

Bitcoin and Cryptocurrency Technologies

Lecture 1: Economics and History

Yuri Zhykin

Feb 8, 2022

- @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

...

- Deep dive into Bitcoin transactions
 - Transaction scripts
 - Transaction validation
 - Bitcoin wallets
- Bitcoin network
 - Peer-to-peer network architecture
 - Mempool and mining
 - Network parameters and dynamics
- 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 - centrally managed ledgers, databases and communication encrypted
- Is it possible to eliminate central management?
- **Byzantine Generals Problem** - how can three generals agree on when to attack if they don't trust each other?
- **How can multiple parties come to a consensus without having to trust each other?**

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 3, 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

Bitcoin Genesis Block

Raw Hex Version

```
00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;ÉíÝz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ,ª
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_IÿŸ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿŸŸŸM.ŸŸ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿŸŸŸ..ð.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠŸ°pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ|q0·.\Ö"(à9.
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybâe.aÞ¶Iök?Lİ8Ä
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.â.Á.Þ\8M+ø..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 ŠLp+kñ._¬....
```

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 than simple value transferring
- **Bitcoin is programmable money**

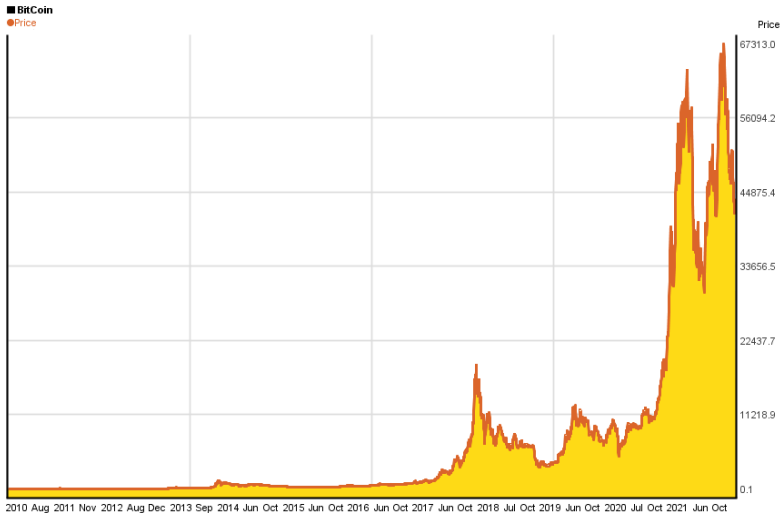
Market acceptance

- 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

Market acceptance 1/2

- 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~~ 2022, bitcoin price is \$44360.51

Market acceptance 2/2



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!