- **Computationally efficient**
- **Consistent**
  hash(x) always yields same result.
- **Collision Resistant**
  Given $hash(W) = Z$, hard to find X such that $hash(X) = Z$
- **One-way**
  Given Y, hard to find X s.t. $hash(X) = Y$



Common Hash Functions:

- **MD5**
- **SHA-1**
- **SHA-2**
  - SHA-256
  - SHA-384
  - SHA-512

Hash Function Example

```
SHA224("")
0x d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f
SHA256("")
0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

```

Even a small change in the message wil result in a mostly different hash.

```
SHA224("The␣quick␣brown␣fox␣jumps␣over␣the␣lazy␣dog")
0x 730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525
SHA224("The␣quick␣brown␣fox␣jumps␣over␣the␣lazy␣dog.")
0x 619cba8e8e05826e9b8c519c0a5c68f4fb653e8a3d8aa04bb2c8cd4c

```

Proof of work first sight:

Given a basic string hello world! + random number nonce

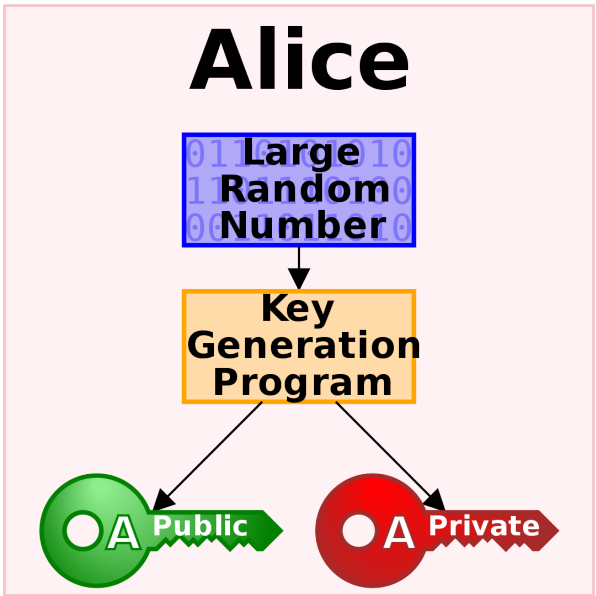
We need the digest have 4 leading 0.

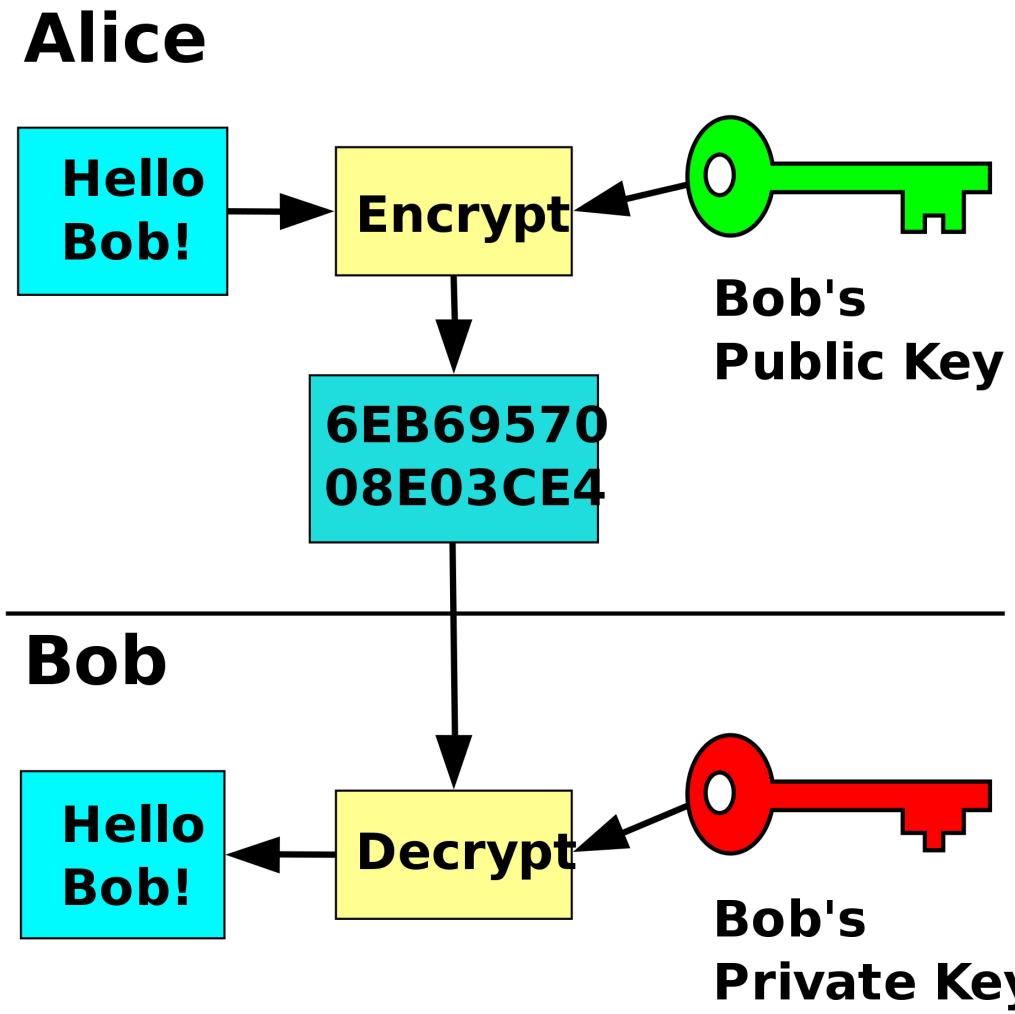
```
"Hello,␣world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello,␣world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello,␣world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello,␣world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello,␣world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello,␣world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

```

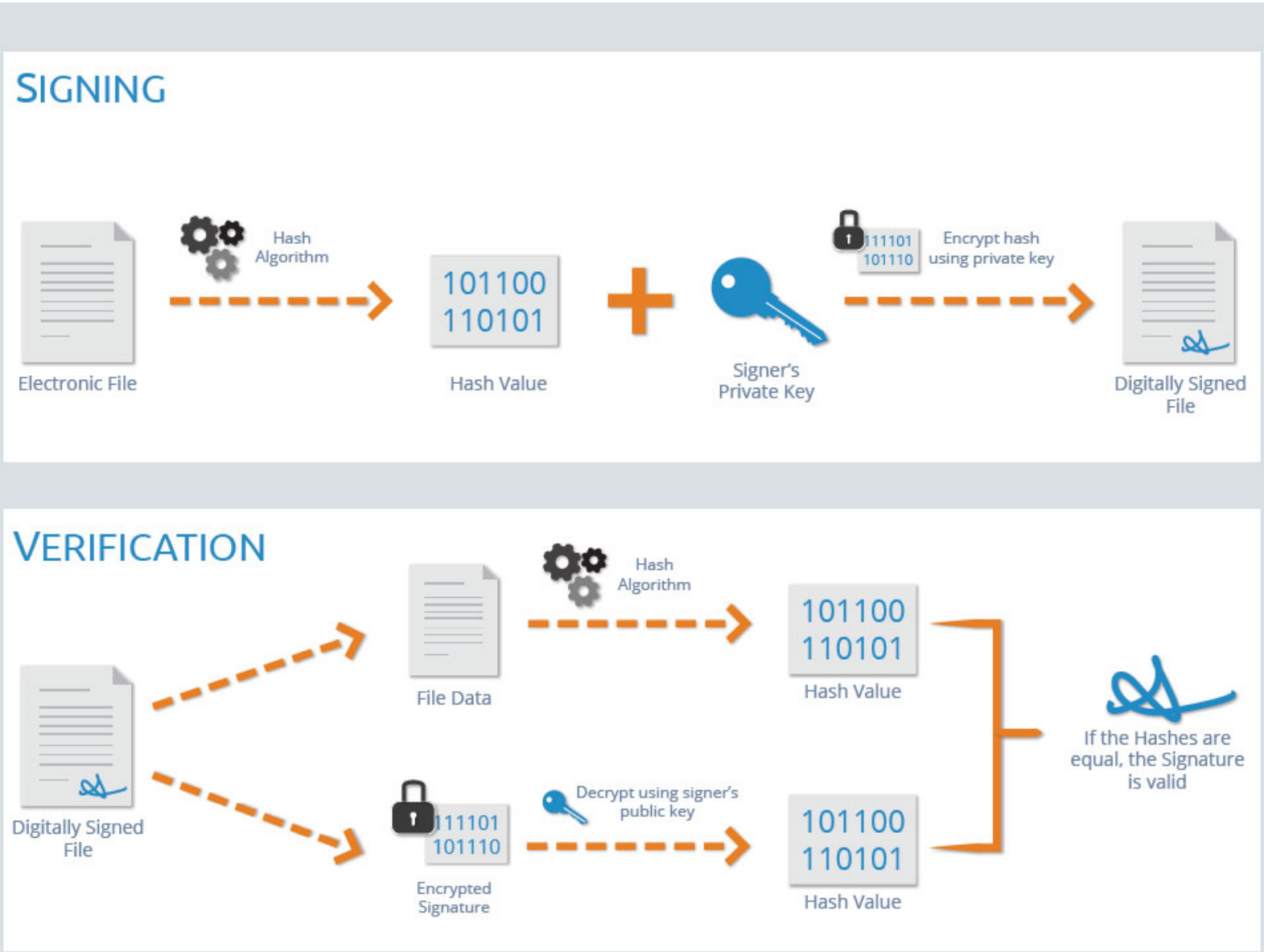
Public Key Crypto: Encryption

Key pair: Public Key and Private Key



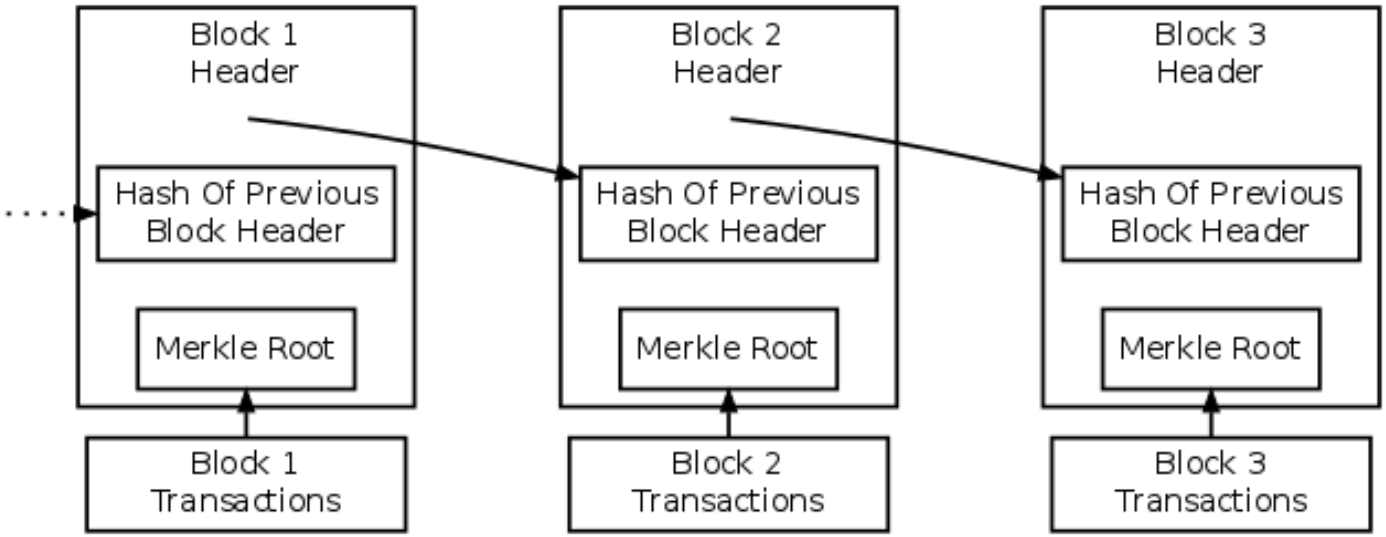


Public Key Crypto: Digital Signature



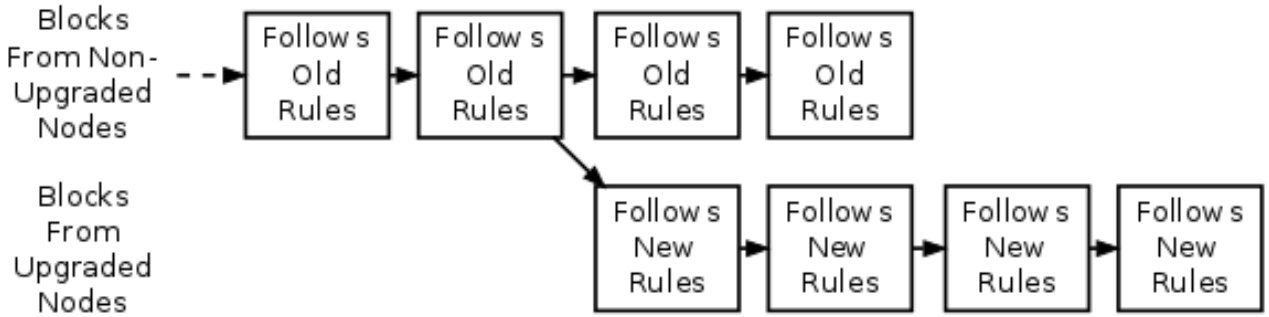
- The block chain provides Bitcoin's public ledger, an ordered and timestamped record of transctions.
- This system is used to protect against double spending and modification of previous transactions records.
- Each full node in the Bitcoin network independently stores a block chain containing only blocks validated by that node.

Block Chian Overview



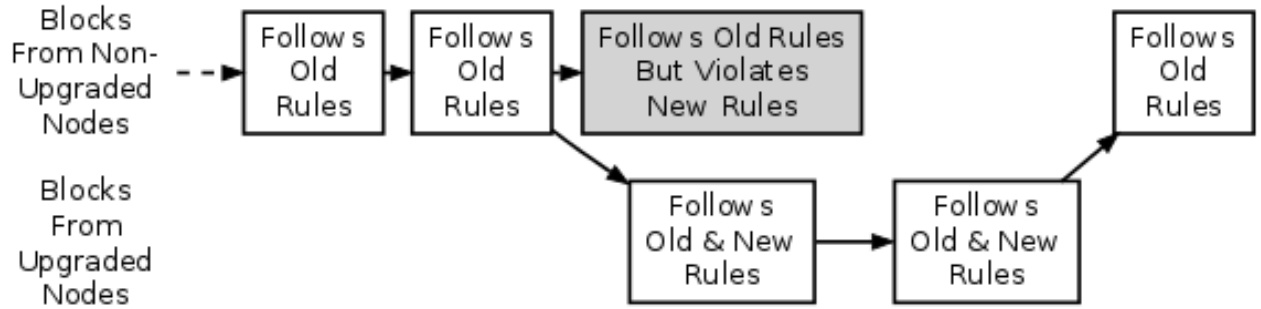
Simplified Bitcoin Block Chain

Hard Fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Soft Fork



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

Mining