



Cryptocurrency

A cursory introduction to Bitcoin, the Blockchain, and other cryptocurrencies



Table of Contents

- Bitcoin
 - Bitcoin..?
 - Centralized vs Decentralized
 - Bitcoin White Paper
 - Transactions and the Blockchain
 - Mining and Deflation
- Altcoins and Forks
 - Forking
 - Altcoins
 - Ethereum
 - Dapps and Smart Contracts
- Trading and Exchanges
- Looking ahead and Ethics



Cryptocurrency

"A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank."

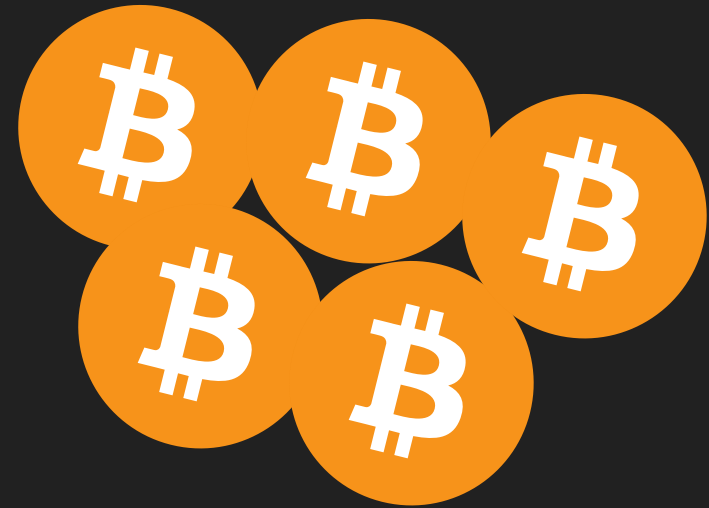


Bitcoins... What are those?



\$6.99 CAD

Now: \$9.99CAD



~\$3.00 CAD

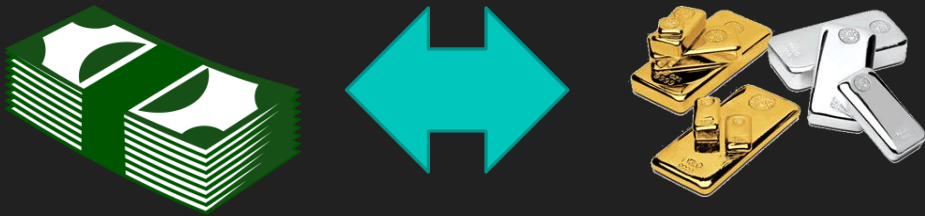
Now: ~\$50,000CAD

What gives Cryptocurrency *value*?

Fiat money

Fiat money is a currency without intrinsic value established as money by government regulation or law.

Representative Currency



Convertibility

Fiat Currency



Who would win?



Big Banks worth Trillions of \$



Magic Internet Money

Centralized Currency

- How is virtual money stored?
 - The “Ledger” approach
- Who keeps track of the “ledger”?
 - Banks. Banks do.
- All transactions are verified by the bank. They can take a cut of all your transactions.
- Banks are unreliable – See The Great Recession (2007)

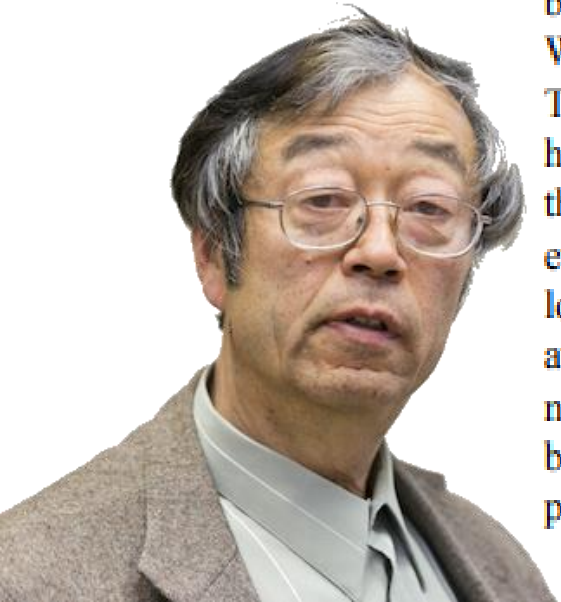


ID	Balance
Stalin	40
Lenin	40
Putin	40
Donald	500000000

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Dorian



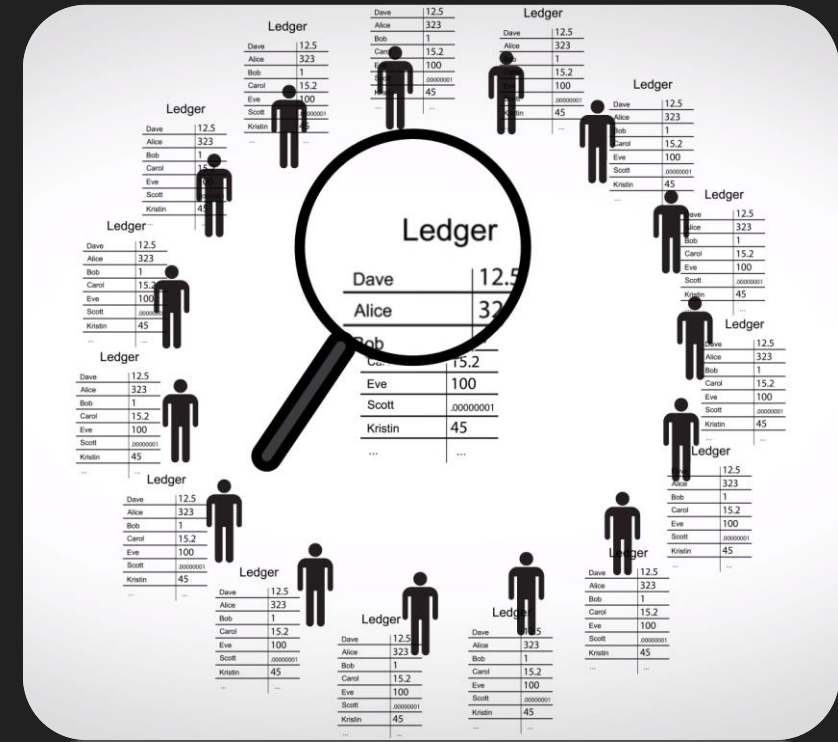
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

Nick



Decentralized Currency

- **Lower transaction costs:** Without the need of a middleman, costs are lower.
- **No need for trust:** Don't need to trust anybody specific in the system. Only need to trust the system.
- **Libre and Gratis:** Nothing is behind closed doors. Everything is open and free.



Decentralized Transactions

Every account created has a

Public Key: Think of this as an *home address*

Private Key: Think about this as a *key to the house*

For every transaction, there must be a:

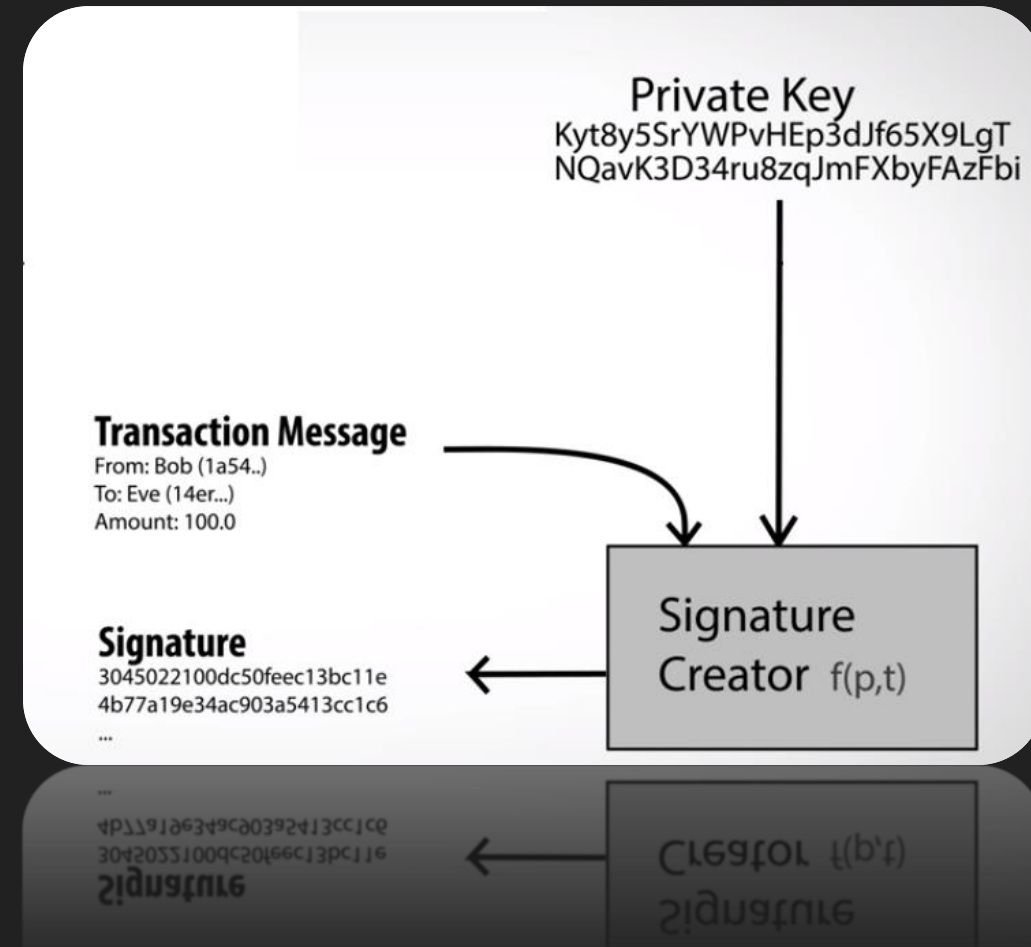
Signature

$f(\text{privateKey}, \text{transactionMessage})$

Each transaction's signature can be verified by:

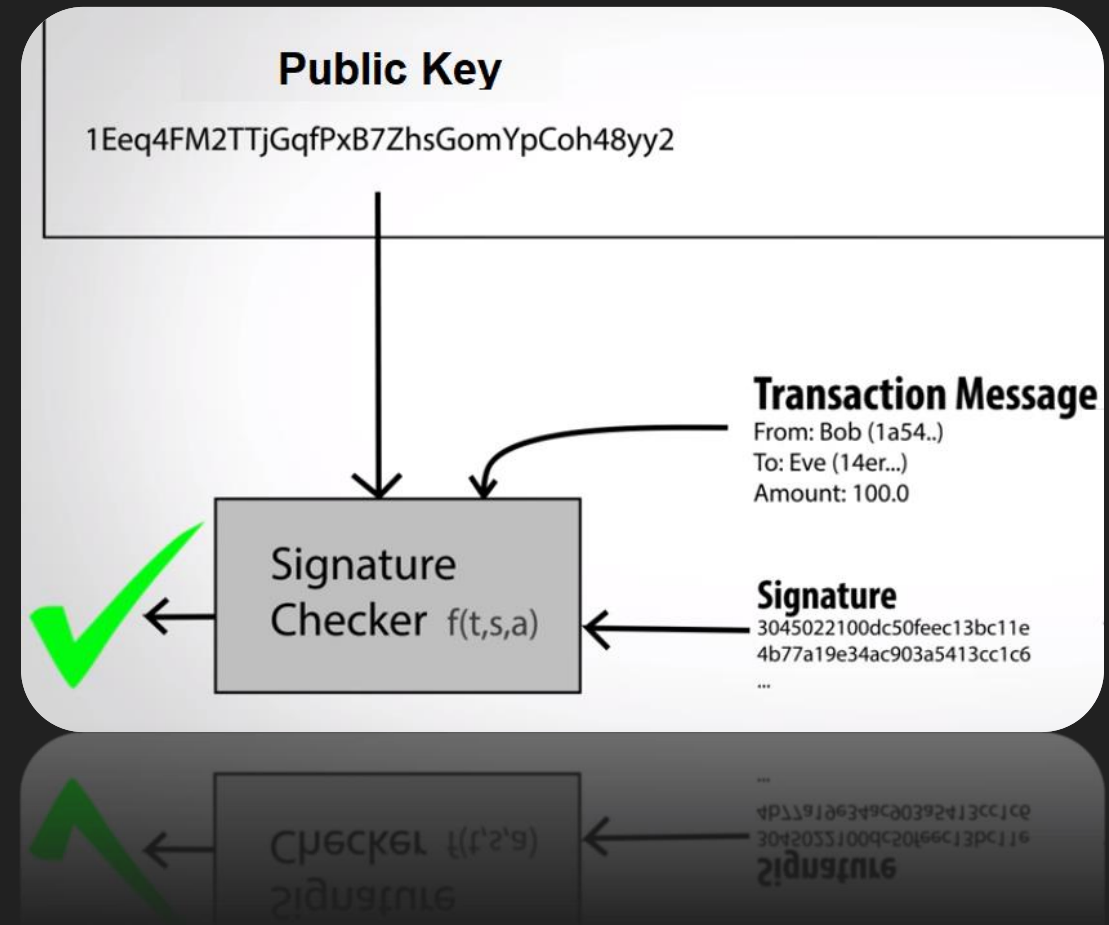
Checking a Signature

$f(\text{transactionMessage}, \text{signature}, \text{publicKey})$



Decentralized Transactions

- Signatures are **easy to verify** – but **NEAR impossible to forge**
- Signatures are unique – because they depend both on the Private Key and the Transaction Message
- Signatures are 'encoded' – you can't find out the private key from a signature



Decentralized Transactions

Cryptocurrencies use **Cryptographic Hashing Functions** to ensure that the information stored is secure.

The SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way function – it cannot be decrypted back.

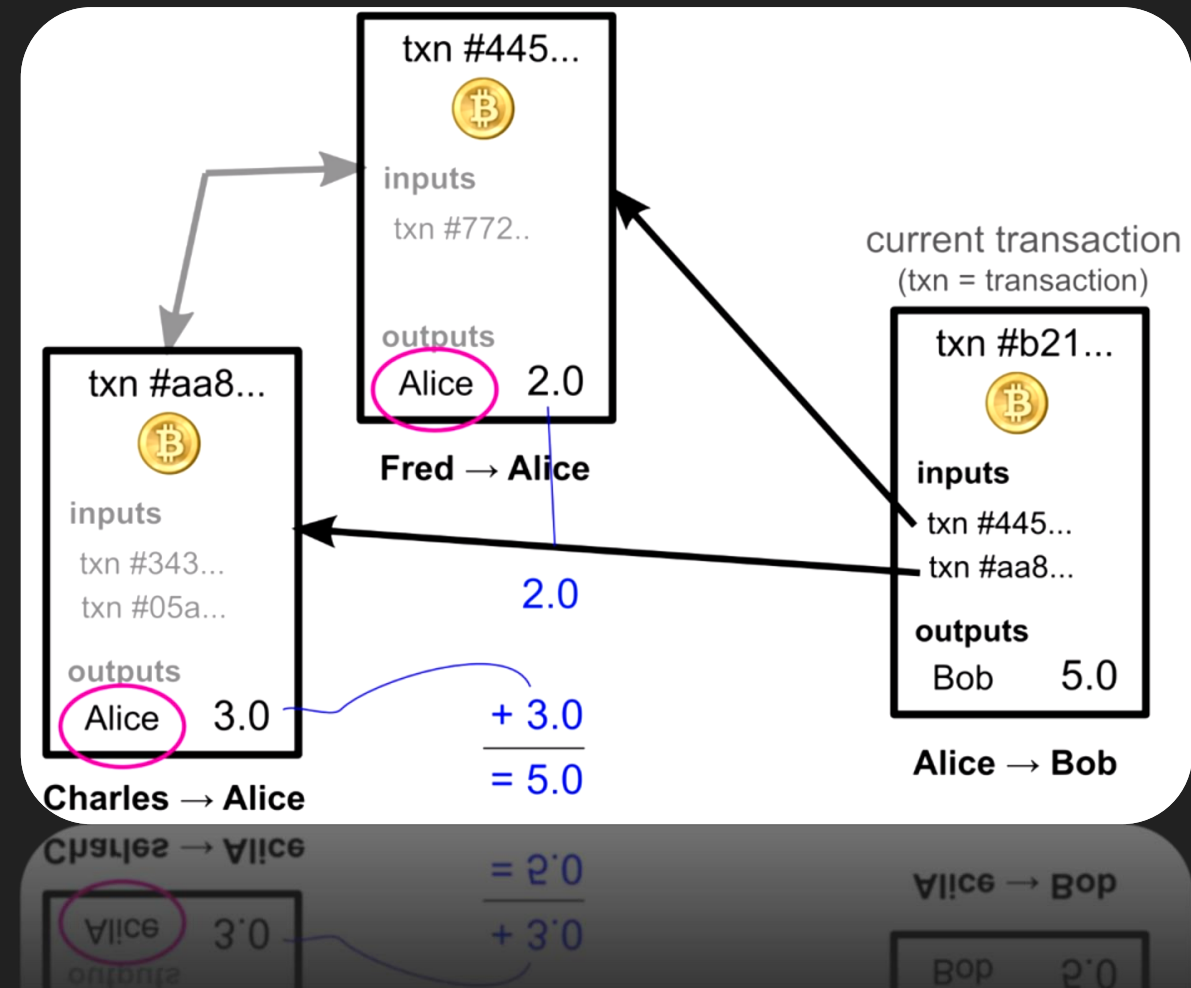
See: ECDSA – Elliptic Curve Digital Signature Algorithm

Input	SHA-256	Hash
The quick brown fox jumps over the lazy dog	>	d7a8fbb307d78094 69ca9abcb0082e4f 8d5651e46d3cdb76 2d02d0bf37c9e592
The quick brown fox jumps over the lazy dog.	>	ef537f25c895bfa7 82526529a9b63d97 aa631564d5d789c2 b765448c8635fb6c

Decentralized Transactions

To process a transaction, it must refer to previous transactions. This process **verifies** that the sender has enough currency to proceed with the transaction

For **leftover transaction currency** (e.g. Charles + Fred gave Alice 5.5 BTC, but she only sends 5.0 BTC to Bob), the leftovers are simply sent to Alice again – to be referenced in future transactions

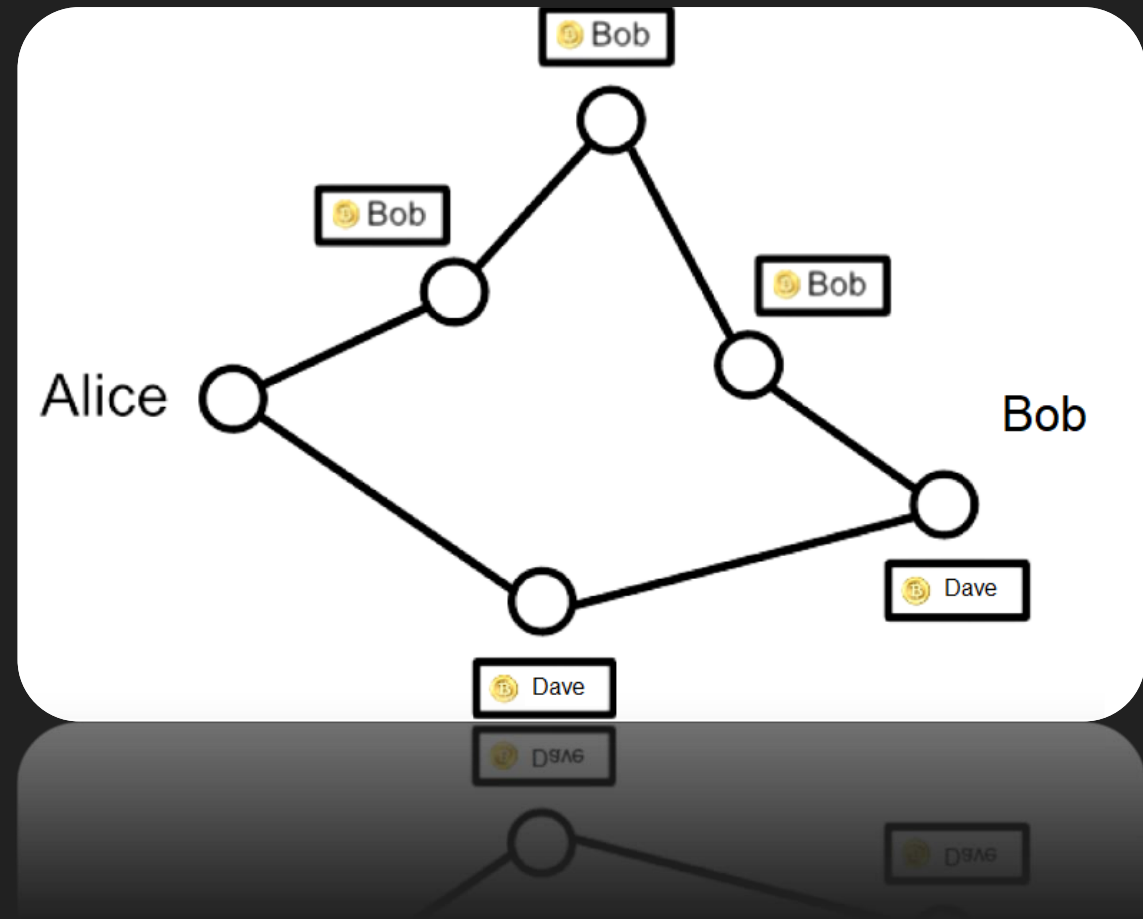


Decentralized Transactions

Double Spending Attack

We now know *who* sent transactions to who – but how do we know **the order** in which they occurred?

How do we get the entire network to agree on the transaction order?





Breaktime

We'll be right back – take ten!

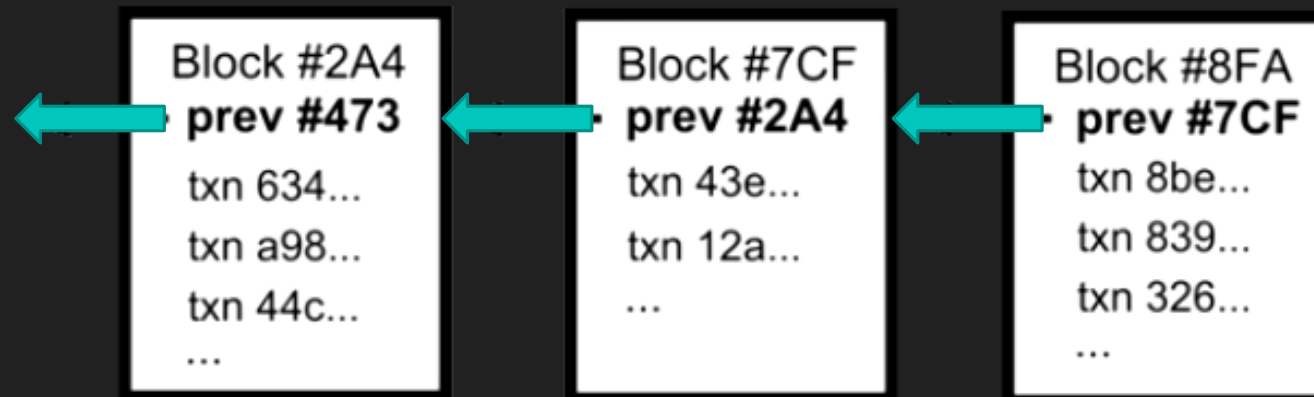


The Blockchain

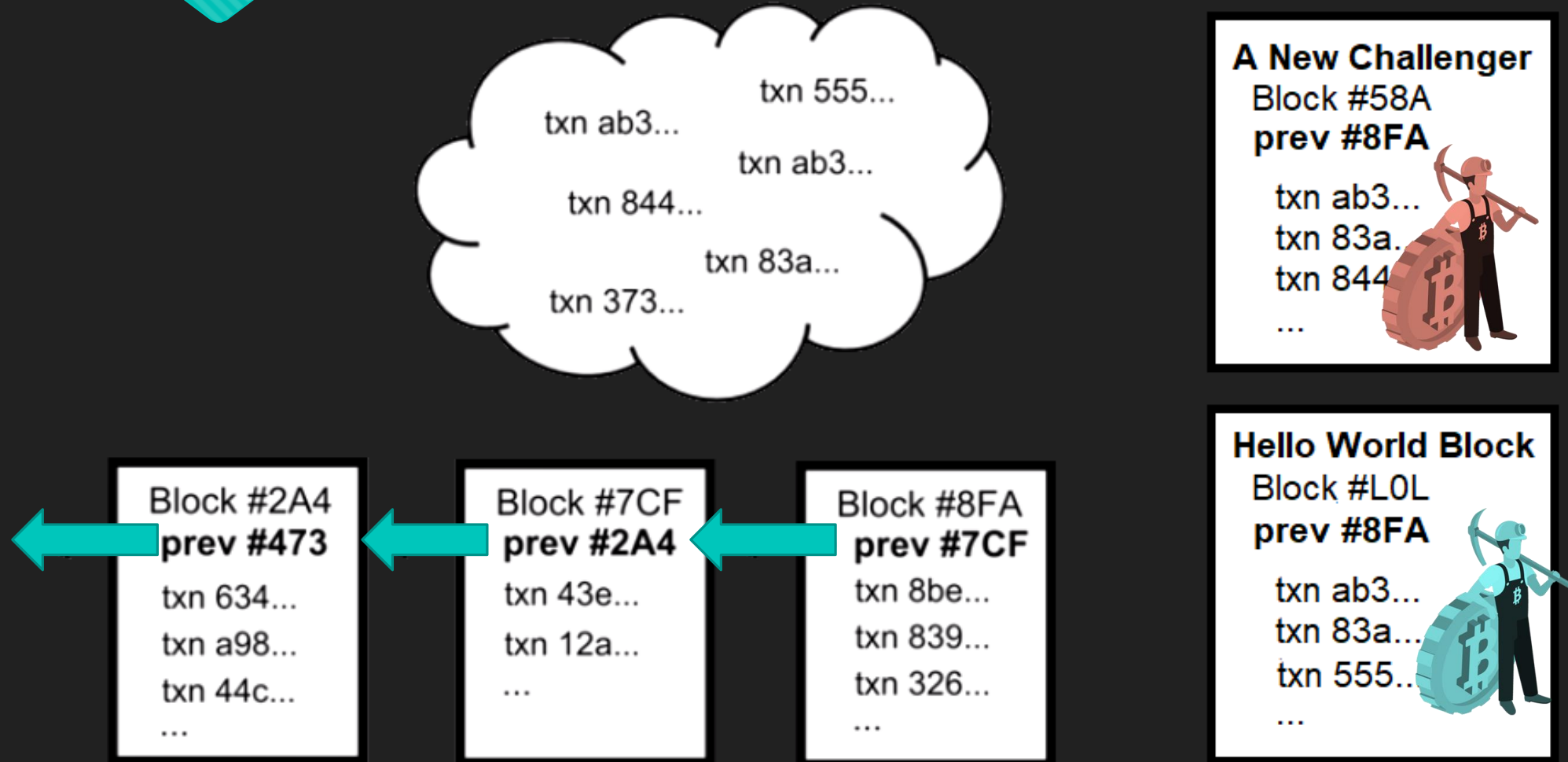
Through the usage of **public keys**, **private keys**, **signatures**, and **transaction messages**, we know who sent how much currency to who – and are able to verify it.

How do we verify **which transactions come first**?

The Blockchain. Blocks of orders are (nodes) added to the end of the chain after each verified transaction. By seeing where the transaction exists on the Blockchain, we can understand out which transaction came first.



The Blockchain



The Blockchain

To find out which Block is accepted into the Blockchain, we use try and solve a mathematical puzzle.

Block value is added with **nonce** – random guess.

$$f(\text{block}) < \text{threshold}$$

The **nonce** is repeatedly changed – brute force guess methods until the threshold is hit – then the block is accepted into the Blockchain.

A New Challenger

Block #58A

prev #8FA

txn ab3...

txn 83a...

txn 844...

...

nonce: 40x9184



The Blockchain

The time it requires for one computer to solve a block may take years. All computers guessing takes on average **10 minutes**.

The *miner*, or the person who solved the nonce and was accepted into the Blockchain receives a reward in Bitcoin - creation of currency.

The difficulty of finding the **nonce**, and therefore the **threshold** of acceptance is adjusted every two weeks to recalibrate the average solve time back to approximately 10 minutes.



The Blockchain

Since it takes to find a valid nonce miners usually gather in groups, or **Mining Pools**.

Each person in a mining pool contributes towards finding the correct nonce for future Blockchain blocks, and are rewarded periodically from the total pool of earnings of all of its members.

The Bitcoin reward is **halved** every four years – bitcoin is deflationary.





Forking and Altcoins

What are all these non-Bitcoin ripoffs?



Forking

Ideas and disagreements with the current status of Cryptocurrencies leads to **Forks**. Forks can either be **Hard Forks** or **Soft Forks**.

Forks copy the codebase of bitcoin. Some forks also copy the current Blockchain up to a point – that is, if you had 5BTC, you'll also have 5BCH (Bitcoin Cash).

Some forks are **successful** – Ethereum is a fork off of Ethereum Classic. Some forks are **unsuccessful** – Bitcoin Cash is not accepted at most vendors or exchanges



Altcoins

Altcoins are cryptocurrencies that were created after the initial success of Bitcoin. These include:

- **Ethereum**
- **Litecoin**
- **Ripple**
- **Dogecoin**
- **More...**

New coins are being created all the time – usually through something called **Initial Coin Offerings (ICOs)**.



Ethereum

Ethereum is another cryptocurrency that is on the rise. It has the **2nd highest market cap** at \$27B following Bitcoin's \$114B.

Primarily it is differentiated from bitcoin due to:

- Distributed Apps (Dapps)
- Smart Contracts

Ethereum's Ether is the primary currency for most ICOs nowadays.

Distributed Applications

Imagine having your car working away, transporting passengers while you're at work. Imagine having your computer utilizing its spare capacity to serve businesses and people across the globe.

This is the goal of distributed apps, or Dapps.

Golem

CGI artists will be able to rent computing resources from other users to render an image quicker. Likewise, an idle machine can also accept tasks from other users.



Smart Contracts

Smart contracts are account holding objects on the Ethereum Blockchain. They contain code functions and can interact with other contracts, make decisions, store data, and send ether to others.

These things run on a concept called 'Gas'.

For example, if you wanted to help someone run a Dapp on your machine, you could sign a Smart contract to receive Ether after your machine fulfills the contract on your end and his end.



Trading and Ethics

Coin Exchanges, Finances, and Ethical Implications of Cryptocurrencies



Trading Cryptocurrencies

Cryptocurrencies are often traded on websites called **Coin Exchanges**. These exchanges often charge a small transaction fee to trade for you.

Popular coin exchanges include:


- Coinbase
- Kraken
- QuadrigaCX
- GDAX

Important note: You do not actually 'own' the coins



Trading Cryptocurrencies

anyone can kill your contract #6995

 Closed

ghost opened this issue 11 days ago · 13 comments



devops199 commented 22 hours ago · edited

I accidentally killed it.

<https://etherscan.io/address/0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4>

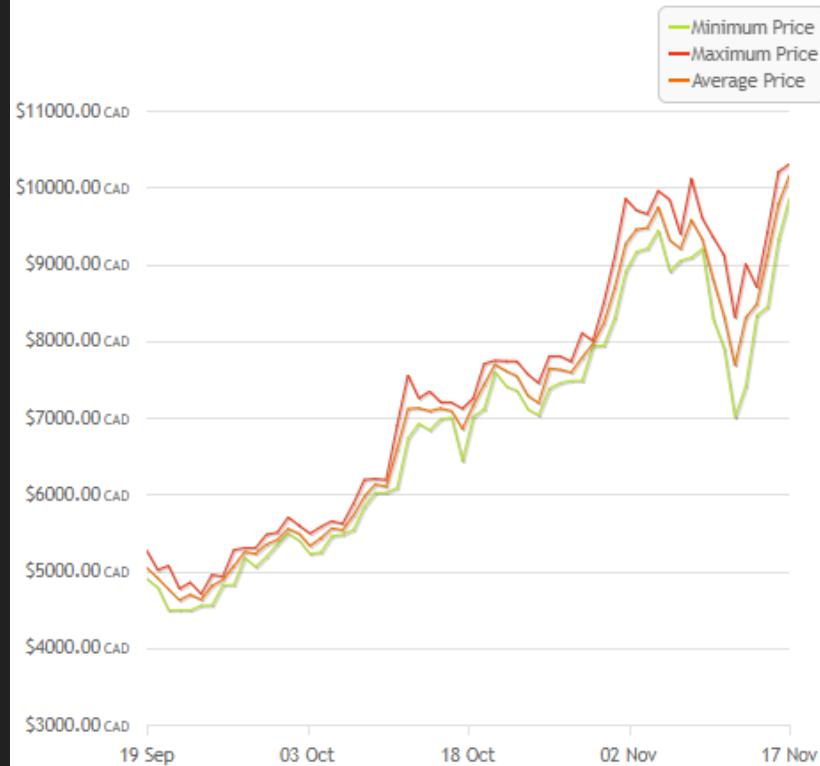
Trading Cryptocurrencies

*On November 7th, 2017 a user “accidentally” screwed something up. A lot of people/companies/ICOs are using Parity-generated multisig wallets. **About \$300M of ETH** is frozen and (probably) lost forever.*

*In February 2014, Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than **\$450 million at the time**.*

Trading Cryptocurrencies

XBT/CAD Price - Last 60 days



My Latest Trades

[more »](#)

	In	Out	Price	Pair
←	\$2,105.60 CAD	0.22400000 XBT	\$9,400.00 CAD	XBT/CAD
→	0.22500000 XBT	\$1,732.27 CAD	\$7,699.00 CAD	XBT/CAD
←	\$1,400.80 CAD	0.16000000 XBT	\$8,755.00 CAD	XBT/CAD
←	\$5.57 CAD	0.00063843 XBT	\$8,735.00 CAD	XBT/CAD
←	\$349.40 CAD	0.04000000 XBT	\$8,735.00 CAD	XBT/CAD
→	0.20200000 XBT	\$2,005.86 CAD	\$9,930.00 CAD	XBT/CAD

→ 0.50500000 XBT 25'002'86 CAD 28'230'00 CAD XBT/CAD

← 23'18'10 CAD 0.04000000 XBT 28'132'00 CAD XBT/CAD

Trading Cryptocurrencies

FOMO – Fear of Missing Out

HODL – Hold on for Dear Life

Moon – It's going to the moon (large increase)

Bullish – Going good. Price is rising or are expected to rise

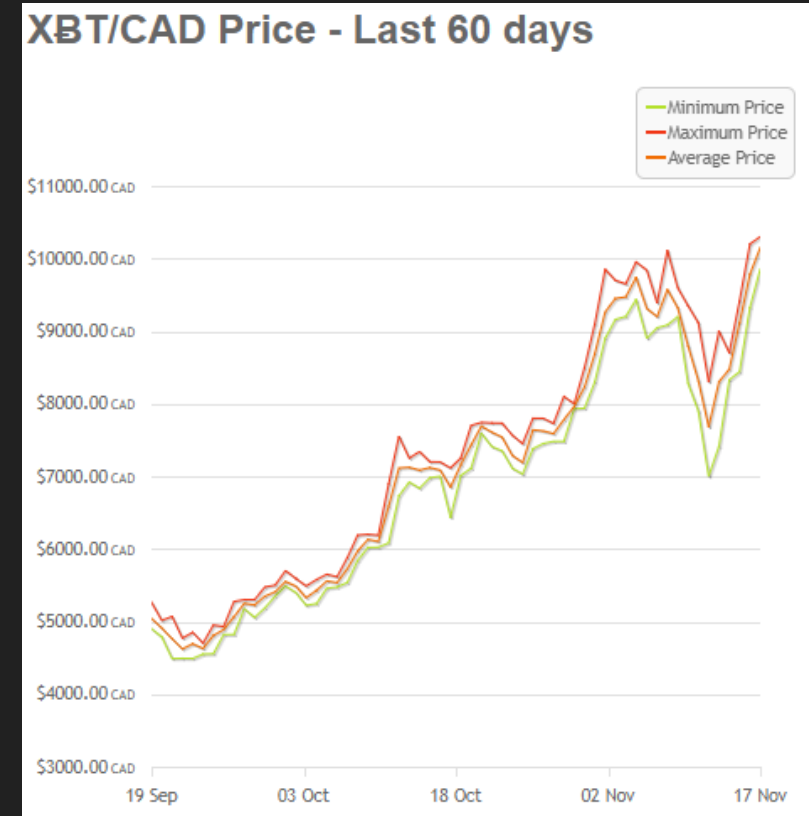
Bearish – Going badly. Price is declining or expected to decline

Futures – Buying/selling at a given date in the future at a predetermined price

ICO – Initial coin offerings, Exchanging BTC/ETH for future cryptocurrencies

Dip – A temporary decrease in value that will recover

Correction – A large increase or decrease that was long overdue



Ethics and Disadvantages

- Cryptominers
- Idea is great – execution...
 - Parity Multisig Wallet Breach, etc.
- Might compete with local currency
 - Banned in Russia, Vietnam, China
- Can be used for illegal activities
 - The Silk Road
 - Supporting anti-government organizations

Getting Involved

- Downloading a Cryptocurrency Wallet
 - Start Mining!
 - Join Mining Pools
- Joining a Coin Exchange
 - Coinbase, GDax, Quadriga, Kraken
- Researching Further
 - Going to cryptocurrency meetups (Ethereum hackathon @ Waterloo, Devcon 3)



Cryptocurrency

Thanks for coming out!

Our slides will be posted on csec.club/seminars

Go to the AMACSS Gaming Night for free Pizza and Games!

6-8PM @IC200/IC204

