Bitcoin and Cryptocurrency Technologies
Lecture 1: Economics and History

Yuri Zhykin

Feb 8, 2021

Contacts

- @rodentrabies on Telegram
- https://github.com/rodentrabies

Course structure 1/2

- History and economics of Bitcoin
  - Economic concepts and properties of money
  - Computer cryptography and cypherpunk movement
  - Bitcoin invention and innovation
- Crypto means Cryptography
  - Cryptography basics
  - Hash functions
  - Public key cryptography
  - Elliptic curves
  - Cryptographic signatures
- Bitcoin chain data model
  - Transactions
  - Inputs and outputs
  - Blocks
  - Chain of blocks and Proof of Work

...

Course structure 2/2

...

- Bitcoin network
  - Peer-to-peer network architecture
  - Mempool and mining
  - Network parameters and dynamics
- Deep dive into Bitcoin transactions
  - Transaction scripts
  - Transaction validation
  - Bitcoin wallets
- Second layer protocols
  - Scalability problem
  - Payment channel networks
  - Non-fungible tokens
- Other cryptocurrency systems
  - Ethereum: maximum flexibility
  - Monero: maximum privacy

Economic concepts and properties of money

- **Money is any item or verifiable record that is generally accepted as payment for goods and services**
- **Durable** - able to retain its value over time
- **Portable** - easy to transport in sufficiently large quantities
- **Divisible** - can be divided into smaller quantities to represent whole range of value
- **Fungible** - two units of the same nominal value must be equally valuable
- **Scarce** - it must be very hard to increase the supply
- **Recognizable** - it must be easy to find peers willing to accept it as payment

Money before Bitcoin

- Seashells
- Silver
- Gold
- Paper money
- Fiat money

Cryptography and electronic money

- **Cryptography** is a method of protecting information and communications through the use of secrets that prevent third parties from accessing it
- Traditional electronic money - encrypted and centrally managed ledgers
- Is it possible to eliminate central management?
- **Byzantine Generals Problem** - how can two generals agree on when to attack, when then don't trust each other?
- **How can multiple parties come to a consensus when they trust no one?**

Centralized monetary system

- In most cases government is the central entity controlling monetary supply
- Assumption that government is competent enough to "manage" the economy
- Government can inflate fiat currency, effectively extracting resources from **all** its people without their consent
- Exclusive control over money is the ultimate tool of controlling people for totalitarian regimes

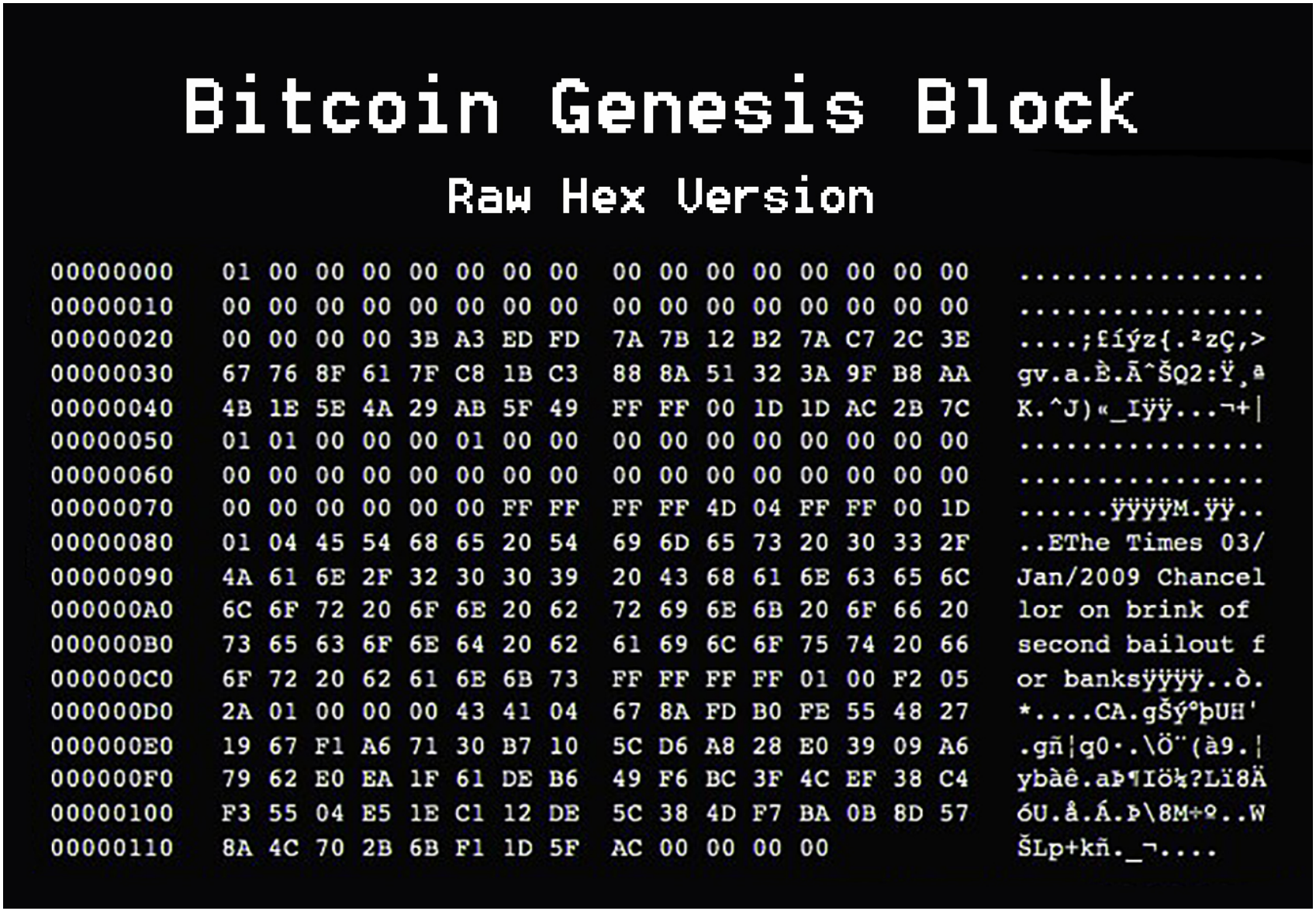
Cypherpunk movement

- Widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change
- **Can we use strong cryptography to solve BGP and create a decentralized monetary system?**
- Several attempts:
  - David Chaum - DigiCash, 1989
  - Wei Dai - b-money, 1998
  - Nick Szabo - Bit Gold, 1998
  - Adam Back - Hashcash, 1997-2002

Satoshi Nakamoto and Bitcoin Genesis 1/3

- Financial crisis of 2007-2008
- On October 31, 2008, pseudonymous person **Satoshi Nakamoto** published a whitepaper titled "Bitcoin: A Peer-to-Peer Electronic Cash System"
- In late 2008 - early 2009, Nakamoto contacted Wei Dai, Adam Back and Hal Finney about the electronic cash system he was working on
- On January 9, 2009, Nakamoto released version 0.1 of the Bitcoin software and launched the network by mining the **genesis block**

Satoshi Nakamoto and Bitcoin Genesis 2/3



Satoshi Nakamoto and Bitcoin Genesis 3/3

- Satoshi Nakamoto continued Bitcoin development until mid-2010, when he transferred control over the repository to Gavin Andersen
- On April 26, 2011, Nakamoto wrote his last known email to Gavin Andersen, and never appeared online since
- The Bitcoin software written by Satoshi Nakamoto is the basis for the Bitcoin Core project (https://github.com/bitcoin/bitcoin)

Bitcoin invention

- Cryptographic Proof of Work system solves the generalized Byzantine Generals Problem, eliminating the need to trust anyone on the network
- **Bitcoin is decentralized money**
- Transaction scripting system provides flexibility for more complex use cases then simple value transfering
- **Bitcoin is programmable money**

Market acceptance

- In 2010, the first known commercial transaction using bitcoin occurred when programmer Laszlo Hanyecz bought two Papa John's pizzas for 10,000 BTC
- In 2011, Bitcoin becomes accepted as donations by Electronic Frontier Foundation and WikiLeaks
- In 2011, price went from \$0.30 to \$5.27
- In 2012, from \$5.25 to \$13.30
- In 2013, from \$13.30 to \$770
- On February 8, 2021, bitcoin price is \$38831.60

Additional resources

- https://www.activism.net/cypherpunk/manifesto.html - Cypherpunk Manifesto
- https://unenumerated.blogspot.com - Nick Szabo's Blog
- The Bitcoin Standard: The Decentralized Alternative to Central Banking, 2018 - Saifedean Ammous
- Human Action: A Treatise on Economics, 1949 - Ludwig von Mises

The end

Thank you!