IERG5590
Advanced Blockchain

Sherman Chow
Chinese University of Hong Kong
Spring 2022
Lecture 1: Introduction of Bitcoin and Blockchain
What is this lecture about?

- How bitcoins born? Can I mine my own?
- How does bitcoin transaction work?
- How the blockchain works for recording your transaction?
- It’s “electronic money.” How to prevent double-spending?
- What if we have different views of the blockchain state?
- Any other mechanism to maintain the distributed ledger?

Based on the slides by Foteini Baldimtsi (George Mason University)
http://www.baldimtsi.com/teaching/cs795_sp17
which in turns used the slides by Stefan Dziembowski (University of Warsaw)
https://www.crypto.edu.pl/dziembowski-talks
Why Blockchain Technologies?

Report: Blockchain Technology Market to Reach $7.7 Billion by 2024

Jan 20, 2017 6:10 PM EST  by Jessie Willms

The Blockchain Matters More Than The President

By The Foundation for Economic Education  on January 19, 2017 2:35 pm  in Politics
Why Blockchain Technologies?

Contact info@venturescanner.com to see all 725 companies
Why Blockchain Technologies?
Why Blockchain Technologies?

Visa to Launch Blockchain Payments Service Next Year

Stan Higgins (@mpmcsweeney) | Published on October 21, 2016

Walmart Testing Blockchain Technology for Supply Chain Management

Dec 21, 2016 4:16 PM EST by Giulio Prisco
“Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”

Available freely [here](#) (pre-publication draft)
Common types of payment

Common characteristic?

Trust to a financial institution
Common types of payment
The Bitcoin Revolution
The Bitcoin Revolution

Decentralized peer-to-peer payment system - which works as currency: has units of value - which can be exchanged for “real money”.

Proposed by “Satoshi Nakamoto” in 2008
1) Very small transaction fees (~USD $0.1)
2) Fast transactions (10 - 60 minutes)
3) Accepted in thousands of businesses
Permissionless: Everyone can join – just generates a key pair

“Unspent transaction”: A user can have multiple such key pairs, each is “unspent”

Why not just call it money?
- 1) It’s created by a transaction.
- 2) It’s not your “account”.

The difference will be clearer when we talk about the account model of Ethernum.
Bitcoin Transactions

- Transactions use digital signatures (in turns use hash function)

Alice

PK: hUK67H9fyg
SK: z4Pxc2kKn3

Bob

PK: p2Pknb7frT
SK: n52Hb9Klp

hUK67H9fyg sends 1 to p2Pknb7frT

Transaction $T$

$PK$ served as the Address

$T$ signed under Alice’s $SK$

A transaction is valid only if the signature verifies
Main Problem with Digital Money

Double spending…

Bits are easier to copy than paper!
How Bitcoin prevents double-spending

The users emulate a public write-only (actually, append-only) bulletin-board containing a list of transactions.

A transaction is of a form:

“User $P_1$ transfers a coin #16fab13fc6890 to user $P_2$”

This prevents double spending.
Transaction table: the Bitcoin Blockchain

Stores every transaction (transferring to others and **yourself**)

**Example:**

<table>
<thead>
<tr>
<th>Time t</th>
<th>Time t+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice sends 1 to Bob</td>
<td></td>
</tr>
<tr>
<td>Alice sends 0.7 to Chris</td>
<td></td>
</tr>
<tr>
<td>Alice sends 0.3 to Alice’</td>
<td></td>
</tr>
<tr>
<td>Bob sends 1.2 to Dave</td>
<td></td>
</tr>
<tr>
<td>Dave sends 0.2 to Chris</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.3</td>
</tr>
<tr>
<td>5</td>
<td>4.8</td>
</tr>
</tbody>
</table>

**Required properties:**
- Append only
- Cannot revise existing blocks
- Distributed
Who maintains the Bitcoin Blockchain?

In traditional payment systems, what was the financial institution?

Miners: a special type of user
Main difficulty: Some parties can cheat.
Classical result: emulation is possible if the "majority is honest."
e.g., for 5 players, we can tolerate at most 2 "cheaters."
Who maintains the Bitcoin Blockchain?

Every transaction is broadcasted to all users.

Is this the right view of the blockchain?

Voting -> Majority wins

Works well if users are all honest but this is not the case in practice because “sybil” can appear “for free” in a permissionless network.
We have a problem

What does majority mean in a system that everyone is free to participate?

Sybils: Multiple identities belonging to the same (malicious) user
How to check majority of comp. power?

**Majority** is defined as the majority of computational power!

**Sybil creation doesn’t increase** attackers computational power ;)

“Measures” a user’s computational power by how much time is needed for solving a “puzzle”
- the puzzle should be difficult to solve
- but, a solution should be easily verifiable

In Bitcoin, it is based on the **cryptographic hash functions**

\[ H(x) < D \]

**Puzzle:** Given \( D \) find \( x \)!
How to add a block to the blockchain?

A block is added every 10 minutes and has size <~1MB.

Time $t$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Time $t+1$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris
How to add a block to the blockchain?

A block is added every 10 minutes and has size < ~1MB.
How to add a block to the blockchain?

Alice sends 1 Bitcoin to Bob

Broadcast

Miners
How to post to the blockchain?

Just broadcast (over the Internet) your transaction to the miners.

And hope they will add it to the next block.

**Important:**

They *never add an invalid transaction* (e.g. double spending)

the miners are incentivized to do it.

a chain with an invalid transaction is *itself not valid*, so no rational miner would do it.
How to post to the blockchain?

Miners compete on who will make the next block

Transactions not yet on blockchain

= solve a proof-of-work puzzle

New block

Alice sends 1 $\text{BTC}$ to Bob

Bob sends 1.2 $\text{BTC}$ to Dave

Dave sends 0.2 $\text{BTC}$ to Chris

Alice sends 0.7 $\text{BTC}$ to Chris

Alice sends 1 $\text{BTC}$ to Bob

Miners

Broadcast

Time $t$
Main Principles

1. It is **computationally hard** to extend the chain.

2. Once a miner finds an extension he **broadcasts it to everybody**.

3. The users will always accept “**the longest chain**” as the valid one.
Creating a new block

Transactions not yet on blockchain

I found a new block!
I found a new block!

Creating a new block

- Time $t-1$
  - Alice sends 1 to Bob
  - Alice sends 0.7 to Chris
  - Bob sends 1.2 to Dave
  - Dave sends 0.2 to Chris

- Time $t$
  - Alice sends 1 to Bob
  - Alice sends 0.7 to Chris
  - Bob sends 1.2 to Dave
  - Dave sends 0.2 to Chris

- Time $t+1$
  - Alice sends 1 to Bob
  - Alice sends 0.7 to Chris
  - Bob sends 1.2 to Dave
  - Dave sends 0.2 to Chris

New block
Creating a new block

I found a new block!

Time $t$

- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Time $t+1$

- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

New block
What if there is a “fork”?

The “longest” chain counts.
But how long? A few slides later...

this chain is valid

“We have 2 different views”
Does it make sense to work on the shorter chain?

No!

Because everybody else is working on extending the longest chain.

Recall: we assumed that the majority follows the protocol.
Longest chain wins

Time $t-1$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Time $t$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Time $t+1$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Time $t+2$
- Alice sends 1 to Bob
- Alice sends 0.7 to Chris
- Bob sends 1.2 to Dave
- Dave sends 0.2 to Chris

Fork

New block

New block
Consequences

The system should quickly **self-stabilize**.

If there is a fork then one branch will quickly die.

**Problem**: what if your transaction ends up in a “dead branch”?

**Recommendation**: to be sure that it doesn’t happen, wait **6 blocks**, \( \approx 1 \text{ hour} \).
To reverse transactions, an adversary has to create a “fork in the past”. This looks very hard if she/he just has a minority of computing power (the honest miners will always be ahead of him).

It gives the security, but also a “shortcoming” of decentralization.

Incentive to join this “game”? 
I want to join this “game”?  

**Short answer:** they are paid (in Bitcoins) for this.

Can you mine bitcoin? **Short answer:** Yes…

- **Special hardware**
- **Huge mining pools**
Where does the money come from?

A miner who finds a new block gets a “reward” in BTC:

\[ \approx 4 \text{ years} \]

- for the first 210,000 blocks: 50 BTC
- for the next 210,000 blocks: 25 BTC
- for the next 210,000 blocks: 12.5 BTC, and so on...

**Note:** \( 210,000 \cdot (50 + 25 + 12.5 + \cdots) \rightarrow 21,000,000 \)
More Details

Each block contains a transaction that transfers the reward to the miner.

**Advantages:**

1. It provides incentives to be a miner.
2. It also makes the miners interested in broadcasting new block asap.

this view was challenged in a recent paper: Ittay Eyal, Emin Gun Sirer

**Majority is not Enough: Bitcoin Mining is Vulnerable**
Problems with Bitcoin’s PoW

1. high energy consumption
   - costs money
   - bad for environment

2. advantageous for people with dedicated hardware

3. low throughout by design
Drawbacks of Hardware Mining

1. Makes the whole process “non-democratic”.

2. Easier to attack by very powerful adversary?

3. Excludes some applications (mining a as “micropayment”).

Is it the price we must pay for security against sybils/botnets.
Alternatives to PoW

- Proof-of-stake
- Proof-of-knowledge
- Proof-of-space
Proof of Stake

The “voting power” depends on how much money one has.

Justification: people who have the money are naturally interested in the stability of the currency.

Currencies: Peercoin, BlackCoin, NXT, Ethereum, etc.

Problem:
1. How to distribute initial money?
2. How to force coin owners to mine?
**Proof-of-Work vs. Proof-of-Stake**

**Proof-of-Work**
- The probability of mining a block is dependent on how much work is done by the miner.
- Payouts become smaller and smaller for Bitcoin miners, there is less incentive to avoid a 51% attack.
- POW systems have powerful mining communities, but tend to become centralized over time.

**Proof-of-Stake**
- A person can "mine" depending on how many coins they hold.
- The POS systems make any 51% attack more expensive.
- POS systems are more decentralized, but must work hard to build communities around their coins.
I found a new block!

Proof of Knowledge (e.g., of a Private Key)

Proof that I have the right key!
Permissioned Blockchain

for example:

- Legally accountable validators (mintettes)
- Suitable for off-chain assets (securities, fiat, titles)
- Settlement finality (irreversible)