CMPSC 390

Janyl Jumadinova

Credit: Authors of “Mastering Bitcoin” and “Bitcoin and Cryptocurrency Technologies”

February 2, 2021
- Can be backed up and stored in multiple copies.
Can be backed up and stored in multiple copies.

Decentralization is important for security.
- Can be backed up and stored in multiple copies.
- Decentralization is important for security.
- Responsibility and control is in the hands of the users.
Security, Chapter 11 in MB

- Can be backed up and stored in multiple copies.
- Decentralization is important for security.
- Responsibility and control is in the hands of the users.
- Bitcoin is not based on Root of Trust security architecture, which is designed as a series of concentric circles.
Can be backed up and stored in multiple copies.

Decentralization is important for security.

Responsibility and control is in the hands of the users.

Bitcoin is not based on Root of Trust security architecture, which is designed as a series of concentric circles.

Genesis block is the root of trust, a chain of trust built up to the current block.
Can be backed up and stored in multiple copies.

Decentralization is important for security.

Responsibility and control is in the hands of the users.

Bitcoin is not based on Root of Trust security architecture, which is designed as a series of concentric circles.

Genesis block is the root of trust, a chain of trust built up to the current block.

*Balancing risk:* storage, multisig, diversification, survivability.
Consensus in Bitcoin

- what makes a transaction valid
- what makes a block valid
- how P2P nodes should behave
- protocols and formats
Consensus in Bitcoin

consensus about rules

consensus about history

Agree on contents of the blockchain
therefore: which transactions have occurred
therefore: which coins exist and who owns them
Consensus in Bitcoin

- Consensus about rules
- Consensus about history
- Consensus that coins are valuable
  - General agreement that coins have value.
  - “Tinkerbell effect”
Consensus in Bitcoin

- consensus about rules
- consensus about history
- consensus that coins are valuable
Bitcoin Core Software

Open Source (MIT license).

It is the de facto rule book of Bitcoin.

Bitcoin Improvement Proposals (BIPs): proposal for changes to Bitcoin.

https://bitcoincore.org/

Janyl Jumadinova Credit: Authors of “Mastering Bitcoin” and “Bitcoin and Cryptocurrency Technologies”
Bitcoin Core Software

- Open Source (MIT license).
- It is the de facto rule book of Bitcoin.
- **Bitcoin Improvement Proposals (BIPs):** proposal for changes to Bitcoin.
Bitcion Core Software

- Open Source (MIT license).
- It is the de facto rule book of Bitcoin.
- **Bitcoin Improvement Proposals (BIPs):** proposal for changes to Bitcoin.

https://bitcoincore.org/
Users can fork the rules

If there’s a (hard) fork in the rules:

```
“Bitcoin”
```

```
Valid under A rules
Invalid under B rules
```

```
Valid under B rules
Invalid under A rules
```

```
```
Users can fork the rules

If there’s a (hard) fork in the rules:

```
“Bitcoin” ————> "A-coin" ————> Valid under A rules
                    |                            | Invalid under B rules
                    |                            | Valid under B rules
                    |                            | Invalid under A rules
                    |                            |
                    |                            |
                    |                            |
                    |                            |
                    |                            |
                    |                            |
```

“B-coin”
Users can fork the rules

If there’s a (hard) fork in the rules:

"Bitcoin" —> "A-coin" —> "the currency forked"

"Bitcoin" —> "B-coin" —> "the currency forked"
Who has power in Bitcoin ecosystem?

- **Claim**: Bitcoin Core developers have the power.
Who has power in Bitcoin ecosystem?

- **Claim**: Bitcoin Core developers have the power.
- **Claim**: Miners have the power.
Who has power in Bitcoin ecosystem?

- **Claim**: Bitcoin Core developers have the power.
- **Claim**: Miners have the power.
- **Claim**: Investors have the power.
Who has power in Bitcoin ecosystem?

- **Claim:** Bitcoin Core developers have the power.
- **Claim:** Miners have the power.
- **Claim:** Investors have the power.
- **Claim:** Merchants and their customers have the power.
Who has power in Bitcoin ecosystem?

- **Claim**: Bitcoin Core developers have the power.
- **Claim**: Miners have the power.
- **Claim**: Investors have the power.
- **Claim**: Merchants and their customers have the power.
- **Claim**: Payment services have the power.
Founded in 2012.
- Pays core developers.
- “voice of Bitcoin” to governments.
Governments and Bitcoin

- Untraceable digital cash defeats capital controls.
Governments and Bitcoin

- Untraceable digital cash defeats capital controls.
- Untraceable digital cash makes certain kinds of crimes easier ... but
Governments and Bitcoin

- Untraceable digital cash defeats capital controls.
- Untraceable digital cash makes certain kinds of crimes easier ... but
  - Hard to keep real and virtual separate.
  - Hard to stay anonymous for a long time.
  - Feds can “follow the money”
Should Cryptocurrency be regulated?

Simplified Debate!

- Arguments with examples.

https://www.loc.gov/law/help/cryptocurrency/world-survey.php

Janyl Jumadinova Credit: Authors of “Mastering Bitcoin” and “Bitcoin and Cryptocurrency Technologies”
Should Cryptocurrency be regulated?

Simplified Debate!

- Arguments with examples.
  - Three arguments **for**.
  - Three arguments **against**.