

# CMPSC 390/Art 387

## Crypto Introduction

Janyl Jumadinova and Byron Rich

January 19, 2021

# Cryptocurrency? Crypto? Bitcoin? Blockchain? ...



- Share what you know, have heard, have seen, etc.!

# Cryptocurrency? Crypto? Bitcoin? Blockchain? ...



- Share what you know, have heard, have seen, etc.!
- [Group Jamboarding Session!](#)

# Bitcoin vs. bitcoin vs. Blockchain

## Bitcoin:

Concepts and technologies that form the basis of a digital money ecosystem (cryptocurrency).

# Bitcoin vs. bitcoin vs. Blockchain

## Bitcoin:

Concepts and technologies that form the basis of a digital money ecosystem (cryptocurrency).

## bitcoin:

Unit of digital currency.

# Bitcoin vs. bitcoin vs. Blockchain

## Bitcoin:

Concepts and technologies that form the basis of a digital money ecosystem (cryptocurrency).

## bitcoin:

Unit of digital currency.

## Blockchain

A public transaction ledger (a data structure).

- 2008: The Bitcoin white paper

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.



Not this guy!

# Bitcoin

- 2008: The Bitcoin white paper

## Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto  
satoshin@gmx.com  
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

### 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.























Not this guy!

- 2009: Reference implementation



# Cryptocurrency Prices by Market Cap

<a href="#">Watchlist</a>   <a href="#">Cryptocurrencies</a>   <a href="#">Derivatives</a>   <a href="#">DeFi</a>   <a href="#">Storage</a>   <a href="#">Yield Farming</a>								
Show rows <b>100</b> ▼ <a href="#">Filters</a>								
#	Name	Price	24h	7d	Market Cap	Volume	Circulating Supply	Last 7 Days
1	 Bitcoin BTC	\$36,256.46	▲ 1.29%	▲ 13.21%	\$675,333,123,402	\$50,133,442,650 1,381,075 BTC	18,604,062 BTC	
2	 Ethereum ETH	\$1,229.70	▼ 0.00%	▲ 25.28%	\$140,739,352,729	\$26,199,411,910 21,278,776 ETH	114,306,428 ETH	
3	 Tether USDT	\$1.00	▲ 0.06%	▲ 0.10%	\$24,376,256,947	\$82,619,064,759 82,537,300,419 USDT	24,352,132,870 USDT	
4	 Polkadot DOT	\$16.69	▼ 0.77%	▲ 116.53%	\$15,060,778,359	\$3,839,919,941 229,895,688 DOT	901,687,549 DOT	
5	 XRP XRP	\$0.2828	▲ 1.86%	▲ 2.48%	\$12,834,394,625	\$3,311,914,827 11,716,507,094 XRP	45,404,028,640 XRP	
6	 Cardano ADA	\$0.3678	▼ 2.10%	▲ 46.97%	\$11,449,011,717	\$3,713,869,991 10,092,375,301 ADA	31,112,484,646 ADA	
7	 Litecoin LTC	\$149.09	▲ 4.52%	▲ 20.78%	\$9,899,435,595	\$6,561,025,968 43,946,860 LTC	66,308,091 LTC	
8	 Bitcoin Cash BCH	\$490.45	▲ 2.00%	▲ 14.05%	\$9,136,787,804	\$4,381,377,077 8,934,102 BCH	18,630,900 BCH	
9	 Chainlink LINK	\$21.89	▼ 4.21%	▲ 62.82%	\$8,795,679,399	\$3,963,604,843 180,932,609 LINK	401,509,556 LINK	
10	 Stellar XLM	\$0.2987	▼ 0.78%	▲ 29.08%	\$6,603,795,912	\$1,092,133,193	22,095,601,011 XLM	

<https://coinmarketcap.com/> as of January 18, 2021.

Rewards and Fees: <https://www.blockchain.com/stats>

# Trust?

## *Capital One Data Breach Compromises Data of Over 100 Million*

## Credit firm Equifax says 143m Americans' social security numbers exposed in hack

- Atlanta-based company says 'criminals' accessed personal data
- Before notifying public, Equifax executives sold \$1.8m in shares



# Trust?

## *Capital One Data Breach Compromises Data of Over 100 Million*

## Credit firm Equifax says 143m Americans' social security numbers exposed in hack

- Atlanta-based company says 'criminals' accessed personal data
- Before notifying public, Equifax executives sold \$1.8m in shares

### 27 MAY 2020 NEWS Data Breach at Bank of America

500K Zoom Accounts Discovered for Sale on the Dark Web

## Walgreens Reports Data Breach from Personal Mobile Messaging App Error

A report filed with California shows an internal error on the Walgreens messaging app exposed the personal messages stored on its database to be viewable by other customers.



# NOTICE OF DATA BREACH

Dear Customer,

We want to let you know about a sophisticated attack that we recently identified and quickly shut down, which may have impacted some of your personal information.



# Decentralization



- Here comes Blockchain!
- First, let's see what questions we need to think about answering.  
Take [the pre-survey](#)

# Blockchain

- **Decentralized control:** consensus of the community.
- **Tamper-evidence:** can immediately detect data tampering.
- **Nakamoto consensus:** have to provably spend resources when updating the blockchain.

# Centralization vs. Decentralization

## Centralization:

- Authority by a single party.
- Data stored by a single party.

# Centralization vs. Decentralization

## Centralization:

- Authority by a single party.
- Data stored by a single party.

## Decentralization:

- Authority according to a public protocol.
- Data stored by the participants.

# Centralization vs. Decentralization

## Centralization:

- Authority by a single party.
- Data stored by a single party.

## Decentralization:

- Authority according to a public protocol.
- Data stored by the participants.



client-server



peer-to-peer



# Cryptocurrency Components

- **Identity**: an account (**node**) in the system.
- **Transactions**: sending and receiving units of cryptocurrency.
- **Distributed Ledger**: a public record of transaction history (blockchain).
- **Trustless Consensus**: agreement on changes to the ledger.

# Identity: Private and Public Keys

- **Public Key:** represents an identity, used for “receiving”.
- **Private Key:** “unlocks” public key and the money, used for “redeeming”.

# Identity: Private and Public Keys

- **Public Key:** represents an identity, used for “receiving”.
- **Private Key:** “unlocks” public key and the money, used for “redeeming”.

[HOME](#) > [NEWS](#)

**A man who says he threw away a hard drive loaded with 7,500 bitcoins in 2013 is offering his city \$70 million to dig it up from the dump**

Tom Murray Jan 16, 2021, 5:55 AM



## *Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes*

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Don't be this guy!

# Identity: Private and Public Keys

- **Public Key:** represents an identity, used for “receiving”.
- **Private Key:** “unlocks” public key and the money, used for “redeeming”.

[HOME](#) > [NEWS](#)

**A man who says he threw away a hard drive loaded with 7,500 bitcoins in 2013 is offering his city \$70 million to dig it up from the dump**

Tom Murray Jan 16, 2021, 5:55 AM



*Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes*

Bitcoin owners are getting rich because the cryptocurrency has soared. But what happens when you can't tap that wealth because you forgot the password to your digital wallet?

Don't be this guy!

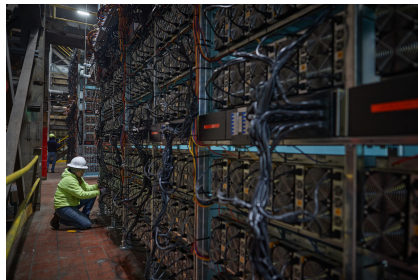
- **A bitcoin address:** representation of the recipient's public key, generated using cryptographic hash function.

My name is Janyl

ac1f48ead15cd2a75c318e0549b433c121020785d0ab1e2fb92473b1c98138d3

# Transactions

- Transactions are processed during a process called **mining**.
- Miners use computational power to verify and record transactions are rewarded with new bitcoin.



# Distributed Ledger: Record Keeping using Blockchain

- Data is stored by everyone.
- Updates are broadcasted to everyone.
- Transactions are bundled into **blocks** with links to enforce ordering.
- Miner creates a block by verifying transactions and solving a hashing problem.

# Consensus

- Process by which participants come to agreement (e.g., making changes to a ledger of transactions).
- Transactions are approved by **Proof-of-Work**.

# Consensus

- Process by which participants come to agreement (e.g., making changes to a ledger of transactions).
- Transactions are approved by **Proof-of-Work**.

More details on the process involved in blockchain next class!