1. Introduction of Bitcoin and Blockchain

IERG5590/IEMS5709 “Advanced Blockchain”
Spring 2020
Sherman S. M. Chow

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 Dziembowsk (University of Warsaw)
https://www.crypto.edu.pl/dziembowsk-talks
What is this lecture about?

- How are bitcoins generated? Can I mine my own?
- How does bitcoin transaction work? or
- 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?
Why Blockchain Technologies?
Common types of payments

Common characteristic?

Trust to a financial institution
Common types of payments
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
Why should I care about bitcoin?

1) Very small fees (~USD $0.1)
2) Fast transactions (10 - 60 minutes)
3) Accepted in thousands of businesses
Some numbers

Bitcoin market capital: ~ 14 billion USD (Jan 2017)

Current exchange rate: 1BTC = 921 USD (23 Jan. 2017)

Highest price: 1216 USD (17 Nov. 2013) and 1150 Dec 2016
Overview of Bitcoin Technology

A combination of techniques from

- Security
- Distributed Systems
- Economics
  and
- Cryptography: This lecture keeps it to “minimal”. (We’ll devote a few weeks to talk about those :)
Bitcoin Users

**Permissionless**: Everyone can join – just generates a key pair

<table>
<thead>
<tr>
<th>Alice</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>public key</td>
<td>PK: hUK67H9fyg</td>
</tr>
<tr>
<td>(secret) private key</td>
<td>SK: z4Pxc2kKn3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bob</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>PK: p2Pknb7frT</td>
<td></td>
</tr>
<tr>
<td>SK: n52Hb9Klp</td>
<td></td>
</tr>
</tbody>
</table>

**“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 Eternum.
Bitcoin Transactions

Transactions use digital signatures (in turns use hash function)

Alice

PK: hUK67H9fyg
SK: z4Pxc2kKn3

Bob

PK: p2Pknb7frT
SK: n52Hb9Klp

hUK67H9fyg sends 1 Bitcoin 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 the digital money

Double spending...

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

The users emulate a public write-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**)

**Required properties:**
- Append only
- Cannot revise existing blocks
- Distributed

**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>0.3 to Alice’</td>
</tr>
<tr>
<td>Alice sends 0.7 to Chris</td>
<td>4.8 to Bob</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>...</td>
<td></td>
</tr>
<tr>
<td>Dave sends 0.2 to Chris</td>
<td></td>
</tr>
</tbody>
</table>
Who maintains the Bitcoin Blockchain?

In traditional payment systems, that task is handled by a financial institution. However, in blockchain technology, the maintenance of the Blockchain is decentralized and handled by a network of users known as miners. Miners are a special type of user in a peer-to-peer network.
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

Yes  No  Yes  Yes  Yes

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 ;)

**Proof of Work**

“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
How to add a block to the blockchain?

A block is added every 10 minutes and has size $<\sim1$MB

The “genesis block” created by Satoshi on 03/Jan/2009
How to add a block to the blockchain?

Alice sends 1 to Bob

Transaction T

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).

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

<table>
<thead>
<tr>
<th>Time t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice sends 1 🍀 to Bob</td>
</tr>
<tr>
<td>Alice sends 0.7 🍀 to Chris</td>
</tr>
<tr>
<td>Bob sends 1.2 🍀 to Dave</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>Dave sends 0.2 🍀 to Chris</td>
</tr>
</tbody>
</table>

New block

solve a proof-of-work puzzle
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!
Creating a new block

I found a new block!

Block B

New block
Creating a new block

I found 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
What if there is a “fork”?

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

“**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
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**.  
*≈ 1 hour*
Can transactions be “reversed”?

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.
How are the miners incentivized to participate in 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:

- 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: $210,000 \cdot (50 + 25 + 12.5 + \cdots) \rightarrow 21,000,000$

https://www.bitcoinblockhalf.com
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**
Problem with Bitcoin’s PoW

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

2. advantageous for people with **dedicated hardware**
Alternatives to PoW

Proof-of-stake

Proof-of-knowledge

Proof-of-space*
Proofs 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: BlackCoin, Peercoin, NXT, etc.

• Problem:
  1. How to distribute initial money?
  2. How to force coin owners to mine?
**PROOF-OF-WORK**  OR  **PROOF-OF-STAKE**

**THE PROBABILITY OF MINING A BLOCK IS DEPENDENT ON HOW MUCH WORK IS DONE BY THE MINER**

**PERSON CAN “MINE” DEPENDING ON HOW MANY COINS THEY HOLD**

**PAYOUTS BECOMES SMALLER AND SMALLER FOR BITCOIN MINERS, THERE IS LESS INCENTIVE TO AVOID A 51% ATTACK**

**THE POS SYSTEMS MAKES ANY 51% ATTACK MORE EXPENSIVE**

**POW SYSTEMS HAVE POWERFUL MINING COMMUNITIES - BUT TEND TO BECOME CENTRALIZED OVER TIME**

**POS SYSTEMS ARE MORE DECENTRALIZED - BUT MUST WORK HARD TO BUILD COMMUNITIES AROUND THEIR COINS**
Proof of Knowledge (e.g., of a Private Key)

I found a new block!

Proof that I have the right key!
Permissioned Blockchain from Proof-of-Knowledge

for example:

- Legally accountable validators (mintettes)
- Suitable for off-chain assets (securities, fiat, titles)
- Settlement finality (irreversible)
A couple of slides belong to Stefan Dziembowski and are free to distribute under the following copyright.

©2016 by Stefan Dziembowski. Permission to make digital or hard copies of part or all of this material is currently granted without fee provided that copies are made only for personal or classroom use, are not distributed for profit or commercial advantage, and that new copies bear this notice and the full citation.