What is cryptocurrency and why does it matter?

Jacob Robinson

January 25, 2023


Bitcoin BTC
Bitcoin Cash BCH
Ethereum ETH
Ethereum ETH
Ethereum ETH
Ethereum Classic ETC
Litecoin LTC
Litecoin LTC
EOS EOS
Litecoin Cash LCC
Litecoin Cash LCC
IOTA MIOTA
DASH DASH
Dragonchain DRGN
Ripple XRP
Monero XMR
NEO NEO
Qtum QTUM
Stellar XLM
NEM XEM
Steem STEEM
Stratis STRAT
Zcash ZEC
Bytecoin BCN
Augur REP
Cardano ADA
Decred DCR
Simple Token OST
Raiblocks XRB
ReddCoin RDD
Lisk LSK
ICON ICX
Bitshares BTS
Bitcoin Gold BTG
Waves WAVES
Hshare HSR
Status SNT
Komodo KMD
Kin KIN
Dent DENT
Po.et POE
Bitquence BQX
Verge XVG
Omiseo OMG
Ardor ARDR
Populous PPT
Waves WAVES
Siacoin SC
Dogecoin DOGE
VECHAIN VEN
GOLEM GNT
DIGIBYTE DGB
EXPERIENCE POINTS XP
VERITASIUM VERI
FUNFAIR FUN
Revain R
Binance Coin BNB
KuCoin Shares KCS
Ark ARK
Ethos ETHOS
Request Network REQ
Electroneum ETN
Salt SALT
QASH QASH
U.CASH UCASH
Nano XRB
Digix DAO DGD
Basic Attention Token BAT
Nexus NXS
Peercoin PPC
Civic CVC
District0x DNT
Edgeless EDG
Matchpool GUP
Numeraire NMR
0x ZRX
Aragon ANT
WeTrust TRST
Wings WINGS
Bancor BNT
AidCoin AID
TRON TRX
TETHER USDT
BridgeCoin BCO

Daily Mail, Tuesday, December 5, 2000

Internet 'may be just a passing fad as millions give up on it'

THE Internet may be only a passing fad for many users, according to a report.

Researchers found that millions were turning their back on the world wide web, frustrated by its limitations and unwilling to pay high access charges.

They say that e-mail, far from replacing other forms of communication, is adding to an overload of information.

Experts from the Virtual Society project, which published the report, say predictions that the Internet would revolutionise the way society works have proved wildly inaccurate.

Many teenagers are using the Internet less now than previously, they conclude, and the future of online shopping is limited. Steve

By **James Chapman**
Science Correspondent

Net loss: Two million Britons have logged off the Internet

Woolgar, director of the society, said: "We are often presented with a picture of burgeoning Internet use, but there is evidence already of drop-off and saturation among users.

"Teenagers' use of the Internet has declined. They were energised by what you can do on the Net but they have been through all that and then realised there is more to life in the real world and gone back to it."

The project, sponsored by the Economic and Social Research Council, gathered together research by 25 universities across Europe and the U.S.

It estimated that in Britain alone there could be more than two million people who regularly used the Internet but had now given up.

Analysts say some simply became bored, while others were frus-

EXCLUSIVE!

NOW
IN
COUL

"A tool for computer experts"

"Not secure, no one will share information"

"Not useful, I don't use it in my daily life"

"A tool for computer experts"

"No one will use this for payments"

"I don't use it in my daily life"

The Internet? Bah!

Hype Alert: Why cyberspace isn't, and will nev

By Clifford Stoll

After two decades online, I'm perplexed. It's not that I haven't had a gas of a good time on the Internet. I've met great people and even caught a hacker or two. But today I'm uneasy about this most trendy and oversold community. Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems.

pretense of completeness.
ers or critics, the Internet h
unfiltered data. You don't k
what's worth reading. Logg
Web, I hunt for the date o
Hundreds of files show up,
unravel them—one's a bi
eighth grader, the second
doesn't work and the third
monument. None answers
search is periodically inter
"Too many connections, try

Won't the Internet be us
net addicts clamor for gover
Andy Spano ran for county
County, N.Y., he put every p
paper onto a bulletin board
with plenty of computer co
ers logged in? Fewer than 3

Instantly share and transfer information

Accessible anywhere

Highly distributed

No single point of failure

Crypto Is Now Dead

FTX, a cryptocurrency exchange, collapsed last week, proving a lot of cool guys horribly wrong

Chetan Bhagat

Bitcoin, the original cryptocurrency, the gold standard for all things crypto, crashed last week. Bitcoin prices fell a whopping 75% in the last year, or down to a fourth of its value. This, for something touted to be a better store of value than gold, US dollars or any other fiat currency or precious metal.

Other cryptocurrencies have done worse. Many are down 80-90% in a year, some completely wiped out. Most investors in crypto are now sitting on losses. FTX, one of the big crypto exchanges, where people come to trade and store their cryptocurrencies, also collapsed last week. This was due to massive alleged irregularities, including customer deposits being inappropriately used to buy and prop up the company's own issued cryptocurrency, the FTT token.

Sam Bankman-Fried, the 30-year-old CEO of FTX, who works out of an island in the Bahamas apologised on Twitter. FTX filed for bankruptcy, wiping out $32bn of value which FTX had in the last funding round. Sam himself lost most of his $17bn fortune in days. Customers, lenders and employees of FTX all have money stuck in the company, all probably gone. Other crypto entities like Celsius Network, Three Arrows and Voyager also went belly up last year, making investors lose billions.

Crypto is done. This toxic nonsense now stands exposed. However, it is interesting to go through what happened that made crypto into the world's greatest con. In this are lessons for all of humanity, on how easily we can be fooled as people.

- The warnings were there.
- One of the world's greatest investors, Warren Buffet had said he wouldn't buy all the Bitcoin in the world for $25.
- He noted that ultimately, he would have to sell it to someone else to get rid of it, as it had no other use.
- As the famous quote by Gertrude Stein goes, "There is no there there," implying something with no substance.
- This applies to cryptocurrencies too, which have no end use, no exit, no purpose, really.

Vishnu Sahu

And yet, how they boomed. Bitcoin grew over 5,500% from March 2017 to March 2021 alone! Instagram was filled with crypto millionaires buying yachts and Lamborghinis.

Crypto was the ethical, purer, more transparent and 'good' alternative to normal fiat currencies. Every Bitcoin transaction is in the blockchain ledger, so it is all in the open! There's a limited number of Bitcoins, they can't be printed indiscriminately like governments print money! Hedge funds, banks, brokers, reporters – anyone in the finance business had a 'crypto view' and 'crypto strategy'. Bitcoin was mainstream.

In the middle of all this, it was hard to be a crypto sceptic. Buffet was called "too old and dated".

The money flow to crypto was so good that many intermediary firms were created. They called themselves exchanges. Many of them were simply casinos of speculation. People blindly trusted them with their money. None of it was regulated. Nothing was transparent. But ordinary people took loans, sold homes, put their life savings in this once in a lifetime opportunity. Most are sitting on heavy losses. Some are wiped out.

Crypto became like communism, which promises power to the people through decentralisation, but ultimately leads to power in the hands of a select few. Plus, whenever something is regulation-government free, it also attracts the shadiest characters and most unethical behaviours. And that is exactly what happened

Crypto became like communism, which promises power to the people through decentralisation, but ultimately leads to power in the hands of a select few. A few cult-like stars of crypto became the power-centres. Their opaque intermediate entities ran the show and took their cult-like followers for a ride. Big celebrity brand ambassadors were hired. Crypto followers, like religious followers, simply 'believed' in it all.

Terms like HODL or 'Hold on to dear life', which means to never sell, even if the market crashes, became popular. Of course, the biggest believer was usually the one to be left standing behind with the biggest losses. And since all this was unregulated, there was no recourse. The government was the problem you see. However, whenever something is regulation-and-government-free, it also attracts the shadiest characters and most unethical behaviours. And that is exactly what happened.

Then followed the imminent collapse. Bubbles eventually burst, we just don't know when and which needle will prick it. This time, it was the collapse of FTX, in an environment of high inflation, high interest rates and generally decreased risk appetite. Now, there will be few new takers for crypto. You really want to put your hard-earned money in the hands of a 30-year-old unregulated nerd in the Bahamas?

Crypto is never coming back. It's done. Please do not waste your money on it. It is not an investment. Stay away from it. If you already lost money, sorry. Hope the lesson was learnt. Lessons that apply to all who want to invest money. Investing is boring. Real returns take a lot of time.

Remember these truths:

- There's no quick money.
- There's no 'it's different this time.'
- There's no 'old-fashioned thinking' when it comes to money.
- Young and cool doesn't make it a good investment.
- Value, real assets, cash generation, end use, they all matter.
- Regulation and government backing matters.

Make money the long hard way – by working hard, being innovative, solving customer needs, earning, saving, and investing in real assets and companies. It's the only way that has worked, and it's the only way that will work in the long term. Stay away from Bitcoins, and get yourself some CommonSenseCoins!

Instantly share and transfer value

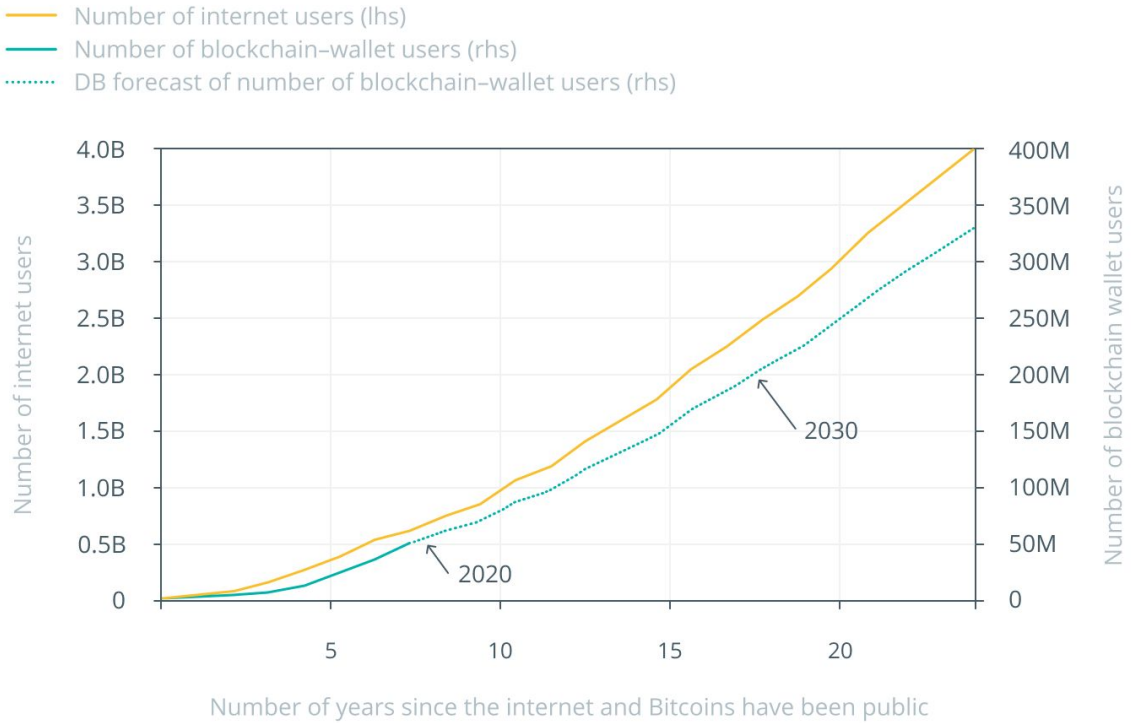
Accessible anywhere

Highly distributed

No single point of failure

Global network

Adoption rates of cryptocurrencies and internet



cointelegraph.com

source: ***Deutsche Bank***

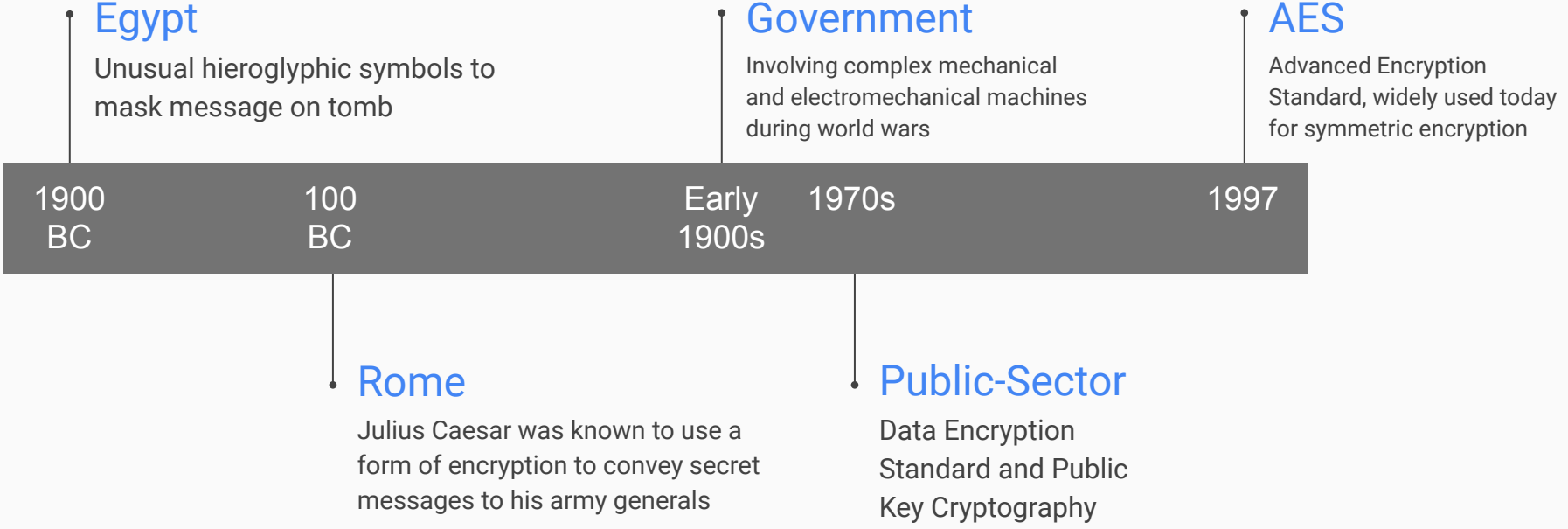
Agenda

1. **Origins of cryptocurrency**
2. **Bitcoin**
3. **Digital assets**
4. **Why this matters**

1. History

Cryptography

The use of codes and ciphers to protect secrets began thousands of years ago

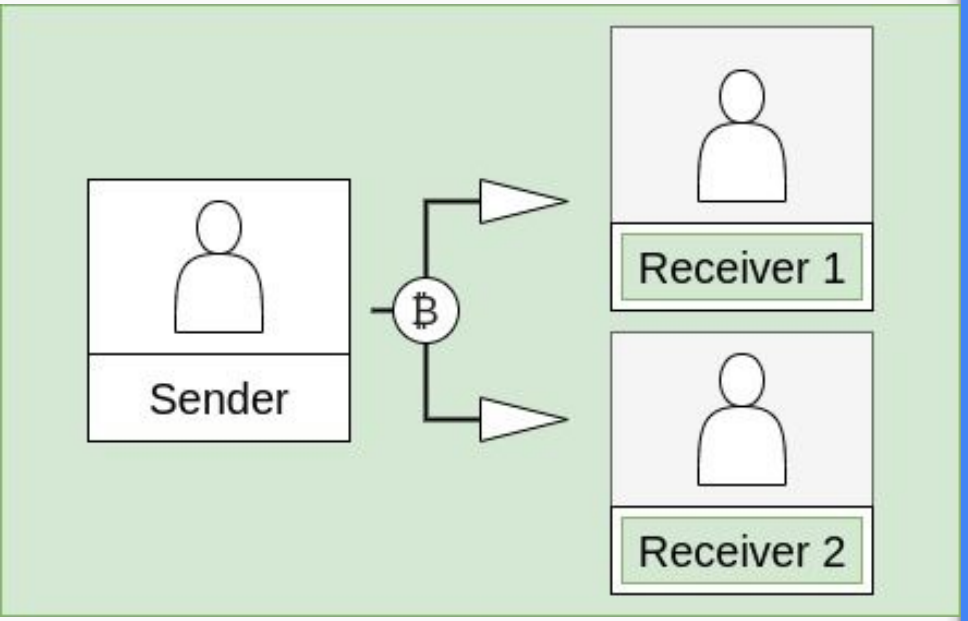


Digital Money & Centralized Intermediaries

When cryptography became widely available and studied in the 1980’s, many researchers began studying the idea of digital money.

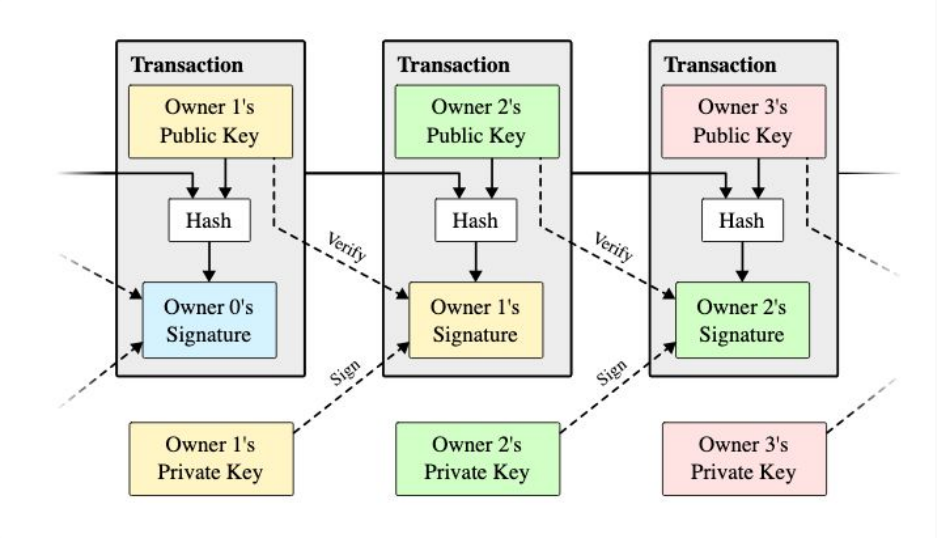
Early digital currency projects issued digital money, usually backed by a national currency or precious metal.

These currencies worked, but were beholden to a centralized intermediary - much like a bank - who acted as a clearinghouse to settle transactions at regular intervals.



The Challenge

2. Bitcoin



The Solution

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.

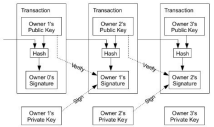
1. Introduction

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. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

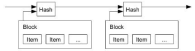


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

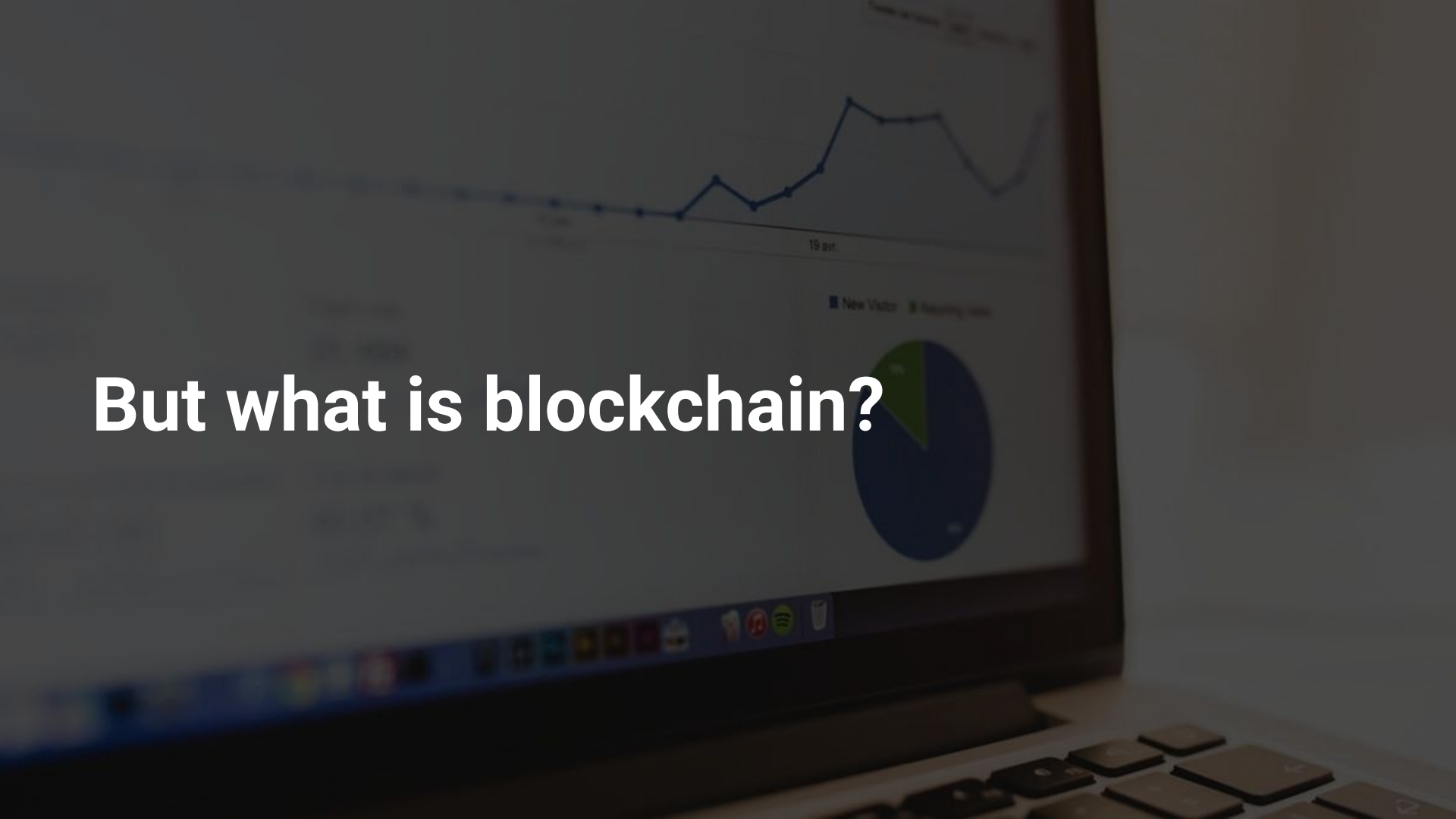
3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



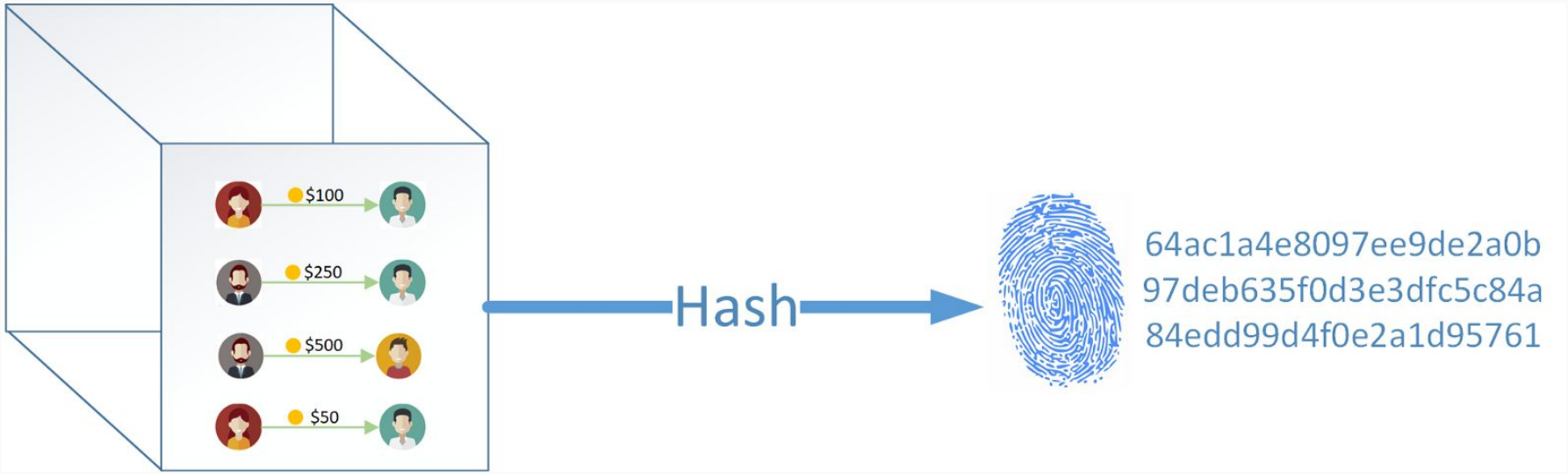
Bitcoin, a peer-to-peer electronic cash system, was outlined in a white paper published by Satoshi Nakamoto.

It introduced a blockchain.

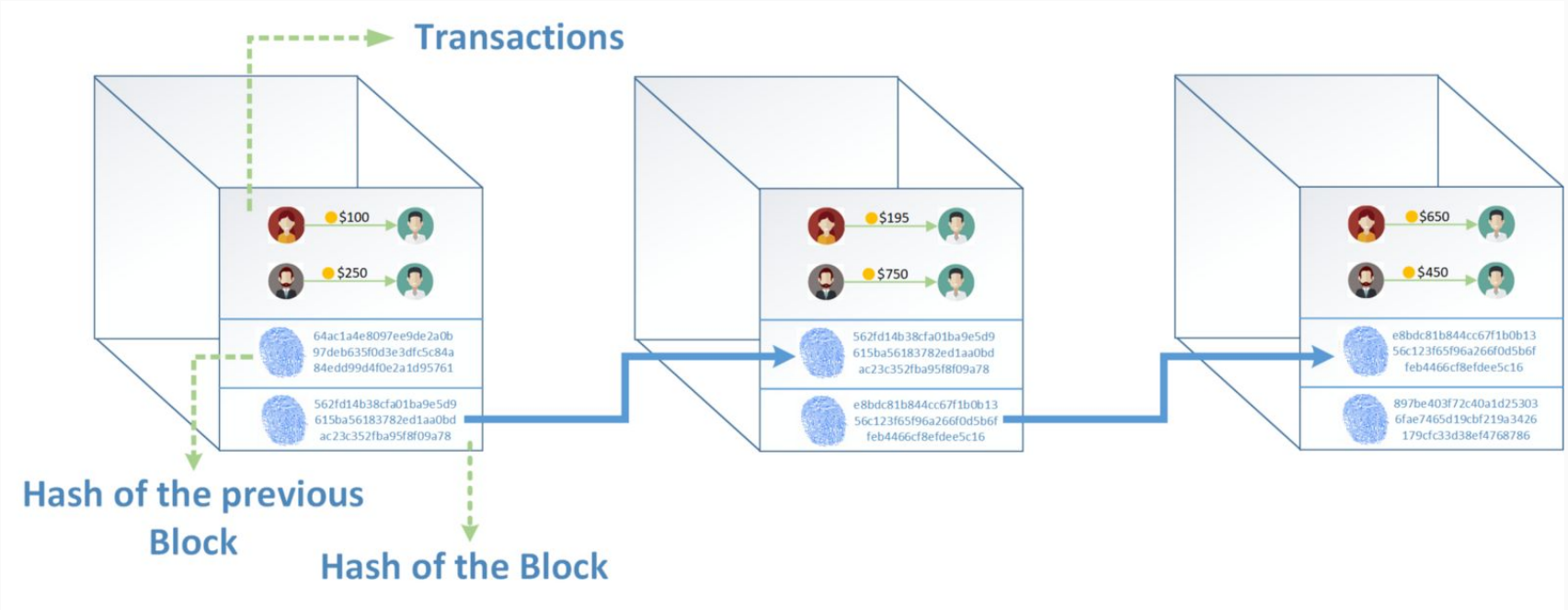


But what is blockchain?

The Block


$100
$250
$500
$50
Hash
64ac1a4e8097ee9de2a0b
97deb635f0d3e3dfc5c84a
84edd99d4f0e2a1d95761

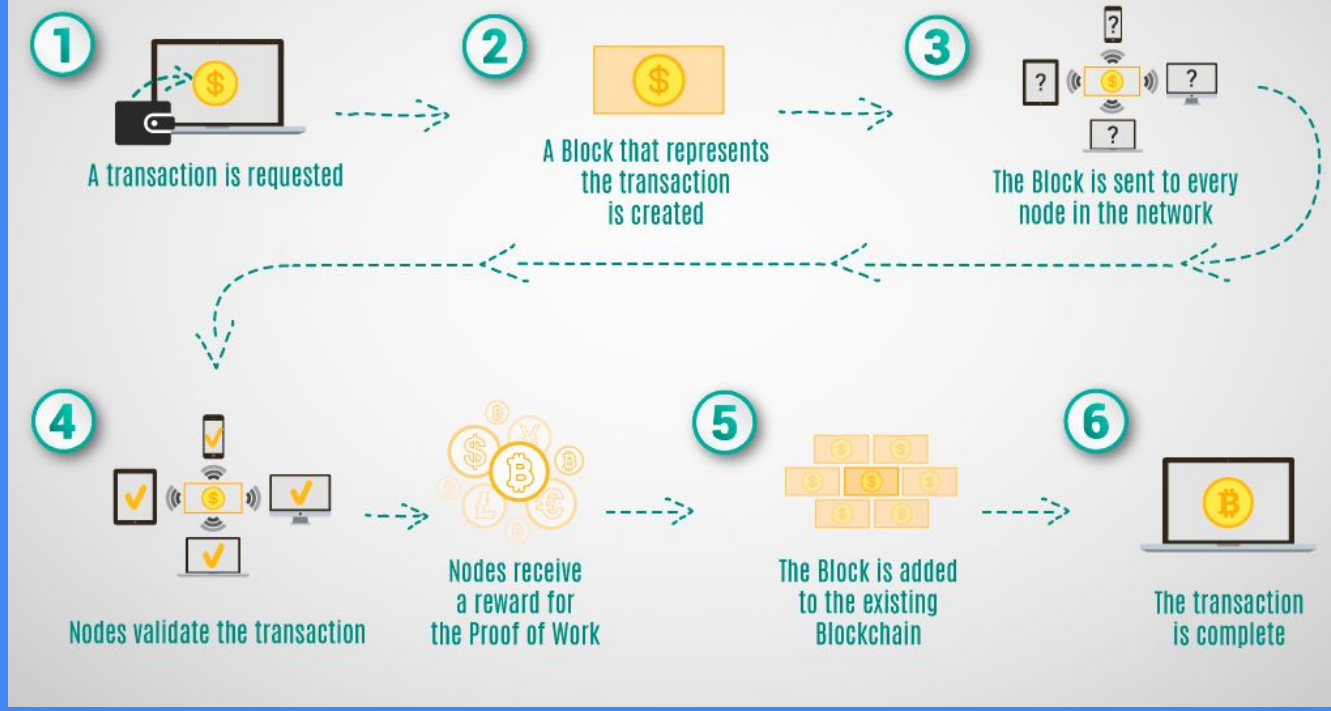
The Chain


Transactions
$100
$250
64ac1a4e8097ee9de2a0b
97deb635f0d3e3dfc5c84a
84edd99d4f0e2a1d95761
562fd14b38cfa01ba9e5d9
615ba56183782ed1aa0bd
ac23c352fba95f8f09a78
$195
$750
562fd14b38cfa01ba9e5d9
615ba56183782ed1aa0bd
ac23c352fba95f8f09a78
e8bdc81b844cc67f1b0b13
56c123f65f96a266f0d5b6f
feb4466cf8efdee5c16
$650
$450
e8bdc81b844cc67f1b0b13
56c123f65f96a266f0d5b6f
feb4466cf8efdee5c16
897be403f72c40a1d25303
6fae7465d19cbf219a3426
179cfc33d38ef4768786
Hash of the previous Block
Hash of the Block

A collection of technologies packaged together to:

- Permit transactions to be recorded on a ledger
- Provides access to the ledger of transactions
- Cryptographically secure ledger in chronological order

HOW BLOCKCHAIN WORKS



TYPES OF BLOCKCHAIN WALLETS

Types of software wallets include web (or crypto exchange) wallets, mobile wallets, and desktop wallets. A hardware wallet is a physical device that secures access to your cryptos offline.

Hosted by an Exchange

Software on a Smartphone or Tablet

Software for PC Users

Access to Your Cryptos Stored Offline

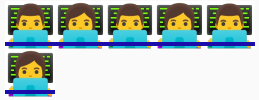
The Motley Fool

Innovation

Cryptocurrencies are not something you buy - they are a tool you use

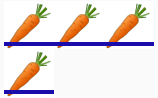
Nodes

Anyone can participate in the consensus protocol of the blockchain



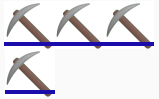
Proof of Work

However, participating in the consensus protocol requires proving your interest in the network's success



Incentives

These participants are incentivized to act honestly, in furtherance of the network, through mining rewards



Miners

Anyone can become a miner by acquiring and connecting the necessary hardware to the blockchain network

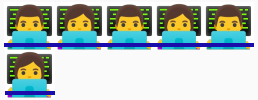
Open Consensus

Think: Pickup basketball

There are no set of fixed participants who work for Bitcoin Inc. that manage the blockchain.

No security: anyone can join the network.

Proof of Work



Think: Rolling dice

Preventing a Sybil attack:

To masquerade as a thousand people, you'd have to do the work of a thousand people, which will cost a thousand times the work of a single person

So long as 51% of the work is honest, open consensus was possible for the first time in history.

Mining

Think: Carving in stone

Why participate in the bitcoin blockchain?

By conducting Proof of Work computations, miners receive a reward of bitcoin.

Cryptographically predictable, following a deflationary supply of 21 million bitcoin.

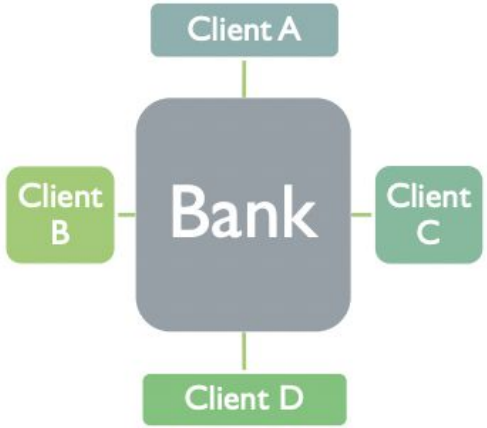
Cryptocurrency

Think: Arcade tokens

Bitcoin is an example of a cryptocurrency. It’s used to transact across the internet and to incentivize participants in the network.

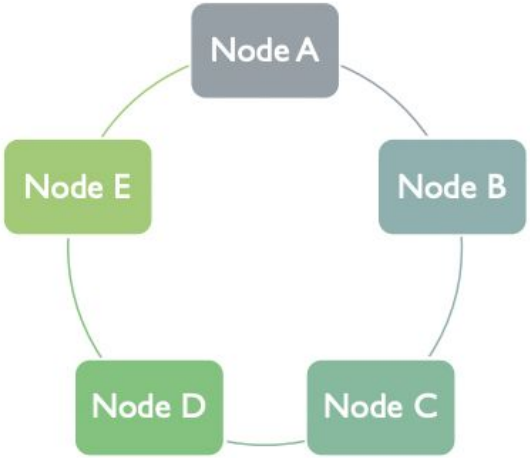
Decentralization

Centralized Ledger



There are multiple ledgers, but Bank holds the "golden record" Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

Distributed Ledger



- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."

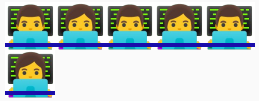
3. Digital assets

Not limited to cryptocurrencies

Digital assets are not something you buy - they are a tool you use

NFTs

Unique assets that can reference ownership in underlying art, rights or property - think: making digital files ownable

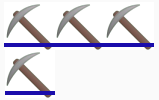


DAOs

Social networks, messaging apps and other internet-based organizations controlled by online communities

Stablecoins

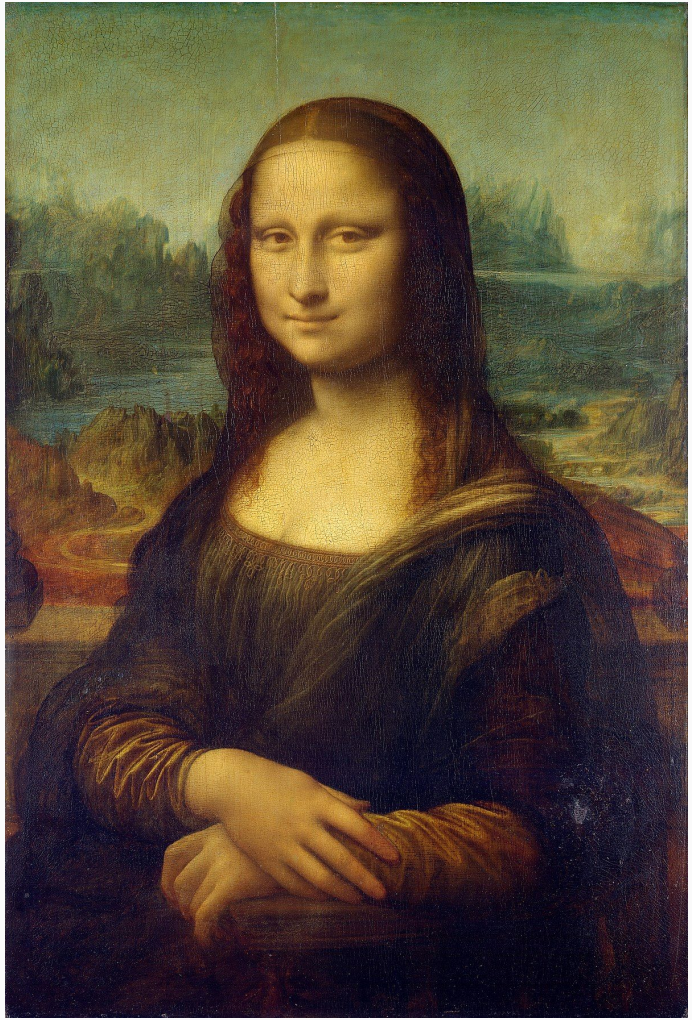
Digital assets can be pegged against real world assets, such as USD or CAD



DeFi

Offers lending, trading and investing without using centralized intermediaries, all run through code

4. Why digital assets matter



Valuable?

Shared belief in the system: Money

Livestock

The oldest form of money, livestock would be traded like currency between 9000 to 6000 BC

Tally sticks

Ancient memory aid device used to record and document transactions.

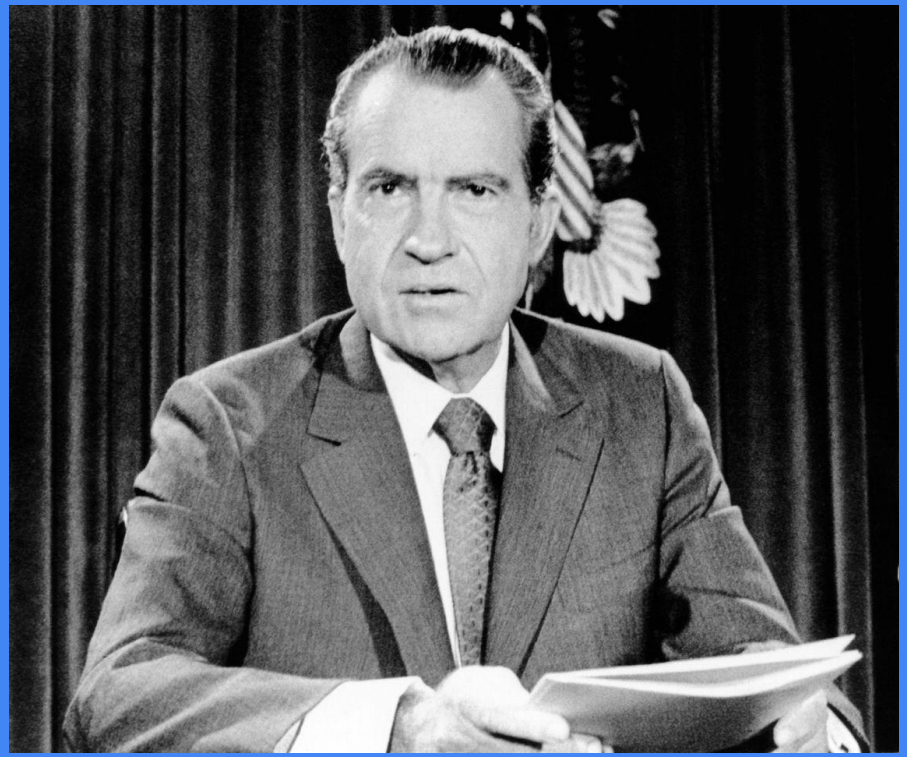
Shells

A common form of currency throughout history, Shells carry many characteristics befitting money – “durability, convenience, divisibility, as well as being easily identifiable.”

The Gold Standard

Within two years, most major currencies “floated,” rising and falling in value against one another based on market demand.

This still holds true today.



What is value?

Exchange

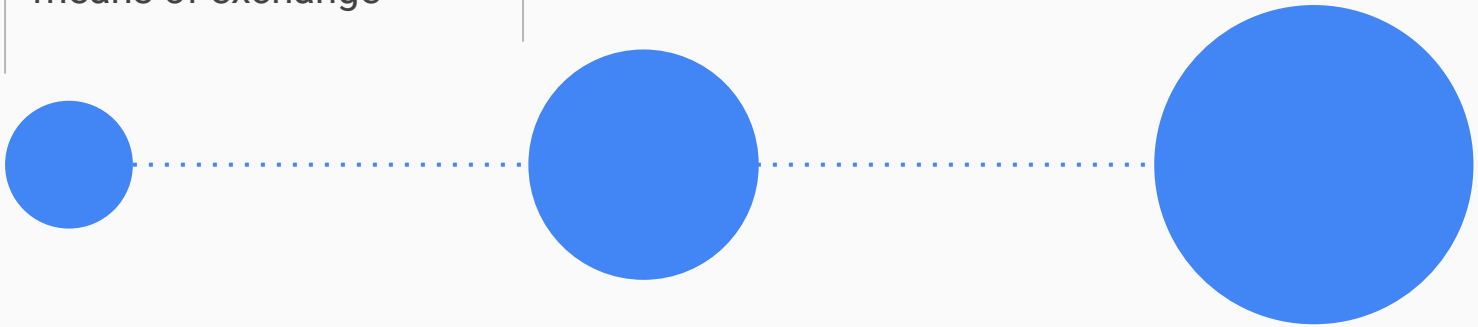
Method of payment and means of exchange

Wealth

Standard of value and store of wealth

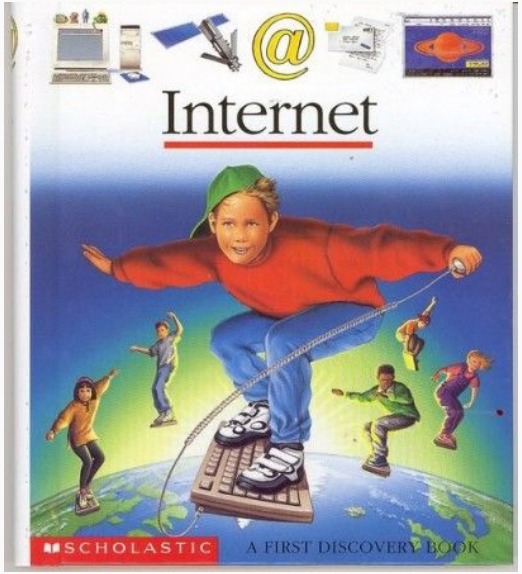
Account

Method of accounting for value



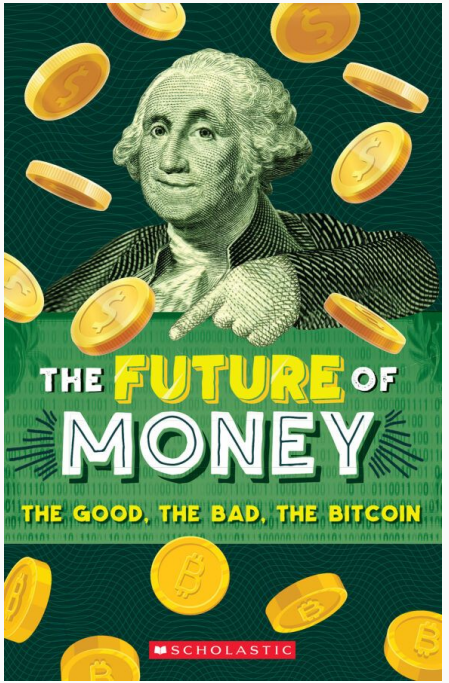
What the internet did for information…

- Can be created and shared instantly
- Accessible anywhere in the world
- Highly distributed
- No single point of failure
- Global network

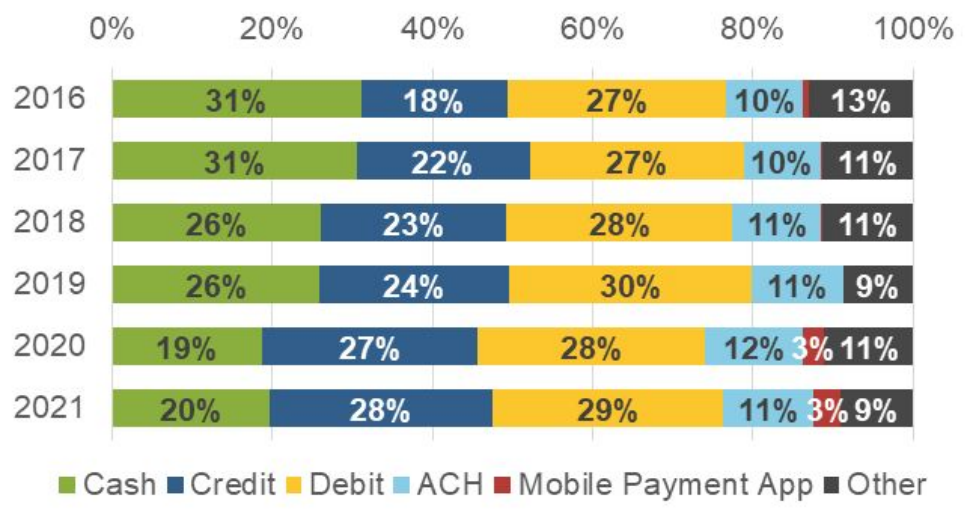


… cryptocurrency does for value

- Created and shared instantly
- Easy to transport and secure
- Accessible anywhere in the world
- Highly distributed
- No single point of failure
- Infinitely divisible



Money is trending towards digital



2022 Findings from the Diary of Consumer Payment Choice - Federal Reserve Bank of San Francisco

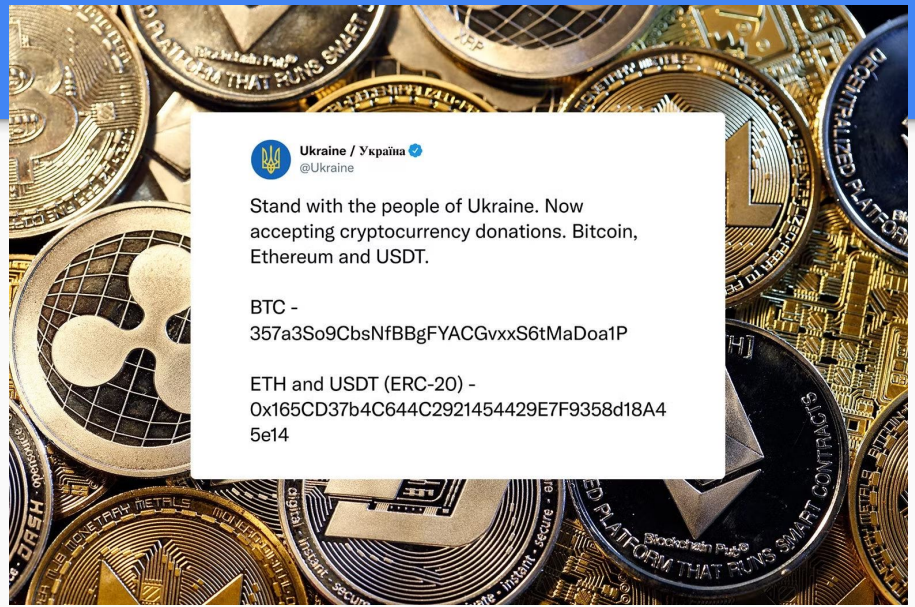
Uncontrollable money

Ire Aderinokun of the Feminist Coalition in Nigeria, explaining how the Coalition had their bank accounts frozen for protesting police violence, and how bitcoin was used to keep operating.

Uncontrollable money

Democracy activist Farida Bemba Nabourema, describing the difficulty for the Togolese diaspora to send money to friends and family back in Togo. The money is often seized in banks, so they often had to smuggle physical cash. Bitcoin simplifies their lives.

Uncontrollable money



Since Russia invaded on Feb. 24, more than 102,000 cryptoasset donations, totaling $54.7 million, went to the Ukrainian government in a matter of weeks.

The World's Top Remittance Recipients

Top 10 remittance-receiving countries in 2020* (billion U.S. dollars)

* expected

Source: KNOMAD via World Bank

In 2020, global remittances totaled roughly $700 billion, $540 billion of which is noted to have been sent to low- and middle-income countries, according to the World Bank.

Open Systems

Digital assets are limited to the video game or social media site

What’s powerful about crypto is the ability to plug into the open protocols, rather than being constrained by the limitations of the platform.

With social media today, when you share a file or a piece of media, you upload the file to the platform. But what's actually happening is your placing ownership of the file with the platform.

With many of these digital assets on the blockchain, they become accessible to anyone, anywhere.

Common Misconceptions

1. It’s a ponzi: Crypto’s sole use is speculation
2. Cryptocurrency is something you buy
3. Crypto is for money laundering
4. It’s unregulated
5. It’s bad for the environment

Takeaways

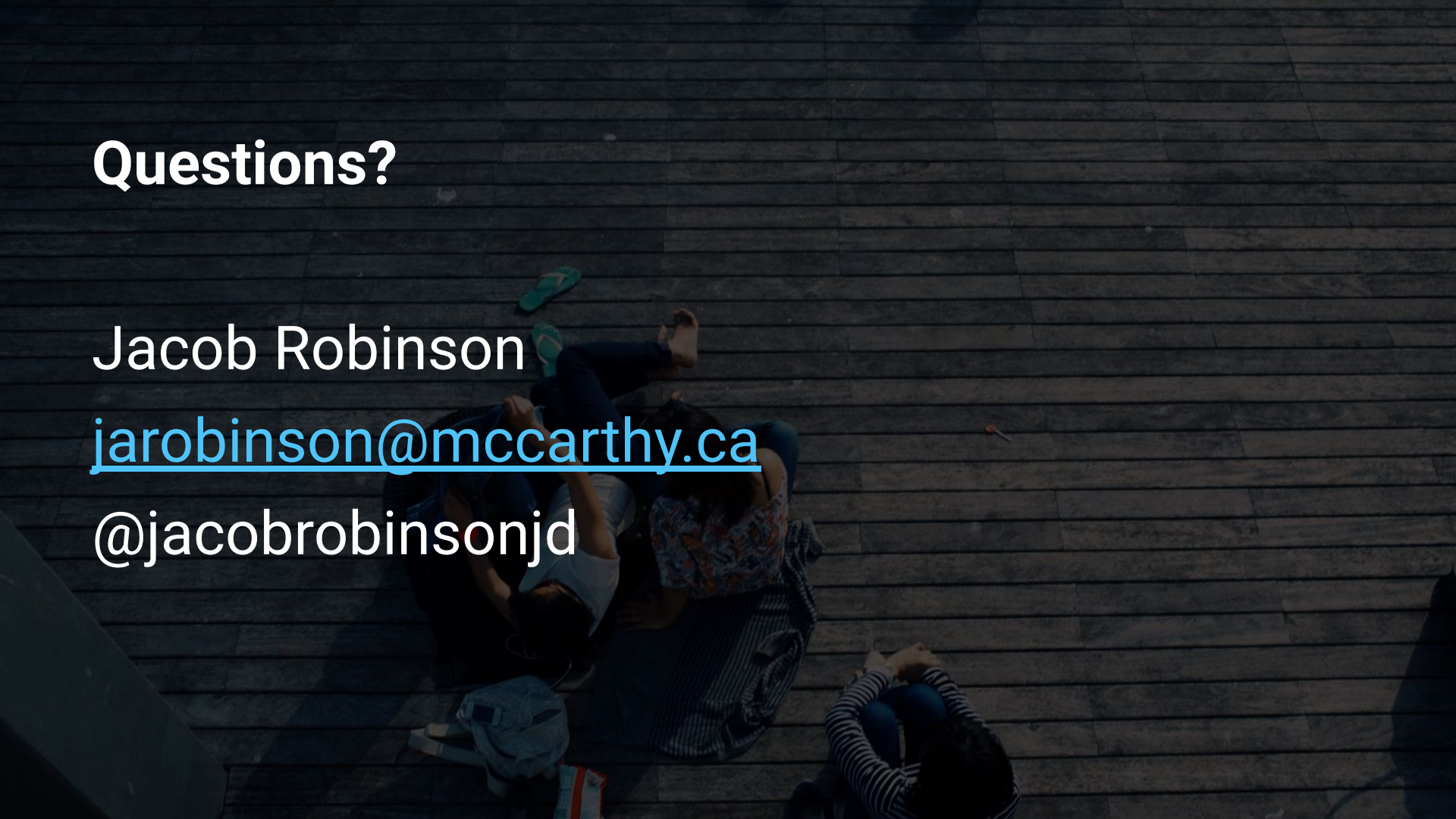
None of this was legal or investment advice.

My hope is that you take three things away from this presentation:

Cryptocurrencies are tools

Value is trending towards digital assets

Cryptocurrencies enable digital value



Questions?

Jacob Robinson
jarobinson@mccarthy.ca
@jacobrobinsonjd