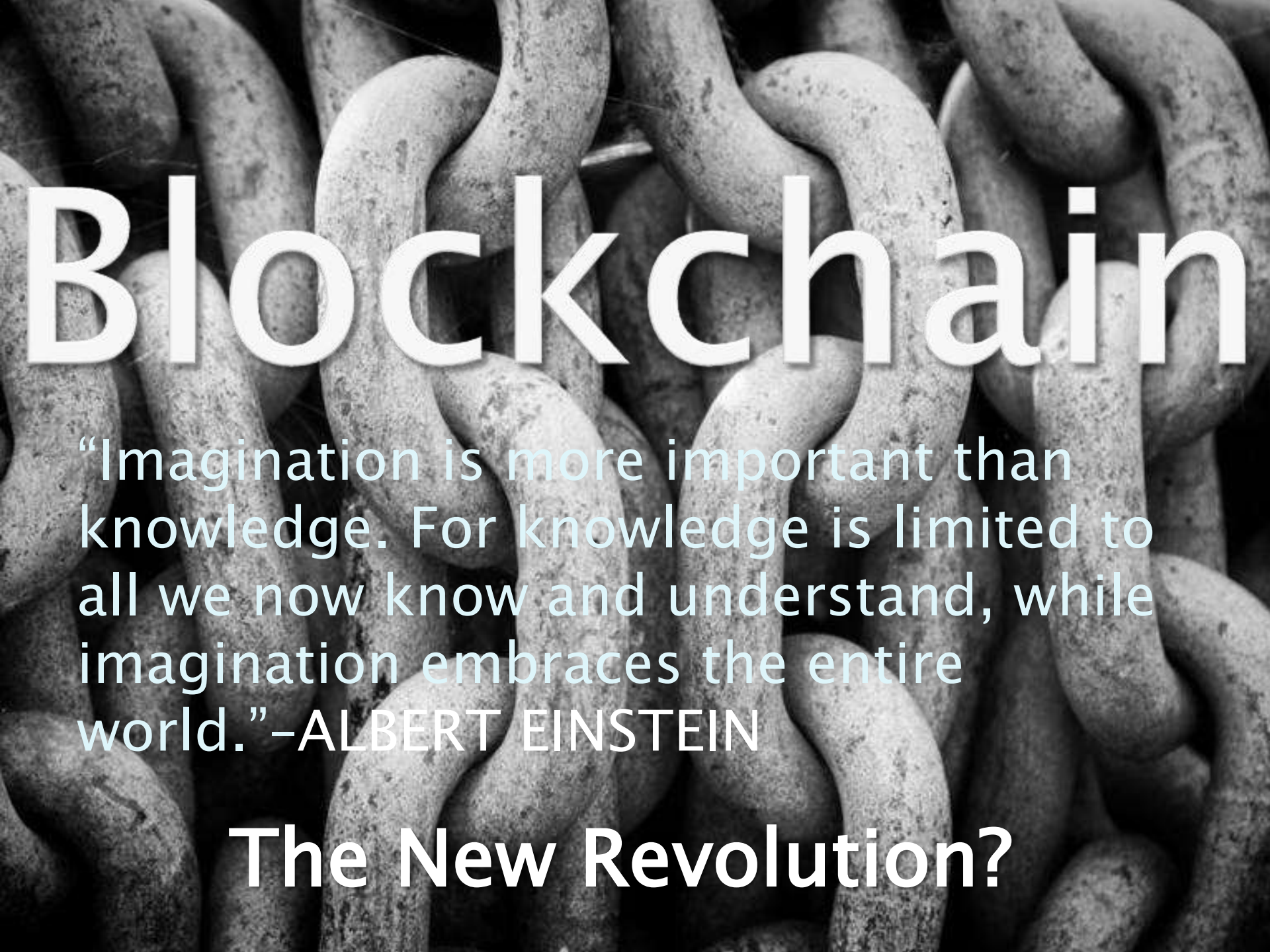
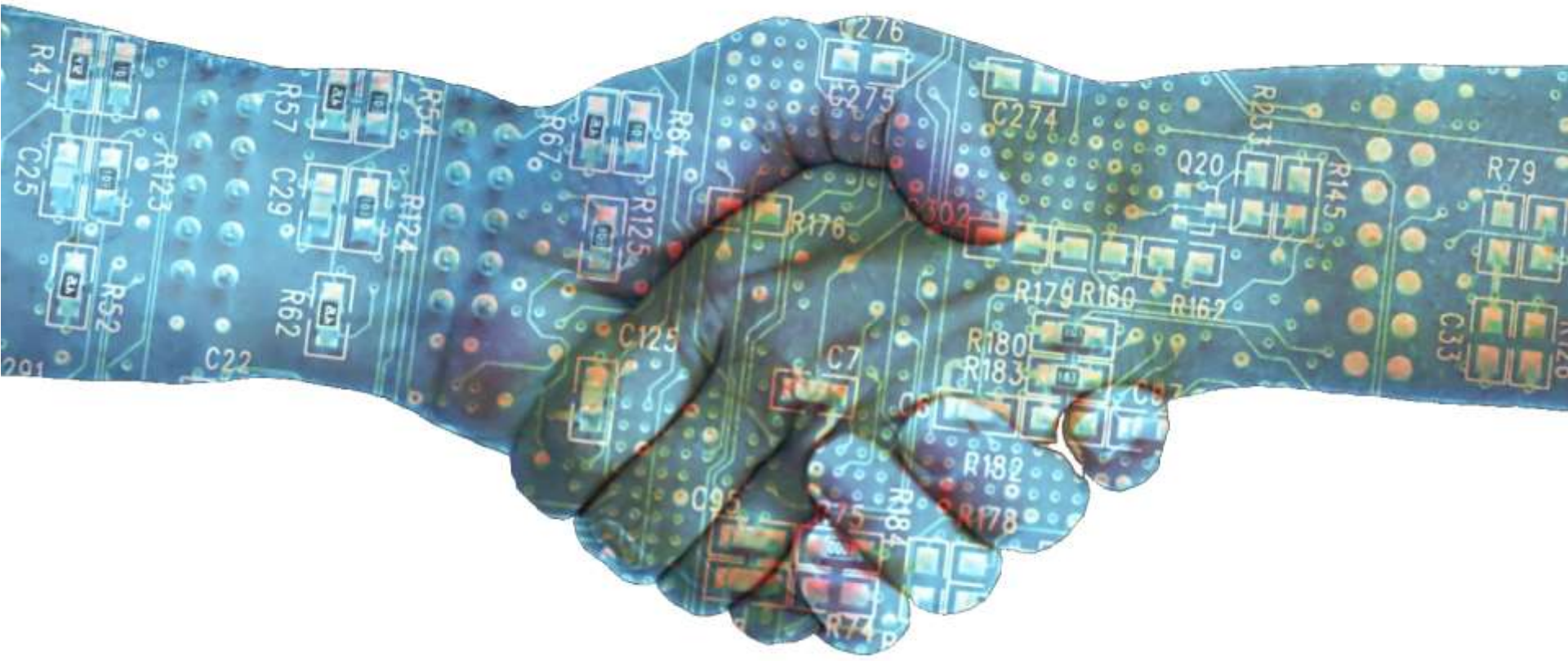

Blockchain
“Imagination is more important than knowledge. For knowledge is limited to all we now know and understand, while imagination embraces the entire world.”-ALBERT EINSTEIN
The New Revolution?

Agenda

- What is Blockchain?
- How It is Started
- How Blockchain Works
- How to Mine?
- Private vs Public Blockchains
- Cryptocurrencies
- Blockchain Use Cases
- Blockchain & Banking
- Getting on the Blockchain Bandwagon
- Q&A

What is Blockchain?



Understanding Blockchains

- Understanding blockchains is tricky. You need to **understand their message** before you can appreciate their potential. In addition to their **technological capabilities**, blockchains carry with them **philosophical**, **cultural**, and **ideological** underpinnings that must also be understood.

- In the same way that billions of people around the world are currently connected to the Web, millions, and then billions of people, will be connected to blockchains. **We should not be surprised if the velocity of blockchain usage propagation surpasses the historical Web users growth.**

Three Complementary Definitions of the Blockchain

- ***Technically***, the blockchain is a back-end database that maintains a distributed ledger that can be inspected openly.

- ***Business-wise***, the blockchain is an exchange network for moving transactions, value, assets between peers, without the assistance of intermediaries.

- ***Legally*** speaking, the blockchain validates transactions, replacing previously «trusted entities».

What is Blockchain?

- Blockchain ≠ Bitcoin
- Blockchain is the technology behind Bitcoin.
- Bitcoin is the digital token, and blockchain is the ledger that keeps track of who owns the digital tokens.
- You can't have Bitcoin without blockchain, but you can have blockchain without Bitcoin.
- It is a revolution bigger than internet!?
- Blockchain's affect is compared to WWW
- It may ruin banks!?
- A blockchain has technical, business and legal definitions.

What is Blockchain?

- Blockchains could not be without the Internet.
- The blockchain is a meta technology because it affects other technologies, and it is made up of several technologies itself
- it is comprised of several pieces: a database, a software application, a number of computers connected to each other, clients to access it, a software environment to develop on it, tools to monitor it, and other pieces.
- **No banks!, no government!, no intermediaries of any kind!. As you shall see, blockchain is a potentially revolutionary technology that promises to dramatically change the world as we know it.**

What is Blockchain?

*A blockchain is a **ledger of facts**, replicated across several computers assembled in a **peer-to-peer network**. Facts can be anything from monetary transactions to content signature. Members of the network are anonymous individuals called **nodes**. All communication inside the network takes advantage of **cryptography** to securely identify the sender and the receiver. When a node wants to add a fact to the ledger, a **consensus** forms in the network to determine where this fact should appear in the ledger; this consensus is called a **block**.*

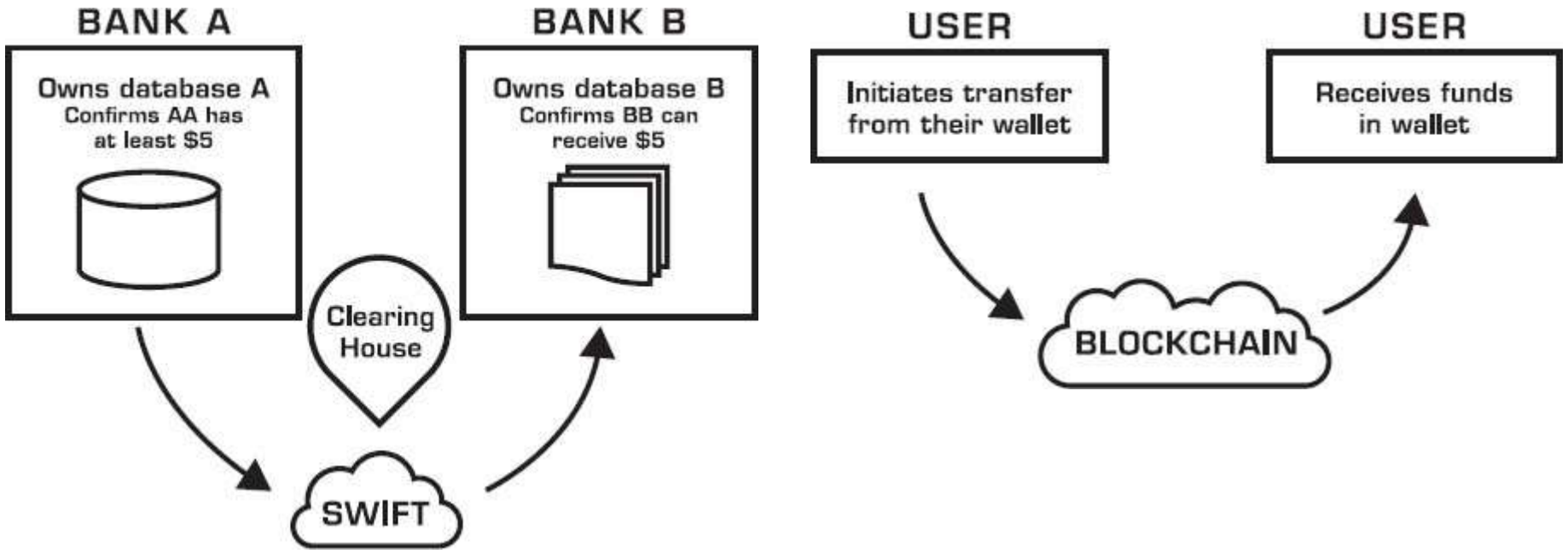
What is Blockchain?

People use the term ‘blockchain technology’ to mean different things, and it can be confusing. Sometimes they are talking about The Bitcoin Blockchain, sometimes it’s The Ethereum Blockchain, sometimes it’s other virtual currencies or digital tokens, sometimes it’s smart contracts. Most of the time though, they are talking about distributed ledgers, i.e. a list of transactions that is replicated across a number of computers, rather than being stored on a central server.

What is Blockchain?

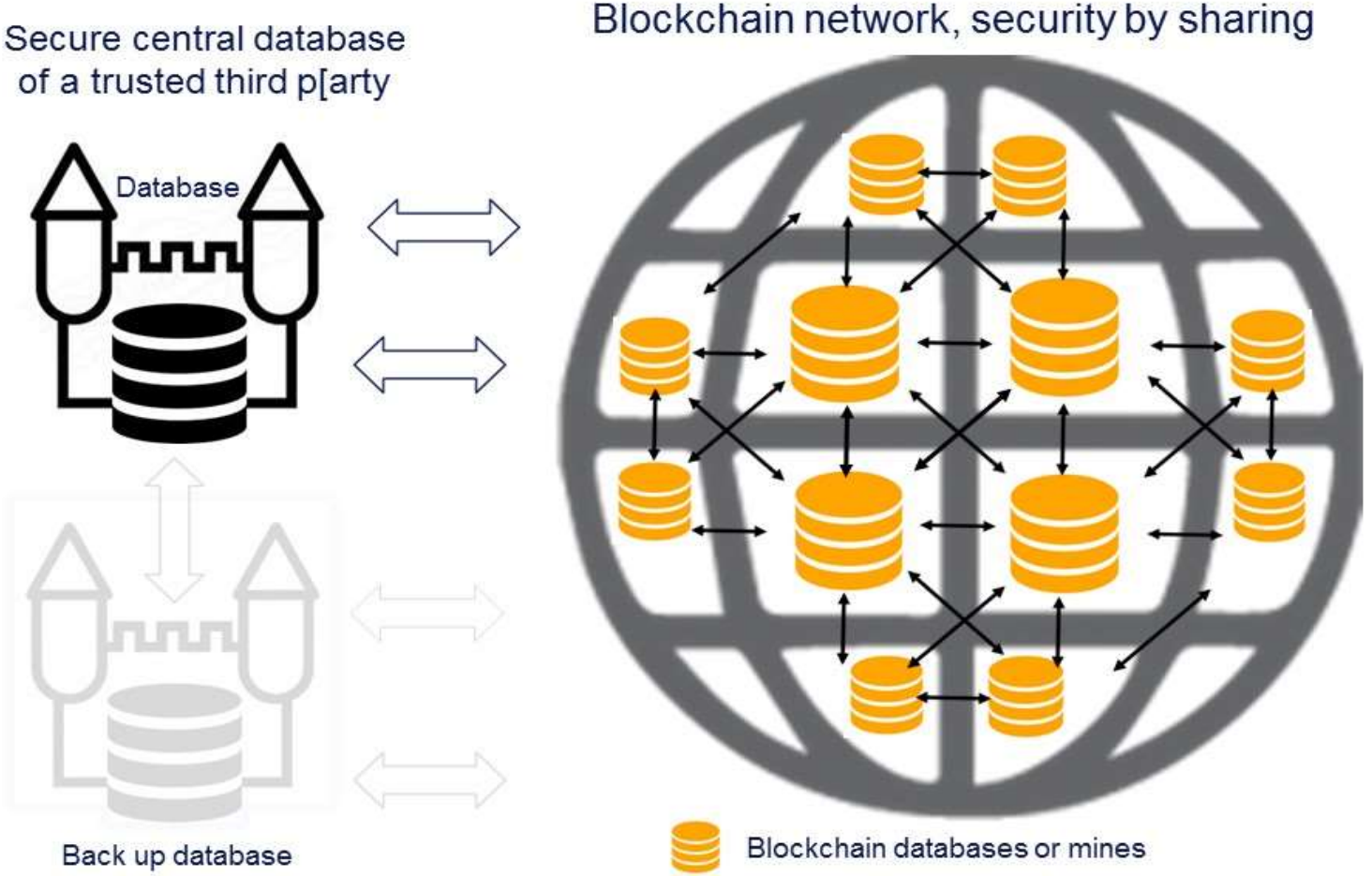
- A **blockchain**, at its simplest level, is just a **corruption-resistant string of ledger entries shared over a network by multiple parties**. Without defining it further, it can be difficult to imagine how useful one is; What exactly could it do now that we couldn't do with database technology like SQL before? Not much, really, and it would also be much slower than a SQL database. **All of the advantages derived from basic blockchain technology can be boiled down to only two benefits; corruption resistance and redundancy.**
- All blockchains have this basic list of pros and cons, but depending on how they are implemented, the benefits could easily be minimized. For instance, if you deploy too few nodes then your network won't be very redundant afterall. The list of advantages and drawbacks grows from there when choosing to deploy either a **public or private blockchain.**

THE DATABASE VS. THE LEDGER

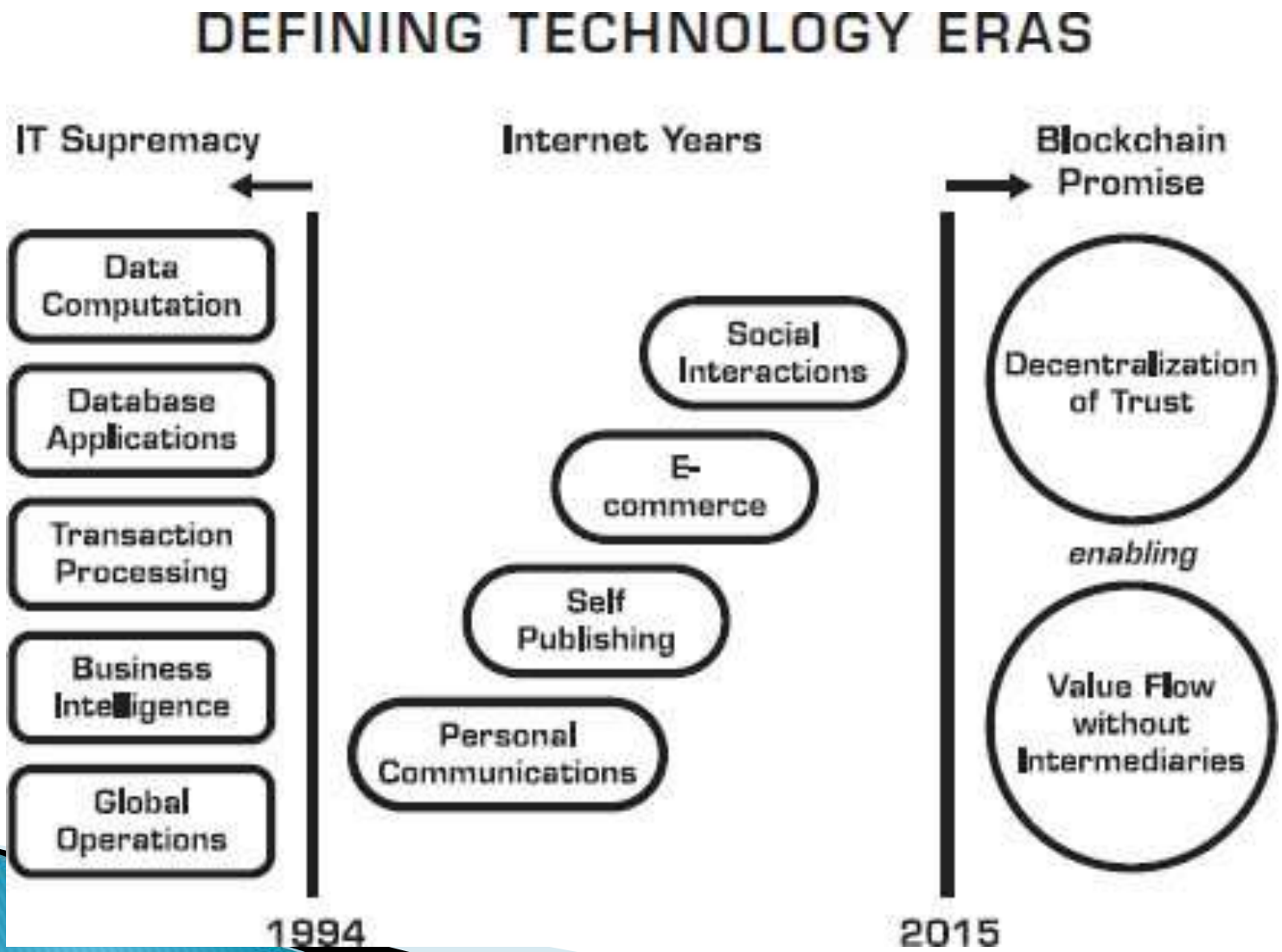


in a blockchain network the data is stored on many computers (the so-called 'miners')

Database vs Blockchain data storage

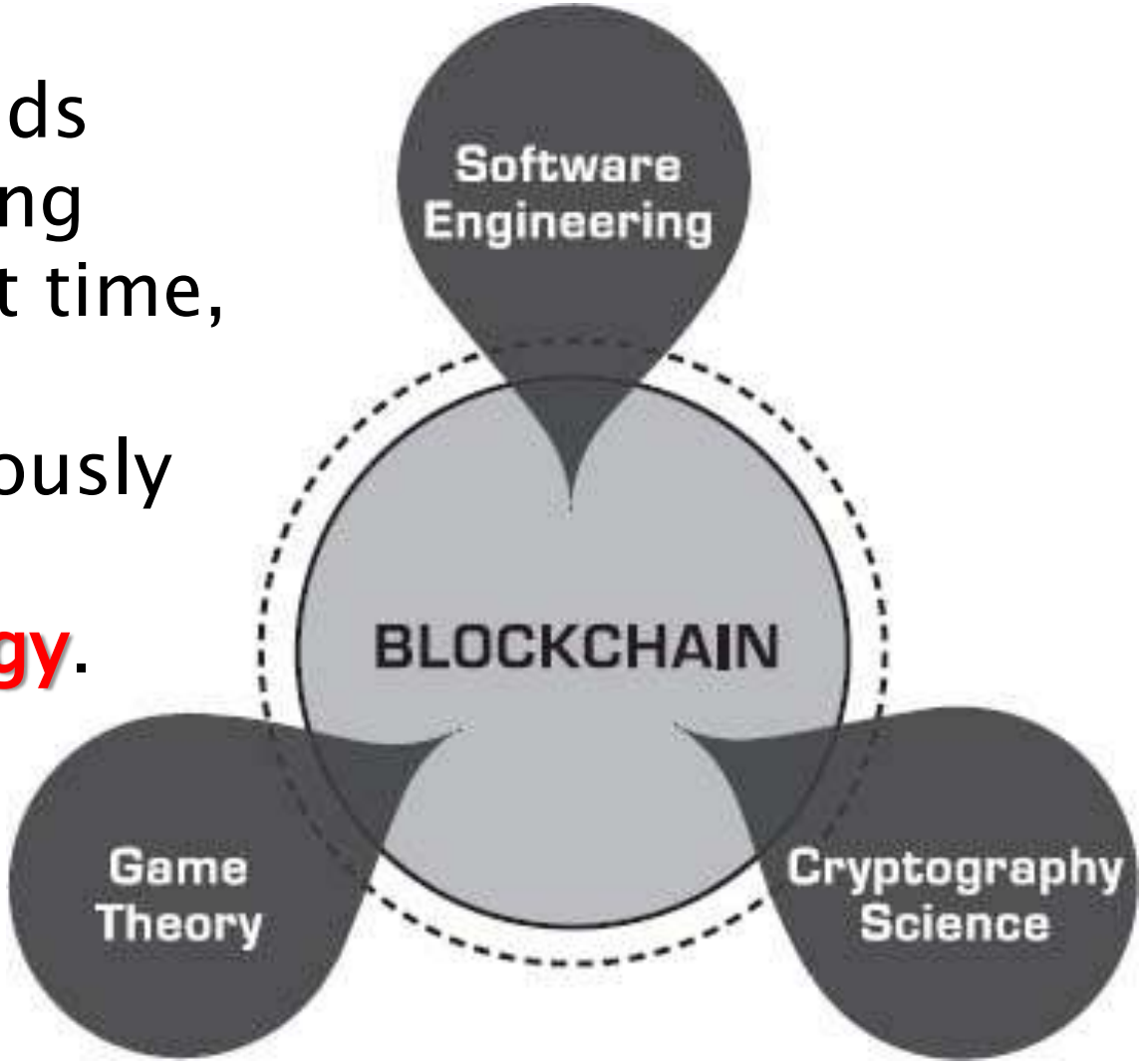


Where does the Blockchain Fit in the Technology Evolution?



SOFTWARE, GAME THEORY AND CRYPTOGRAPHY

Separately, these fields have existed for a long time, but for the first time, they have together intersected harmoniously and morphed inside **blockchain technology**.



Game Theory

- Game theory is 'the study of mathematical models of conflict and cooperation between intelligent rational decision-makers." And this is related to the blockchain because the **Bitcoin blockchain**, originally conceived by Satoshi Nakamoto, **had to solve a known game theory conundrum** called **the Byzantine Generals Problem.**

Byzantine General's Problem

- Several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals **can communicate with one another only by messenger**. **They must decide upon a common plan of action**. However, **some of the generals may be traitors,** trying to prevent the loyal generals from reaching agreement. **The generals must have an algorithm to guarantee that.**

- A. **All loyal generals decide upon the same plan of action.**
- **The loyal generals will all do what the algorithm says they should**, but **the traitors may do anything they wish**. **The algorithm must guarantee condition A regardless of what the traitors do**. The loyal generals need to reach agreement and agree on a reasonable plan that also insures that.
- B. **A small number of traitors cannot cause the loyal generals to adopt a bad plan.**

Byzantine General's Problem

Byzantine Generals Problem, Byzantine Fault Tolerance (BFT), Byzantine Agreement (BA)

- Distributed network security problem
- Problem: achieving consensus in a distributed network with potentially faulty nodes; how to coordinate among distributed nodes to come up with a consensus (common view of the world) that is resistant to attackers trying to undermine that consensus
- Important consensus system properties in a distributed system or distributed algorithm
  - Safety: require that "something bad will never happen"
  - Liveness: require that "something good will eventually happen," the system makes progress (example: eventual consistency)

Byzantine General's Problem

Approaches to Consensus/BFT

- Byzantine Agreement Protocol (synchronous)
  - Microsoft/Lamport: Paxos (state machine replication)
  - Google: Chubby (serve strongly consistent files)

- POW (Bitcoin) 'Nakamoto Consensus' – expensive, high latency
- POS (Tendermint) – requires resource ownership, risk of 'nothing-at-stake' attacks per revoked escrow

- Pebble: ARBC (Asynchronous Randomized Byzantine Consensus)
- UT: BAR (Byzantine, altruistic, rational) protocol
- Stellar: SCP Quorum Slicing
- Other: Prediction Markets (Augur), Meta (Factom)

Cryptography Science

Cryptography science is used in multiple places to provide security for a blockchain network, and it rests on three basic concepts: **hashing**, **keys**, and **digital signatures**.

Software

Although the **concepts of cryptography** have been around for a while, **software engineers** are feasting on **combining it with game theory innovation**, to produce the **overall constructs of blockchains**, where seeming uncertainty is mitigated with overwhelming mathematical certainty.

Blockchain Exhibits Simultaneously the Following Ten Properties:

1. Cryptocurrency
2. Computing Infrastructure
3. Transaction Platform
4. Decentralized Database
5. Distributed Accounting Ledger
6. Development Platform
7. Open Source Software
8. Financial Services Marketplace
9. Peer-to-Peer Network
10. Trust Services Layer

Web and Blockchain Analogy

- **There are many analogies** between **the Web's early years** and today's **blockchain's evolution**, in terms of how the technology will be adopted.

- Let us not forget that **it took about three years for most companies to fully understand the Web's potential (1994–1997 roughly),** after its initial commercialization, and **it took seven years after the Internet's 1983 launch for the Web to come into play**. **There is no doubt the blockchain will remain a semi-mysterious, semi-complex phenomena for the period 2015–2018, just as it took Bitcoin three quiet years (2009–2012) before it became more visibly known to the general public.**

Web and Blockchain Analogy

Parallels to the internet

Blockchains today have been likened to the Internet in 90s.

- ➔ Similar investment levels
- ➔ Similar excitement levels
- ➔ Similar visions of potential uses

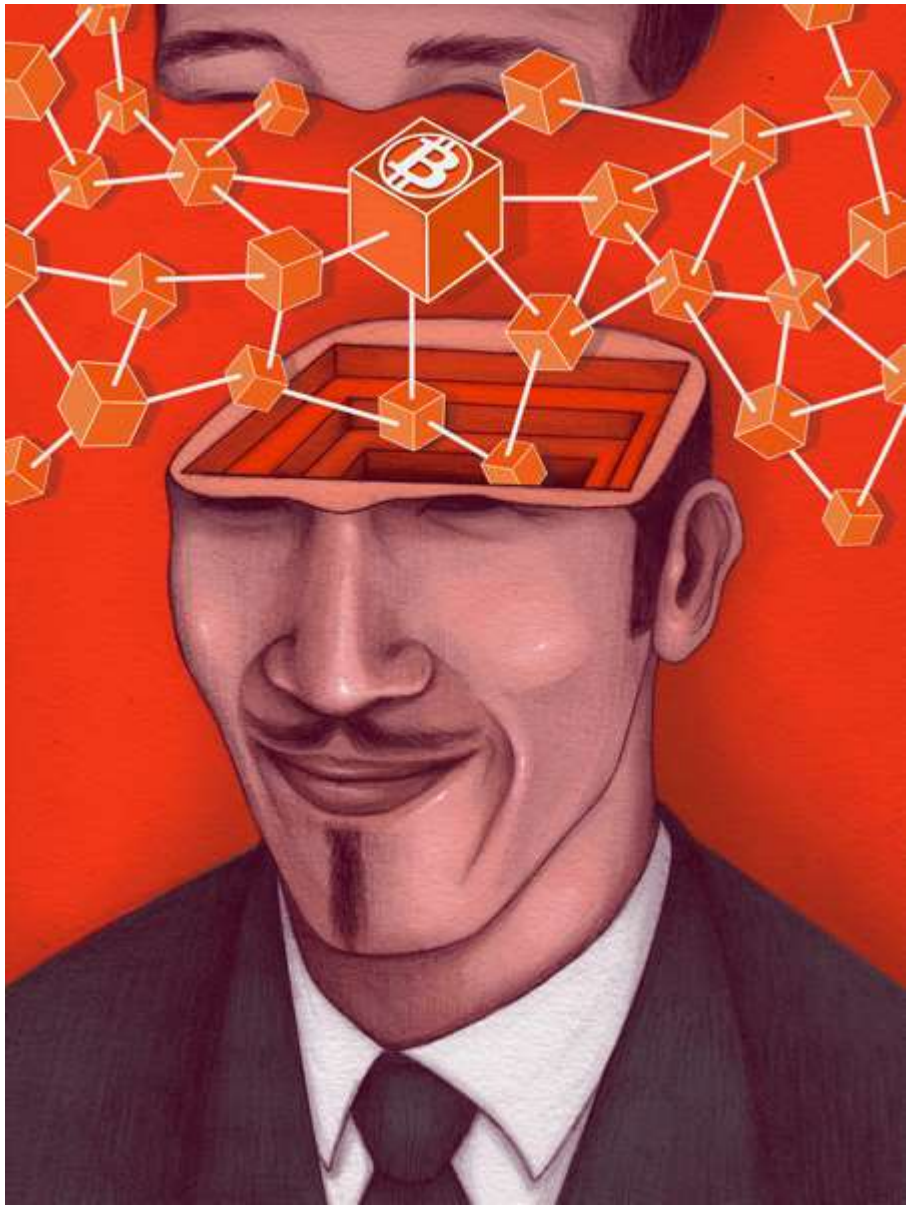
History doesn't repeat, but it rhymes: We expect similar...

- ➔ Similar path to maturity – people, tools, process
- ➔ Similar adoption curve (perhaps faster)
- ➔ Evolution of protocol/services built on blockchains (perhaps faster)

Tip

I know, all these definitions mean nothing at this moment, but don't worry, as we go into more detail, you shall feel more comfortable with it. It is not an easy topic, nor it is mature enough.

How It is Started



How It is Started?

- White paper published November 2008 by Satoshi Nakamoto
- «Bitcoin: A Peer-to-Peer Electronic Cash System»
- Working implementation published 3 months later as an open source project.

It All Begins With Satoshi Nakamoto's Paper

Bitcoin: A Peer-to-Peer Electronic Cash System

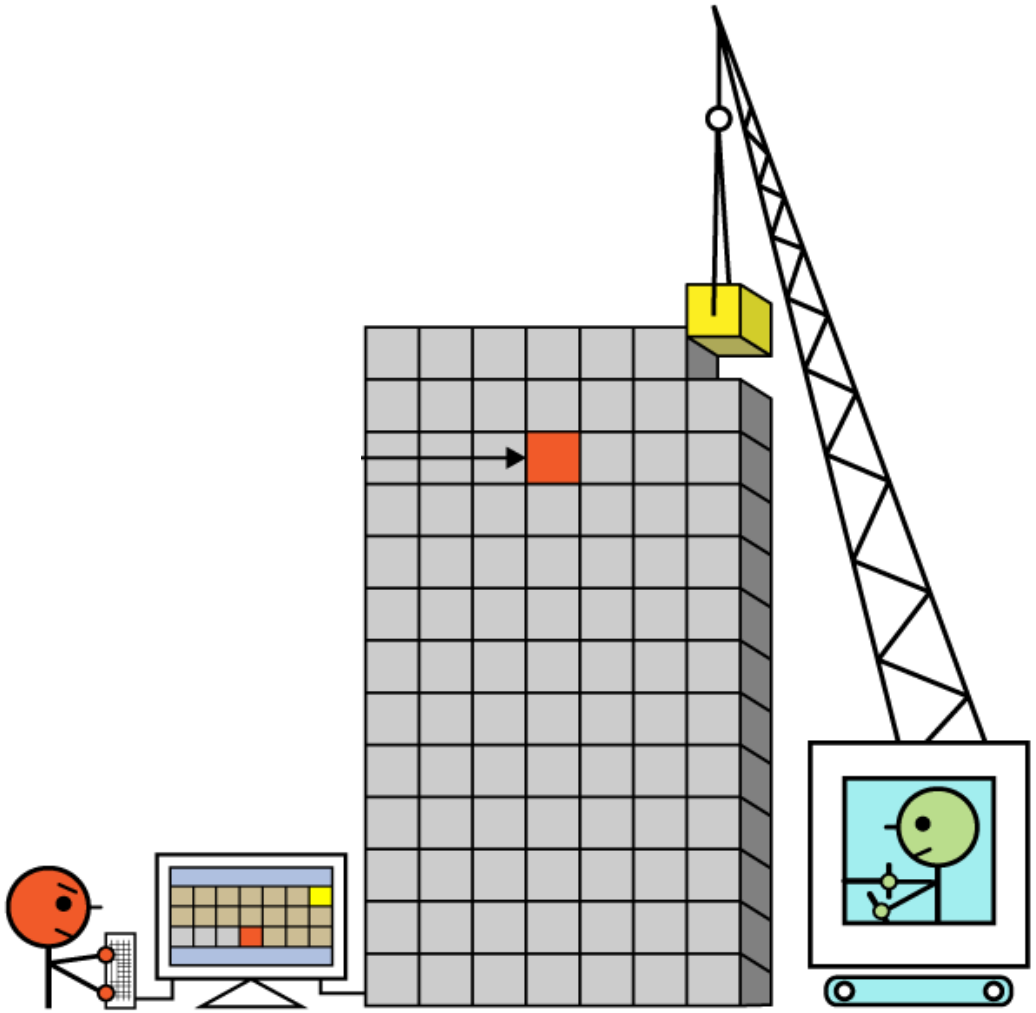
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

Satoshi Makes The Following Statements in His/Her/Their Paper

- Peer-to-peer electronic transactions and interactions
- Without financial institutions
- Cryptographic proof instead of central trust
- Put trust in the network instead of in a central institution

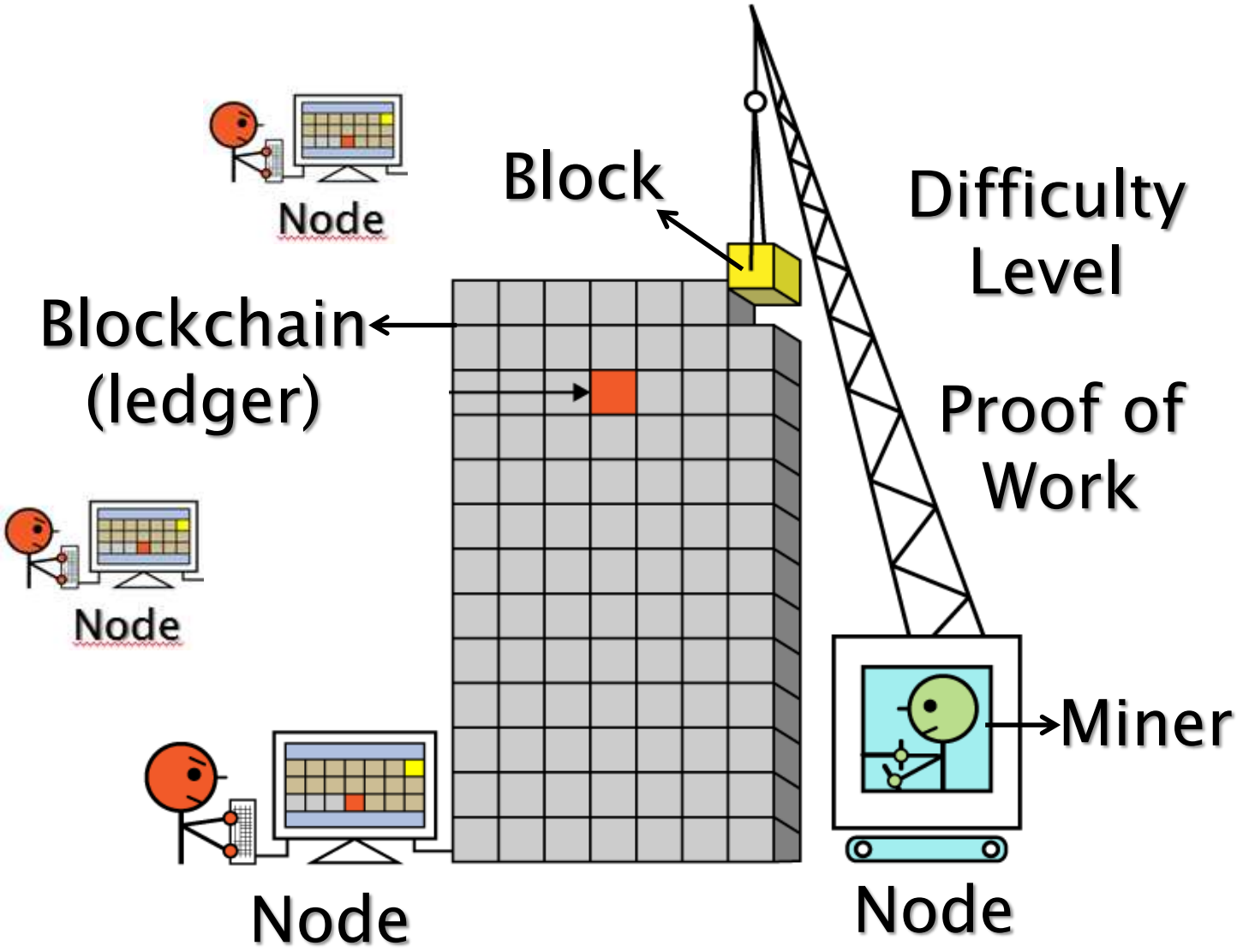
How Blockchain Works



Elements of Blockchain

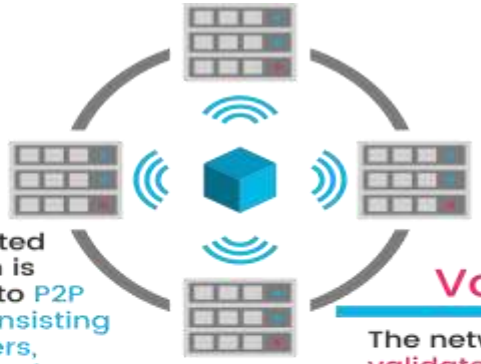
- Nodes
- Miners
- Ledger (Block/Blockchain)
- Proof of work
- Network consensus
- Difficulty Level
- Double Spending Problem

How Blockchain Works

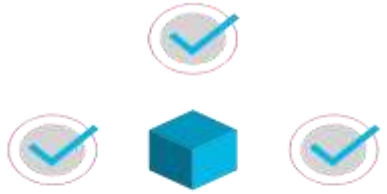


How it works:

Someone requests a transaction.



The requested transaction is broadcast to P2P network consisting of computers, known as nodes.



Validation

The network of nodes validates the transaction and the user's status using known algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.

Has no intrinsic value in that it is not redeemable for another commodity, such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

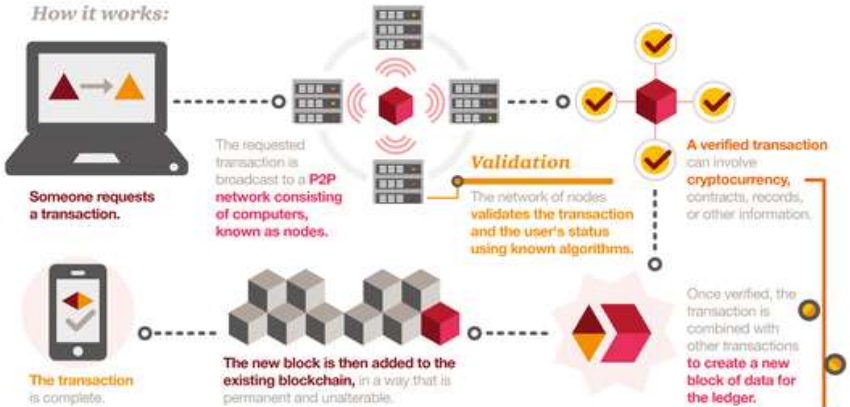
Blockgeeks

A look at blockchain technology

What is it?

The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting, and many other uses.

How it works:



Someone requests a transaction.

The requested transaction is broadcast to a **P2P network consisting of computers, known as nodes.**

Validation

The network of nodes **validates the transaction and the user's status using known algorithms.**

A verified transaction can involve **cryptocurrency,** contracts, records, or other information.

Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

The transaction is complete.

Benefits

- Increased transparency
- Accurate tracking
- Permanent ledger
- Cost reduction

Unknowns

- Complex technology
- Regulatory implications
- Implementation challenges
- Competing platforms

Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.

Has no intrinsic value in that it is not redeemable for another commodity, such as gold.

Has no physical form and exists only in the network.

Its supply is not determined by a central bank and the network is completely decentralized.

Potential applications

Automotive

Consumers could use the blockchain to manage fractional ownership in autonomous cars.

Financial services

Faster, cheaper settlements could shave billions of dollars from transaction costs while improving transparency.

Voting

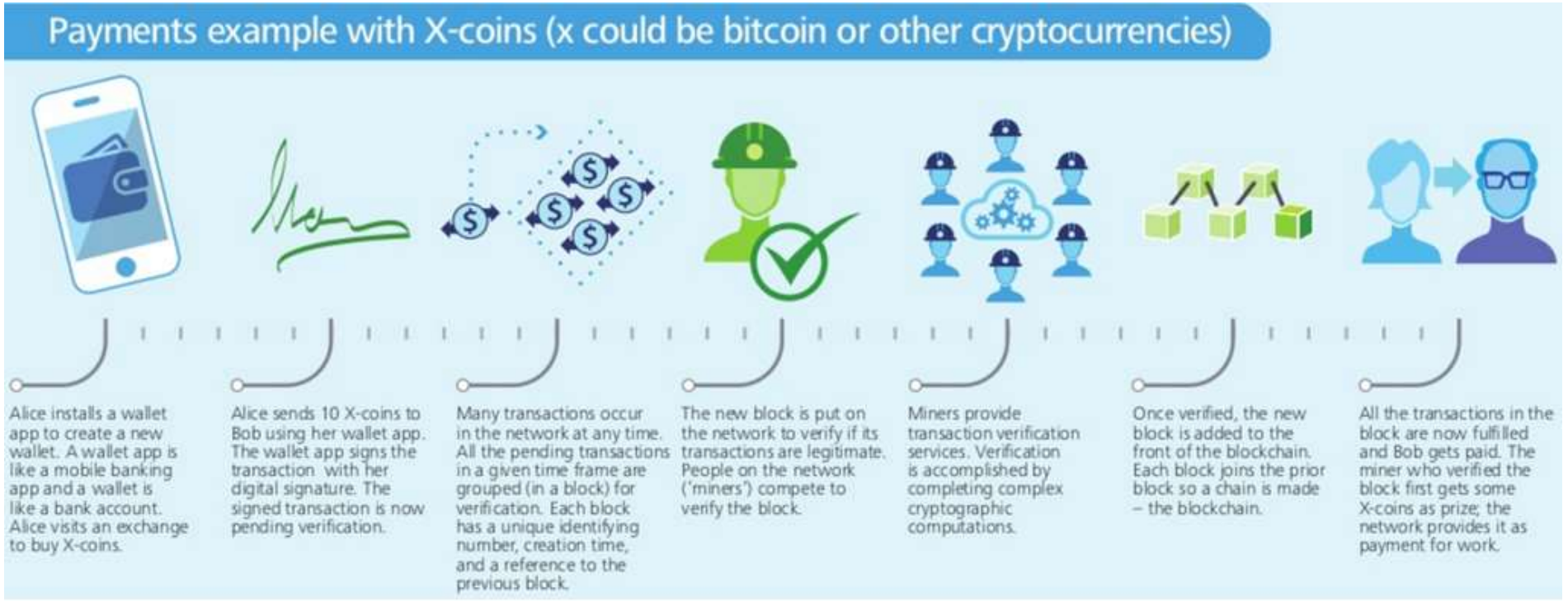
Using a blockchain code, constituents could cast votes via smartphone, tablet or computer, **resulting in immediately verifiable results.**

Healthcare

Patients' encrypted health information could be shared with multiple providers without the risk of privacy breaches.

pwc

How Blockchain Works



How Blockchain Works?

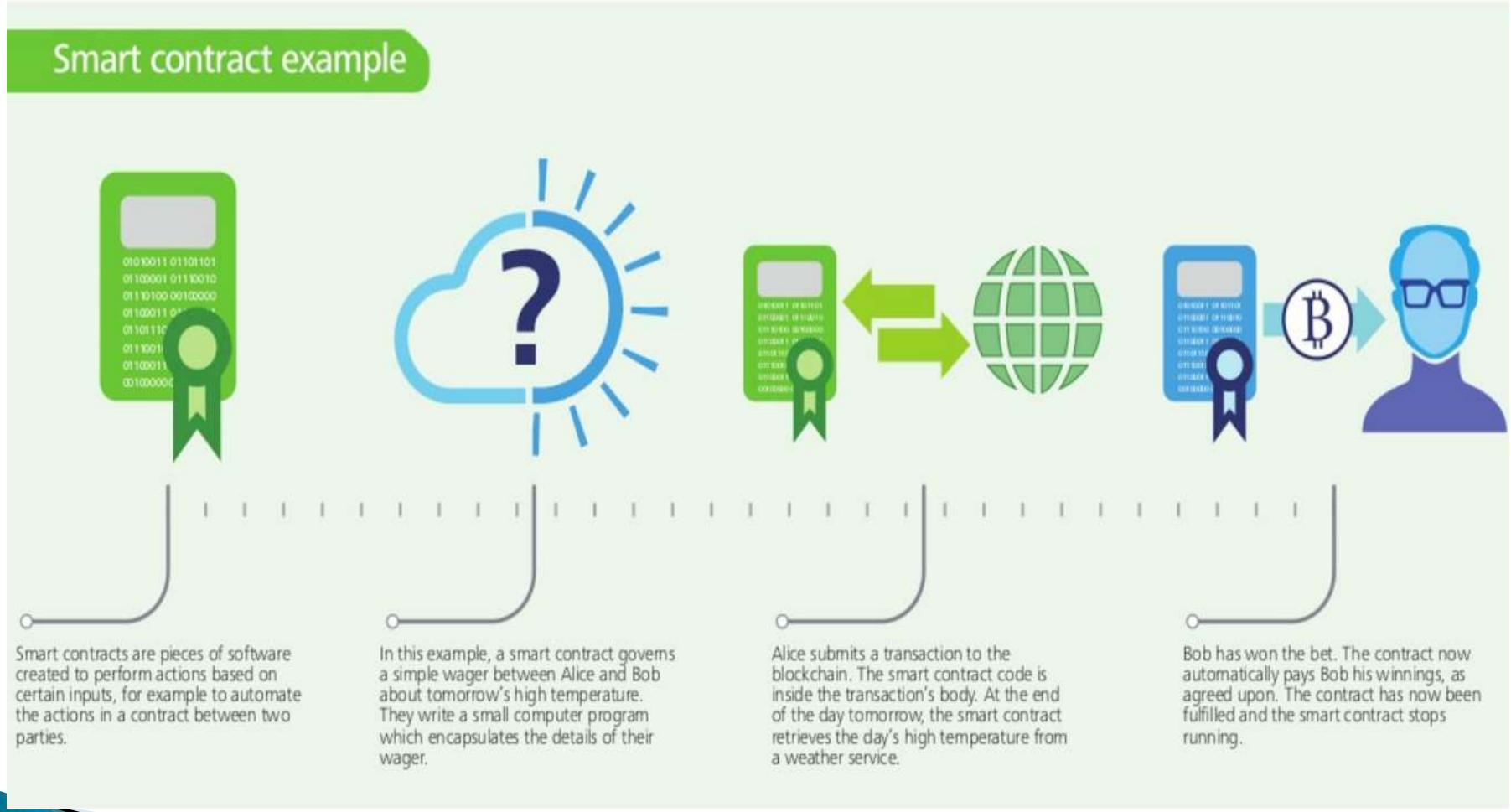
Asset registry example

Tokens or coins on the blockchain can be used to represent an asset's value digitally. Their value is tied to a real-world promise by the asset issuer. Such tokens are mostly used with digital assets; in this example, a digital image.

The image is not stored on the blockchain. The image's token that contains a reference to the image's ownership deed is stored on blockchain. Once put on the blockchain, everyone in the network agrees on who the asset belongs to.

Alice has a digital picture that she wants to sell using a token. This token permanently stores Alice's ownership of the picture. This token can now be freely traded by sending it to someone else. Bob buys the picture and Alice sends Bob the token. Bob now owns the picture.

How Blockchain Works?



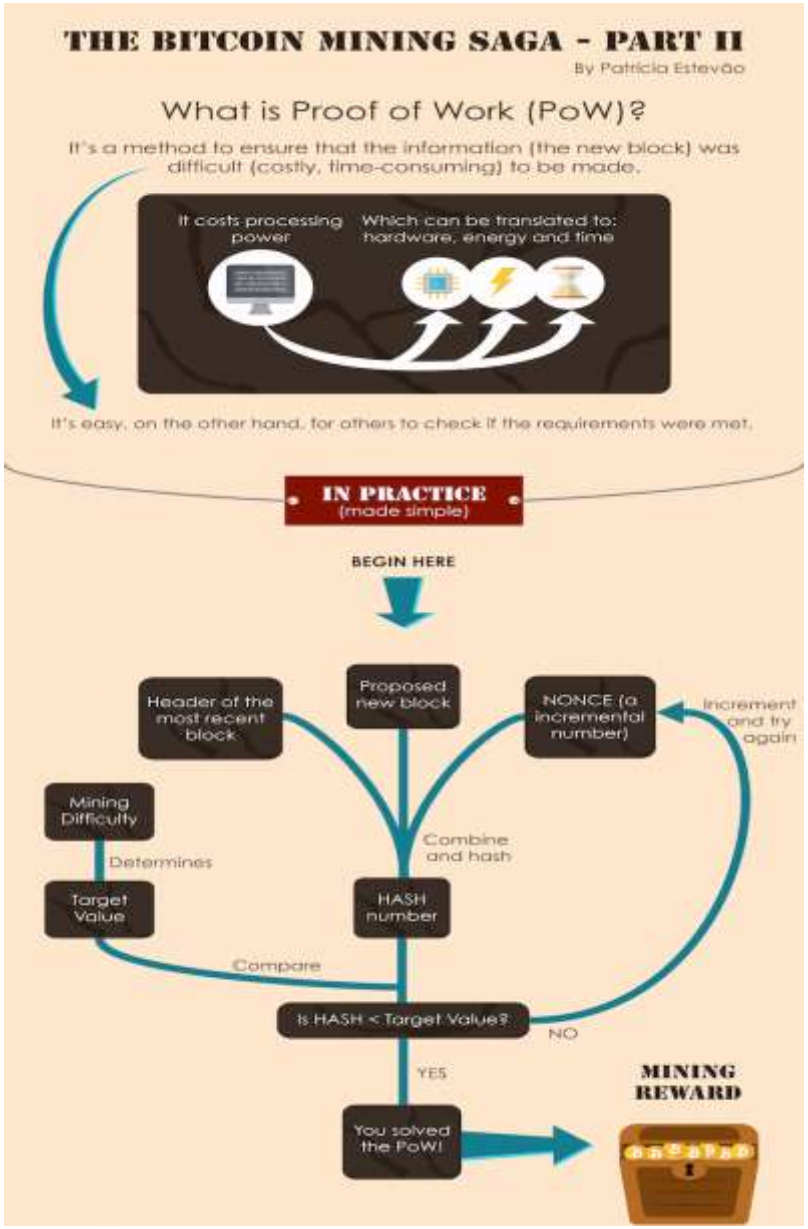
Mining & Proof of Work

What is Mining?

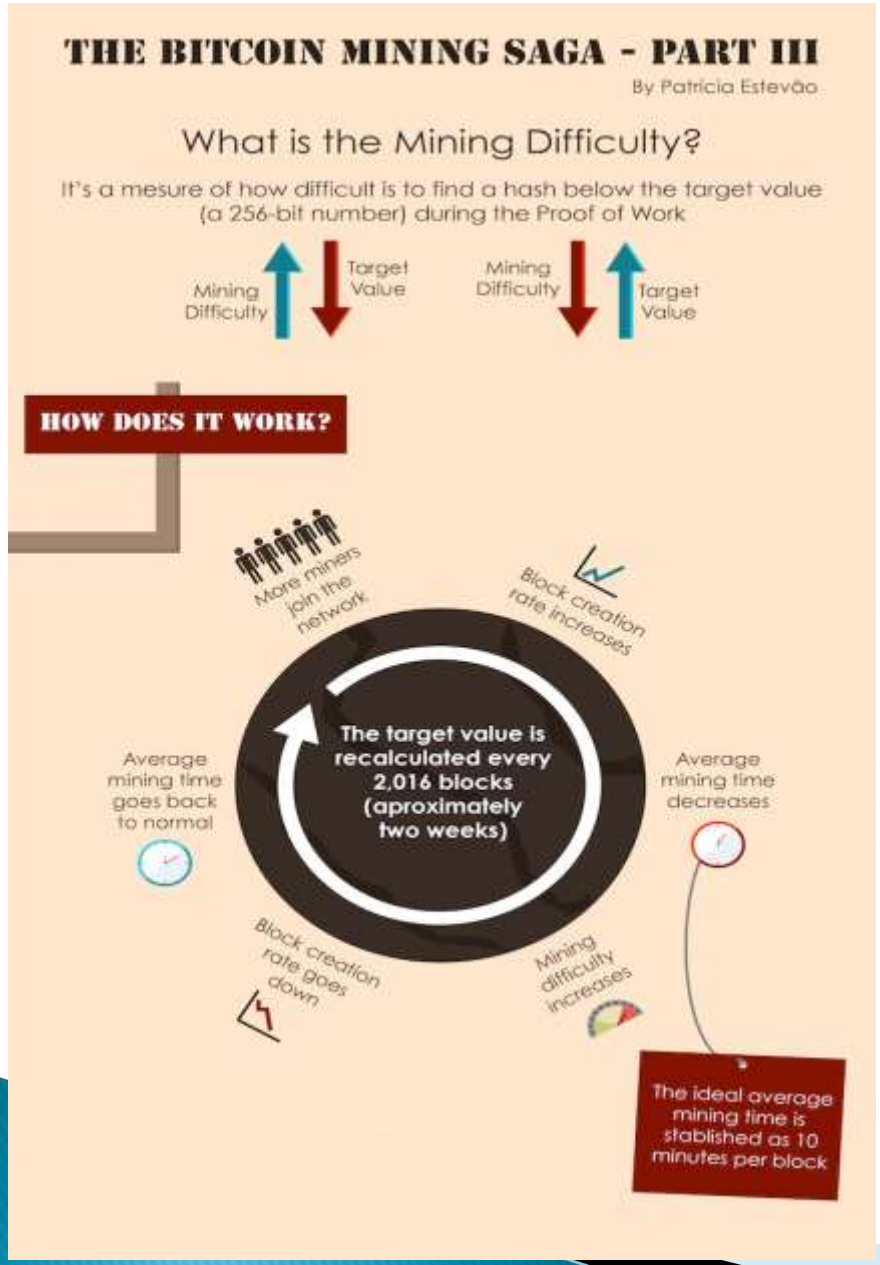
- Bitcoin mining is a lot **like a giant lottery** where you compete with your mining hardware with everyone on the network to earn bitcoins.
- In the big picture, **Bitcoin mining secures transactions that are recorded in Bitcon's public ledger, the block chain**.
- By conducting a random lottery where electricity and specialized equipment are the price of admission, the cost to disrupt the Bitcoin network scales with the amount of hashing power that is being spent by all mining participants.

How to Mine?


THE BITCOIN MINING SAGA - PART I
By Patrícia Estevão
What is Bitcoin Mining?
It's a decentralized computational process that serves 2 purposes:
1.
Confirms transactions in a trustful manner when enough computational power (effort) is devoted to a block
2.
Creates (issues) new bitcoins in each block
IT GOES LIKE THIS:
Bundle transactions in a block
Verify if transactions are valid
Select the header of the most recent block and insert it into the new block as a hash
When the solution is found, the new block is added to the local blockchain and propagated to the network
Solve the Proof of Work problem


THE BITCOIN MINING SAGA - PART II
By Patrícia Estevão
What is Proof of Work (PoW)?
It's a method to ensure that the information (the new block) was difficult (costly, time-consuming) to be made.
It costs processing power
Which can be translated to: hardware, energy and time
It's easy, on the other hand, for others to check if the requirements were met.
IN PRACTICE
(made simple)
BEGIN HERE
Header of the most recent block
Proposed new block
NONCE (a incremental number)
Increment and try again
Mining Difficulty
Determines
Target Value
Combine and hash
HASH number
Compare
Is HASH < Target Value?
NO
YES
You solved the PoW!
MINING REWARD

How to Mine – Mining Difficulty



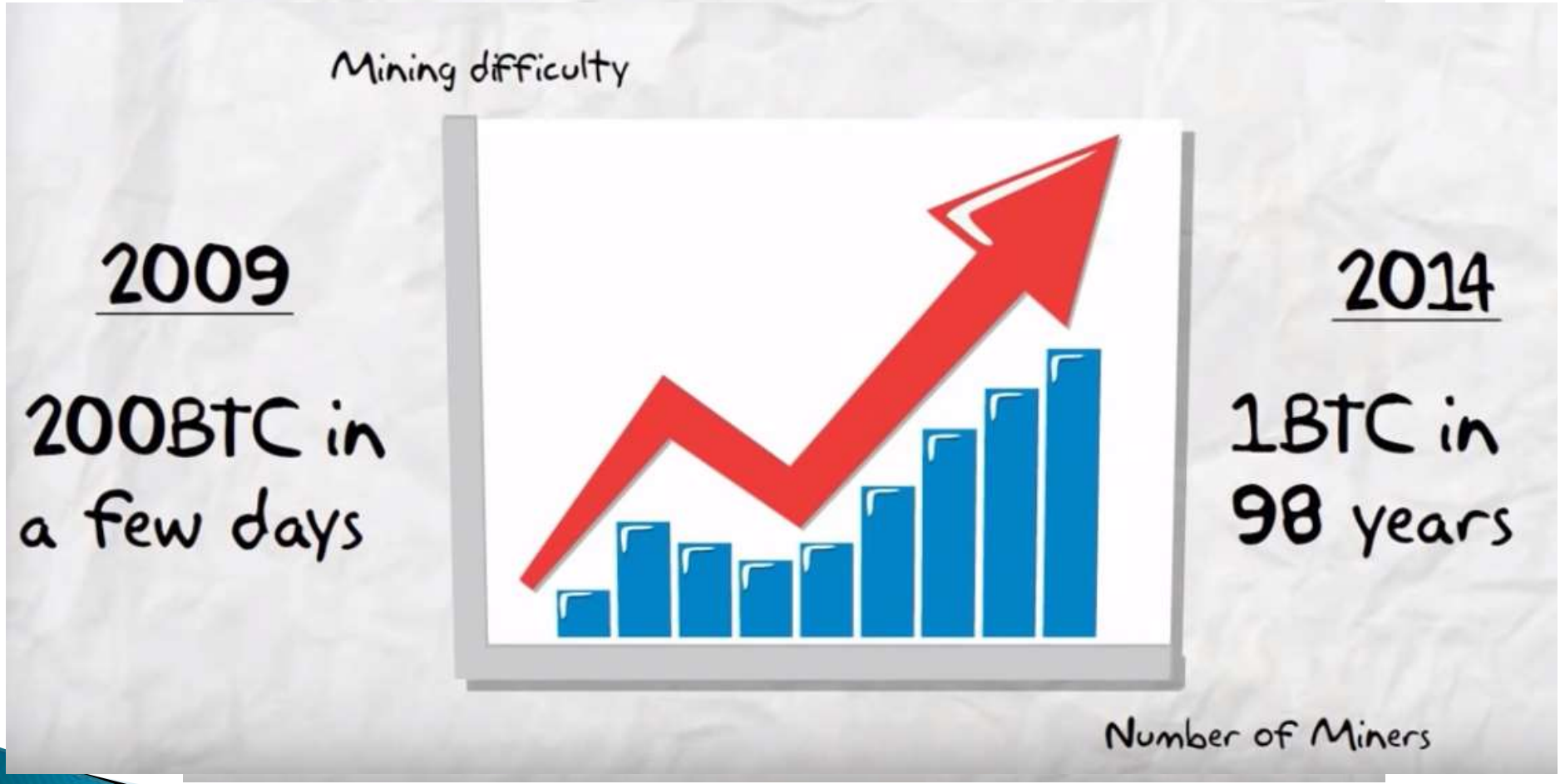
Miners get paid for:

Verifying transactions

Mining Bitcoins

More miners = Reliable & more secure network

Mining Difficulty



Transaction Verification

Transaction Relaying

- Receive transaction from peer
- Verification (simplified):
  - Verify that the signatures are sound
  - Verify that the inputs are unspent
  - Verify that the sum of outputs <= sum of inputs
- Relay transaction to other peers

The Merkle Tree

Making a hash of it

INPUT

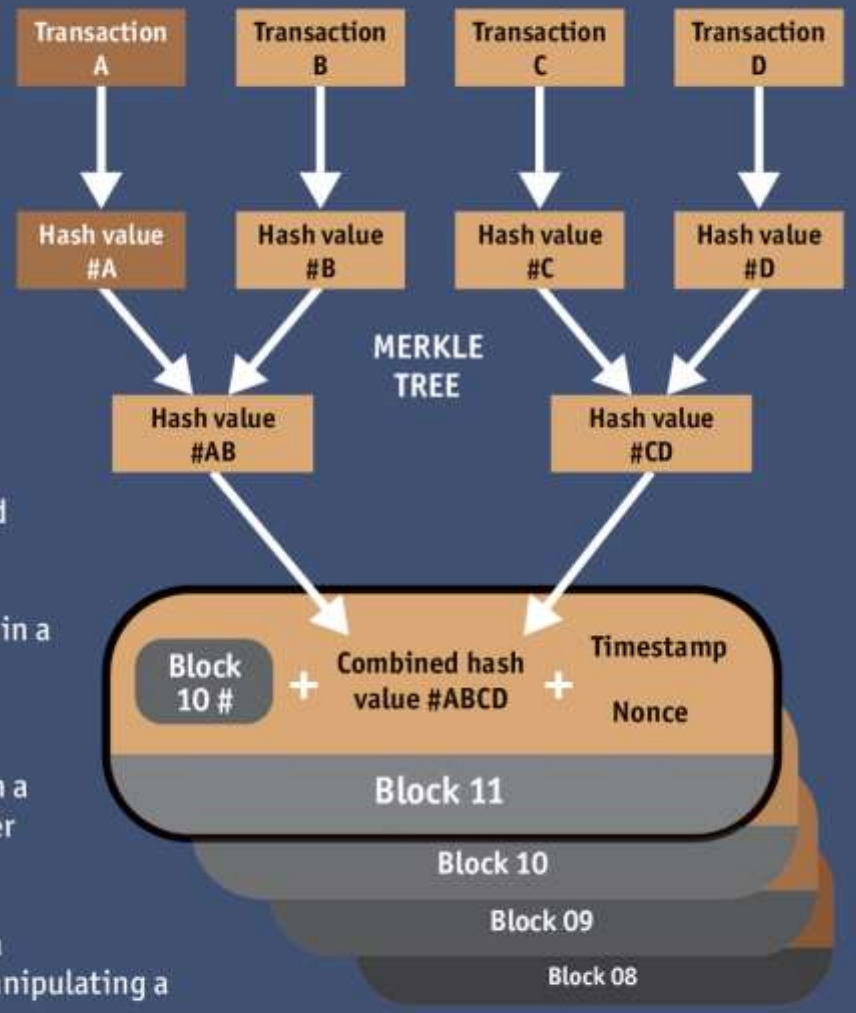
Transaction A

Any length of data

OUTPUT #A

#DFCD 24D9 AEFE 93B9

Unique hash value of fixed length



Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

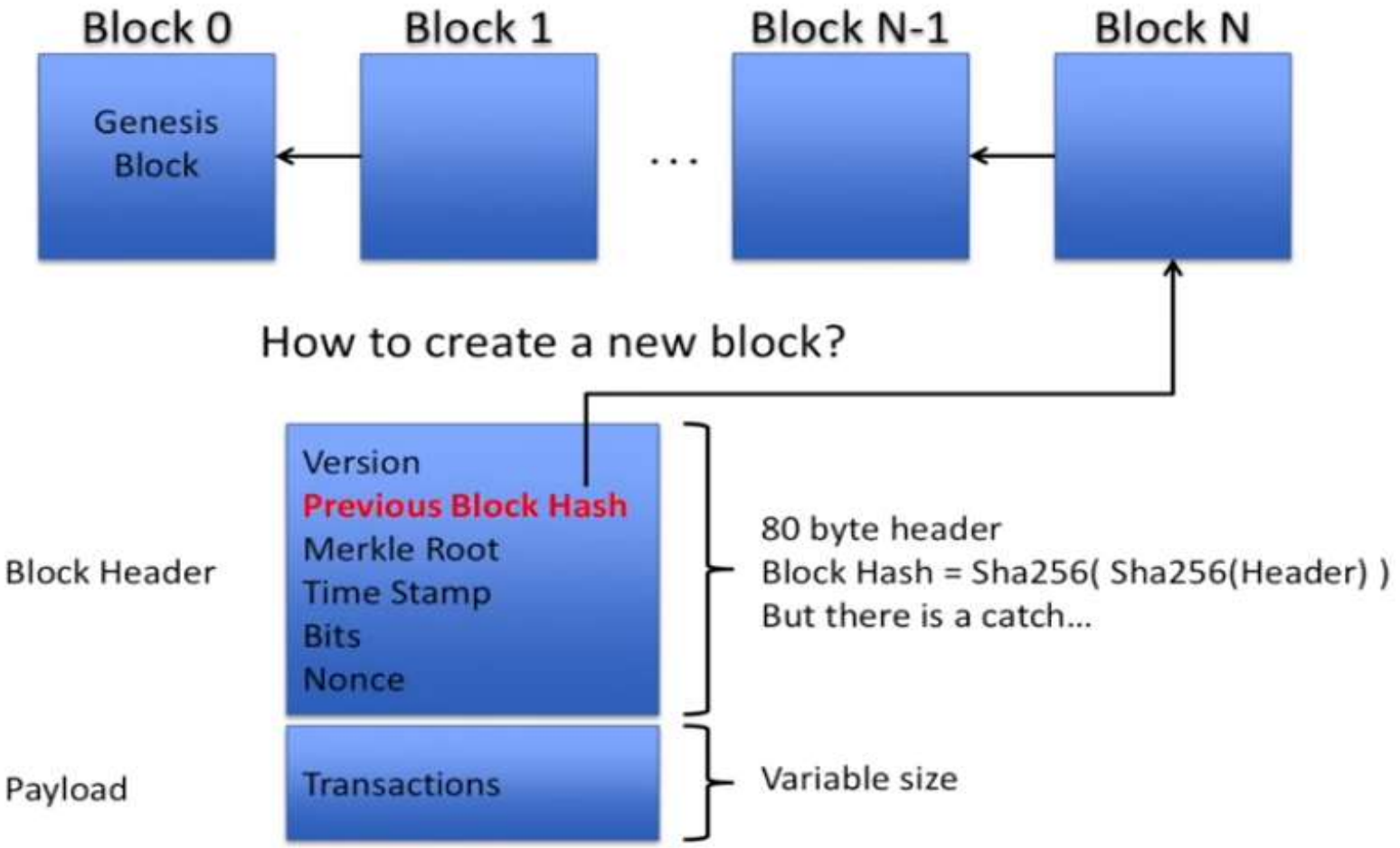
The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

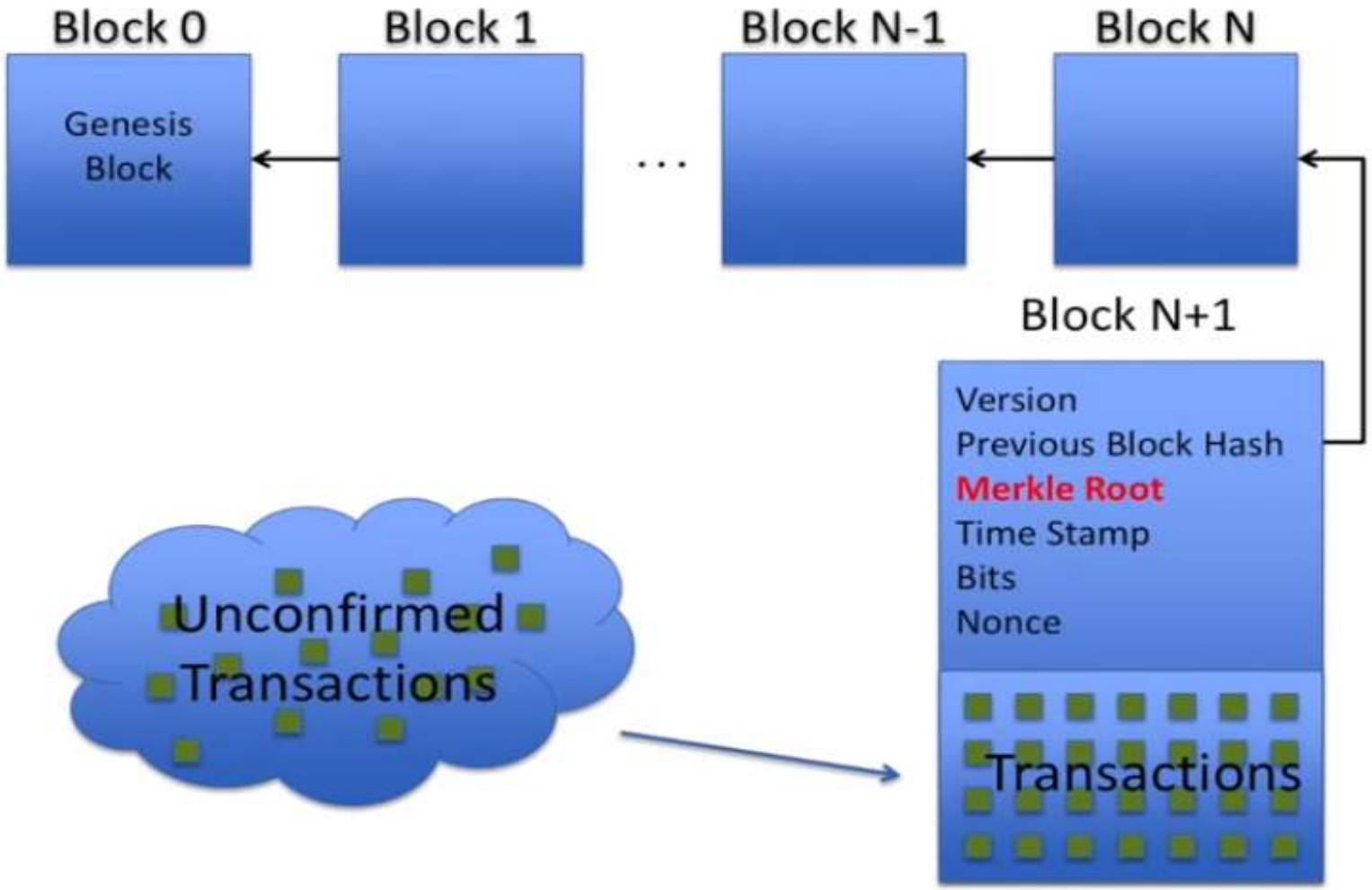
Once a solution is found the new block is added to the blockchain.

What is in a Block?

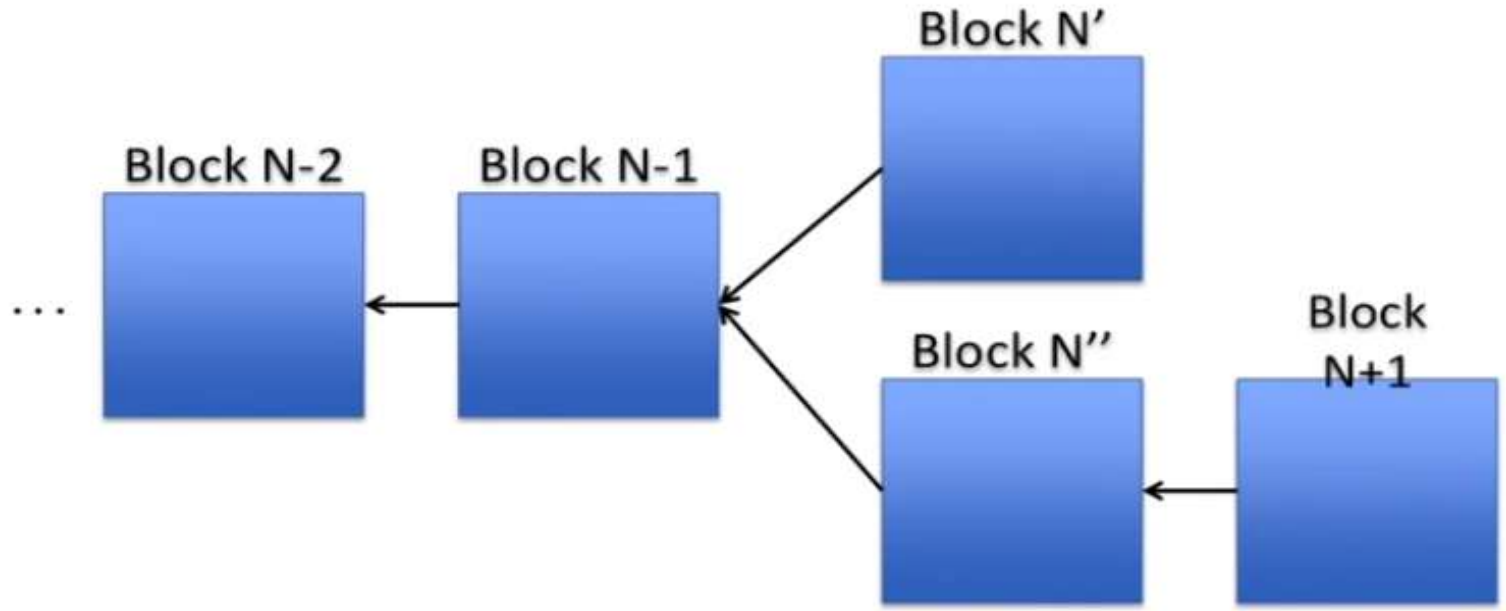
What's in a block?

- ➔ A 'magic number' (0xD9B4BEF9) to show it's a Bitcoin block
- ➔ A size number to specify how much data is coming next
- ➔ Some metadata:
  - A version number of the block format
  - A link to the previous block that came immediately before it
  - Merkle root of all the transactions in the block
  - Timestamp of when the block was created
  - Mining difficulty (more about this later)
  - Nonce for proof-of-work (more about this later)
- ➔ All the transactions that were recorded in this block


Block 0
Block 1
Block N-1
Block N
Genesis Block
...
How to create a new block?
Block Header
Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce
80 byte header
Block Hash = Sha256(Sha256(Header))
But there is a catch...
Payload
Transactions
Variable size


Block 0
Block 1
Block N-1
Block N
Genesis Block
...
Block N+1
Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce
Unconfirmed Transactions
Transactions

Forks are Normal (2)

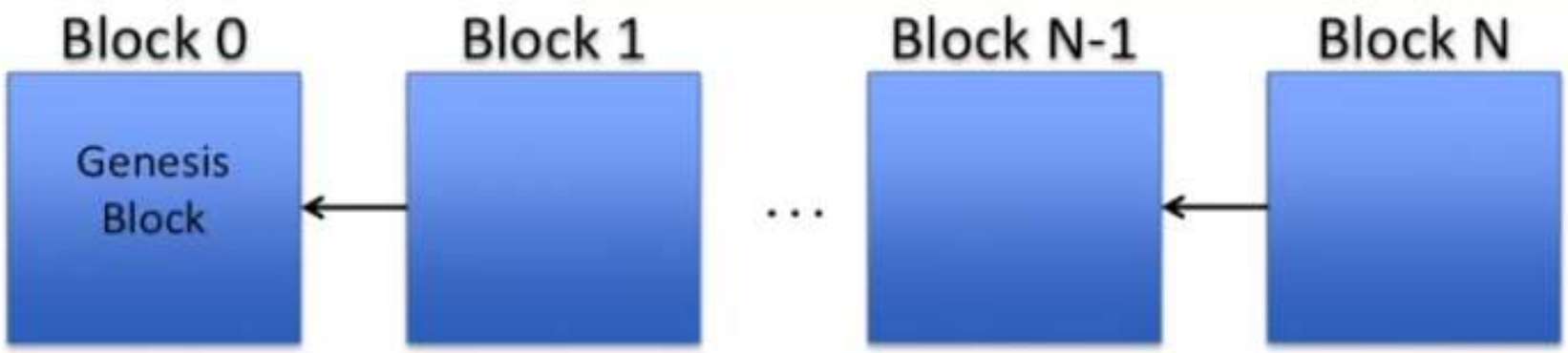


The longest chain wins!

Properties of Bitcoin (1/3)

No Counterfeiting

"NOBODY" can increase money supply at will



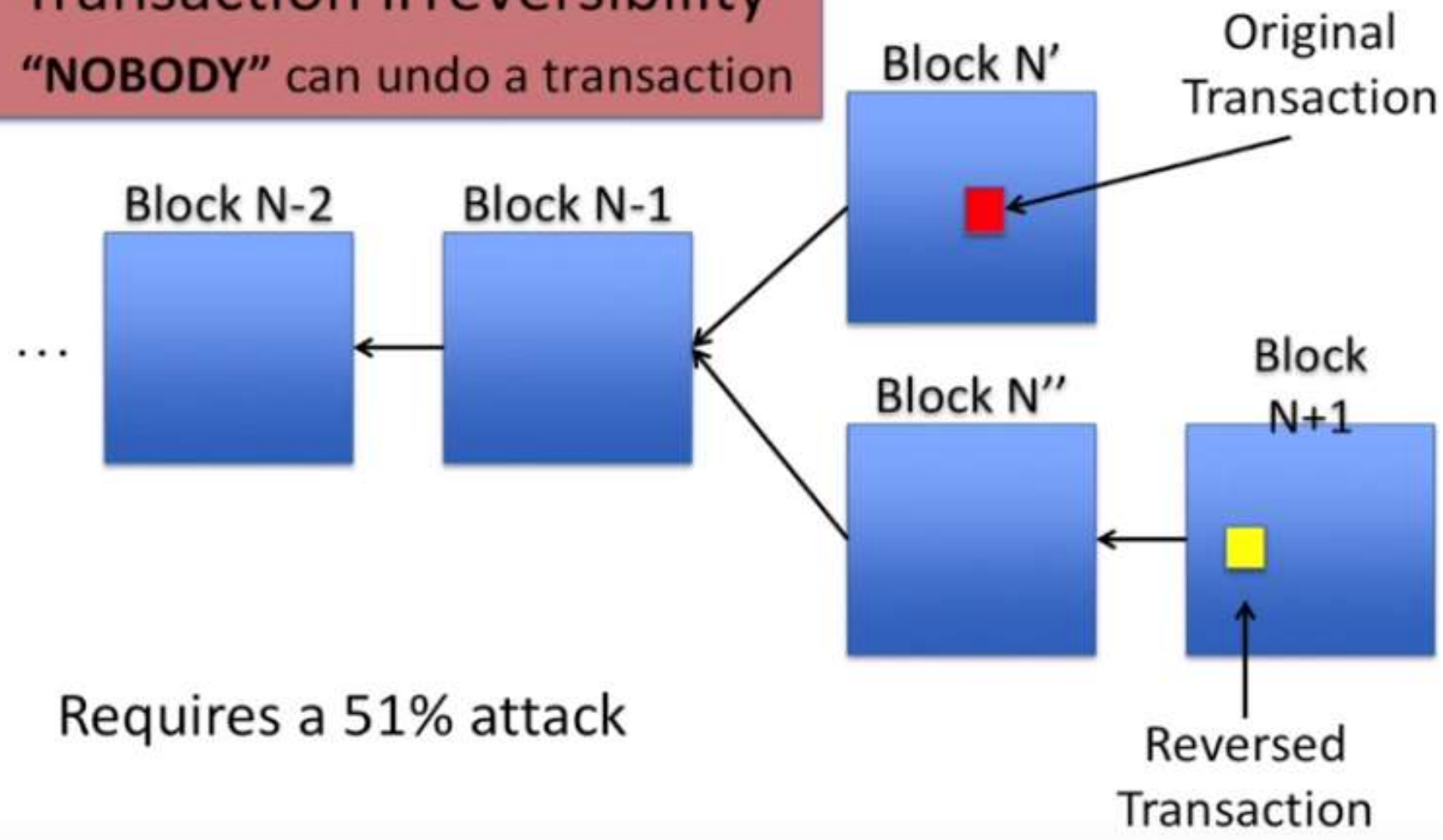
You are competing with the biggest distributed computer the world has seen.

If you can beat it, it just gets harder.

Properties of Bitcoin (2/3)

Transaction irreversibility

"NOBODY" can undo a transaction

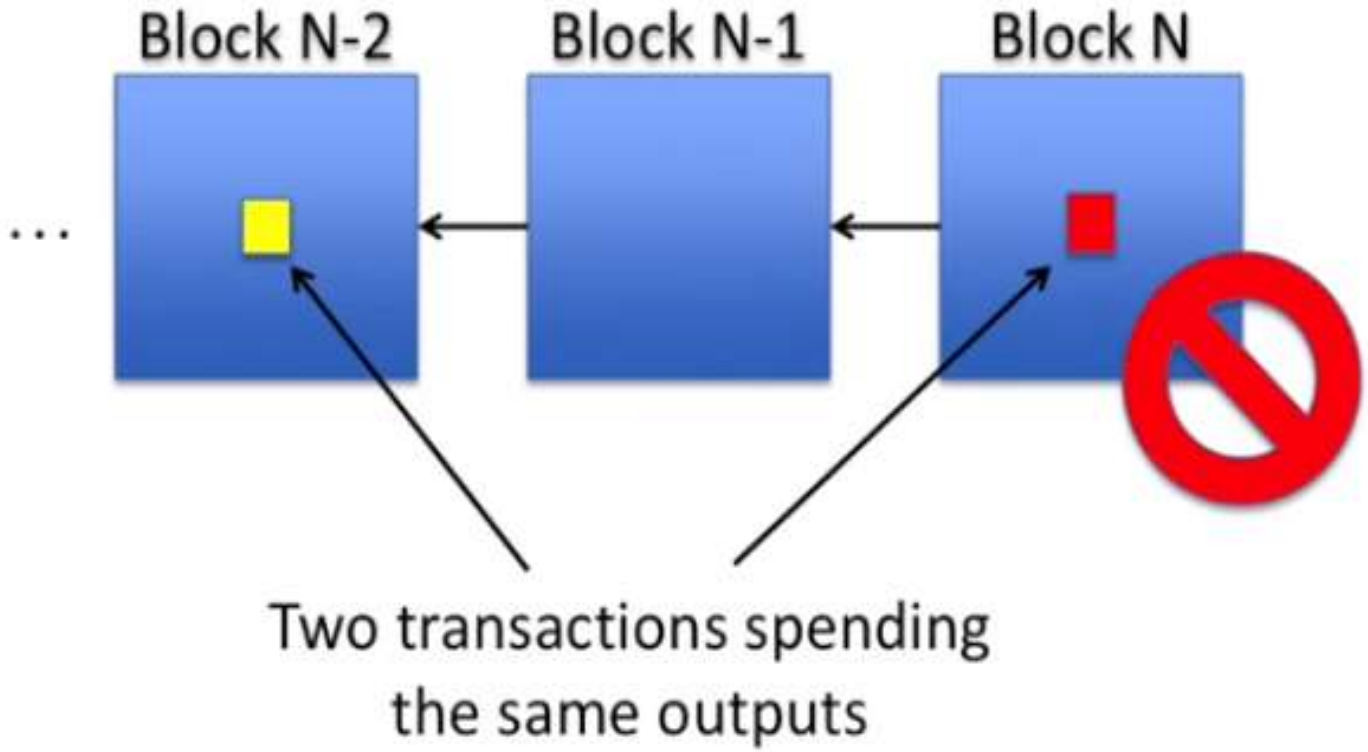


Requires a 51% attack

Properties of Bitcoin (3/3)

No Double Spending

NOBODY can spend the same value more than once



Real Example of Data Stored in Blockchain

- Here's what's happening: a total of 50 BTC is being sent from address 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S. Ten of those BTC are sent to the address 1Q2TWHE3GMdB6BZKafqwxXtWAWgFt5Jvm3, and the remaining forty are being sent back to 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S.


```
{
"hash":"f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16",
"ver":1,
"vin_sz":1,
"vout_sz":2,
"lock_time":0,
"size":275,
"in":[
{
"prev_out":{
"hash":"0437cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9",
"n":0
},
"scriptSig":"304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901"
}
],
"out":[
{
"value":"10.00000000",
"scriptPubKey":"04ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84c OP_CHECKSIG"
},
{
"value":"40.00000000",
"scriptPubKey":"0411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3 OP_CHECKSIG"
}
]
}
```

What Language is Blockchain Written in?

- Asking 'what programming languages are used to build bitcoin' is like asking 'what programming languages are used to build TCP/IP'. Bitcoin, like TCP/IP, is a protocol **it is defined in a programming language neutral way**, **and can be implemented in any programming language**. That said, you're **most likely to find implementations in C++ and Java**, but there's no reason why you couldn't write Bitcoin software in Python or anything you want.
- **The reference implementation, Bitcoin Core, is written primarily in C++,** with various resource files and scripts in other languages.
- Another implementation, mainly used in lightweight clients like MultiBit and Bitcoin Wallet (Android), is bitcoinj. **It is written in Java**.
- **Solidity is a high level language for public Ethereum blockchain** and all the Ethereum based applications are written in this language.

Mining Hardware

Bitcoin Mining Hardware Comparison

Currently, based on (1) price per hash and (2) electrical efficiency the best Bitcoin miner options are:

Bitcoin Mining Hardware

CPU (Central Processing Unit)

In the beginning, mining with a CPU was the only way to mine bitcoins.
Now, you might mine for decades using your laptop without earning a single coin.

GPU (Graphical Processing Unit)

About a year and a half after the network started, it was discovered that high end graphics cards were much more efficient at bitcoin mining and the landscape changed. While any modern GPU can be used to mine, the AMD line of GPU architecture turned out to be far superior to the nVidia architecture for mining bitcoins

FPGA (Field Programmable Gate Array)

While the FPGAs didn't enjoy a 50x - 100x increase in mining speed as was seen with the transition from CPUs to GPUs, they provided a benefit through power efficiency and ease of use. A typical 600 MH/s graphics card consumed upwards of 400w of power, whereas a typical FPGA mining device would provide a hashrate of 826 MH/s at 80w of power. That 5x improvement allowed the first large bitcoin mining farms to be constructed at an operational profit. The bitcoin mining industry was born.

ASIC (Application Specific Integrated Circuit)

The bitcoin mining world is now solidly in the Application Specific Integrated Circuit (ASIC) era. An ASIC is a chip designed specifically to do one thing and one thing only. Unlike FPGAs, an ASIC cannot be repurposed to perform other tasks. An ASIC designed to mine bitcoins can only mine bitcoins and will only ever mine bitcoins. The inflexibility of an ASIC is offset by the fact that it offers a 100x increase in hashing power while reducing power consumption compared to all the previous technologies.

Mining Hardware

Mining Hardware

AntMiner S7

Advertised Capacity:
4,730 Gh/s

Power Efficiency:
0.25 W/Gh

Weight:
8.8 pounds

Guide:
Yes

Price:
$495.95

Buy from amazon.com

Appx. BTC Earned Per Month:
0.9153

Spoondolies Tech SP20 Jackson

Advertised Capacity:
1,500 GH/s

Power Efficiency:
0.80 W/Gh

Weight:
20 pounds

Guide:
Yes

Price:
$300.97

Buy from amazon.com

Appx. BTC Earned Per Month:
0.2902

BPMC Red Fury USB

Advertised Capacity:
2.5 GH/s

Power Efficiency:
1.00 W/GH

Weight:
1.6 ounces

Guide:
Yes

Price:
$23.87

Buy from amazon.com

Appx. BTC Earned Per Month:
0.00077463

Sample GPUs for Mining

Sample ASICs for Mining

Mining Software (sample)

Bitcoin Wallet Software

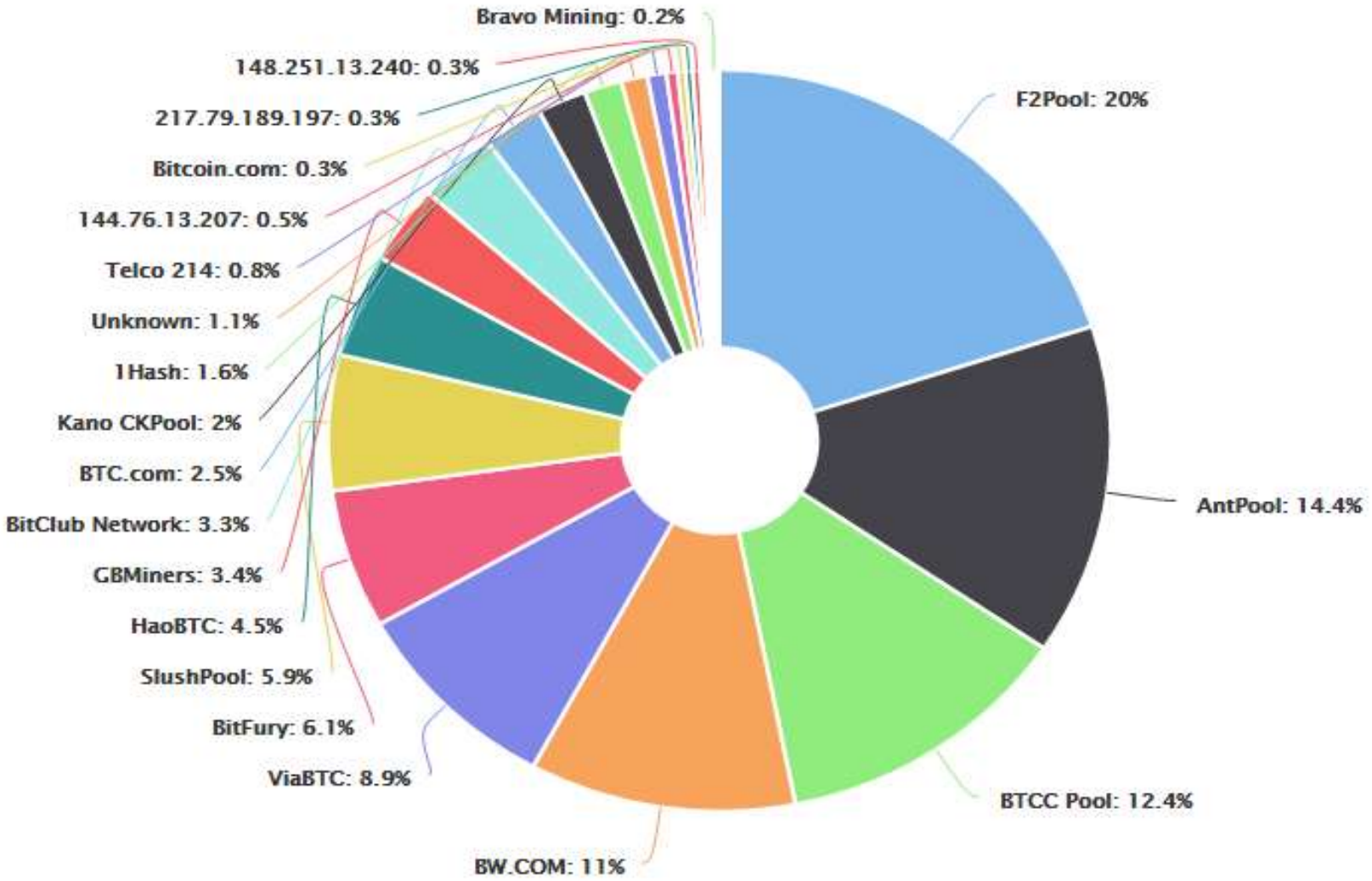
Breadwallet – easy to use mobile Bitcoin wallet
Copay – easy to use mobile Bitcoin wallet
Armory – highly secure desktop Bitcoin wallet

Bitcoin mining software

MinePeon: Open source and may need WinDisk32Imager.
EasyMiner: A GUI based miner for Windows, Linux and Android. EasyMiner acts as a convenient wrapper for the built in CG; BFGminer softwares. It auto configures your Bitcoin miners and provides performance graphs to for easy visualization of your Bitcoin mining activity.
BFGMiner: A modular ASIC, FPGA, GPU and CPU miner written in C, cross platform for Linux, Mac, and Windows including support for OpenWrt-capable routers.
CGMiner: This is a multi-threaded multi-pool GPU, FPGA and ASIC miner with ATI GPU monitoring, (over)clocking and fanspeed support for bitcoin and derivative coins.


pooled mining
/puːld ˈmʌɪnɪŋ/
combines the work of many
miners toward a common goal

Hashrate Distribution Amongst the Largest Mining Pools



Can (Should) I Mine?

- **Most bitcoin users don't mine!**
- Bitcoin mining for profit is very competitive and volatility in the Bitcoin price makes it difficult to realize monetary gains without also speculating on the price.
- **Mining makes sense if you plan to do it for fun**, to learn or to support the security of Bitcoin and do not care if you make a profit.
- If you have **access to large amounts of cheap electricity** and the **ability to manage a large installation and business**, you can mine for a profit.
- If you want to get bitcoins based on a fixed amount of mining power, but you don't want to run the actual hardware yourself, you can purchase a mining contract (**mining pools**).

Bitcoin Mining Calculator

Welcome to 99Bitcoins' simple Bitcoin Mining Calculator

Difficulty factor	220755908330	
Hash rate	0.0002	TH/s
BTC/Block reward	12.5	
USD/BTC exchange rate	621.5950	
Pool Fees %	Leave blank if not sure	
Power (Watts)	Leave blank if not sure	
Power Cost (USD/kWh)	Leave blank if not sure	
Hardware Costs (USD)	Leave blank if not sure	

Calculate mining profit

99Bitcoins' simple Bitcoin Mining Calculator

Performance of Blockchains

- If we are to equate blockchains to other transactions processing networks, what comes to mind is their **processing throughput**, which is measured in transactions per second (TPS). As a reference, in 2015, **VISA handled an average of 2,000 TPS** on their VisaNet, with a **peak rate of 4,000 TPS**, and a **peak capacity of 56,000 TPS**. During 2015, PayPal processed a total 4.9 billion payments,7 equivalent to 155 TPS. As of 2016, **the Bitcoin blockchain was far from these numbers, hovering at 5–7 TPS**, but with prospects of largely exceeding it due to advances in sidechain technology and expected increases in the Bitcoin block size. Some other blockchains are faster than Bitcoin's. For example, **Ethereum started with 10 TPS in 2015, edging towards 50–100 TPS in 2017, and targeting 50,000–100,000 TPS by 2019.**
- **Private blockchains are even faster because they have less security requirements, and we are seeing 1,000–10,000 TPS in 2016**, going up to 2,000–15,000 TPS in 2017, and potentially an unlimited ceiling beyond 2019. Finally, linking blockchain's output to clustered database technology might push these transactional throughput limits even higher, leading to a positive development.

Evolution of the Blockchain Networks

currency and payments (**Blockchain 1.0**)

contracts, property, and all financial markets transactions (**Blockchain 2.0**)

government, health, science, literacy, publishing, economic development, art, and culture (**Blockchain 3.0**)

Private vs Public Blockchains

- A public blockchain is open and interoperable, like the internet, and a private blockchain is closed and limits the people who are granted access, like an intranet.

- However, if you want to transfer digital assets between a closed group of people, want to maintain privacy of transactions between a closed group of people, or have a high volume of transactions per second, then a private blockchain is needed.

- However, the greatest advancements in blockchain technology are all based on the advantages derived from the public, 'open' type of blockchain, while most people in the professional finance world are looking for advancements in the private, 'permissioned' type of blockchain.

- So-called Bitcoin Maximalists support the use Bitcoin's completely public blockchain, where anyone with a computer can join. Banks, on the other hand, are mainly interested in private, or closed, blockchains where participation is limited to known, trusted parties.

- For banks, the debate about public or private blockchain "is academic" in a world where regulators and auditors require information about parties in a financial system, said Mr. Cooper of R3. A completely open, public blockchain like Bitcoin's means that sometimes participants are anonymous, he said. "There is not a regulator on the planet that is comfortable right now with unknown parties responsible for validating financial transactions," he said.

Advantages of Private Blockchains

- **The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc.**
- The validators are known, so any risk of a 51% attack arising from some miner collusion in China does not apply.
- **Transactions are cheaper, since they only need to be verified by a few nodes that can be trusted to have very high processing power, and do not need to be verified by ten thousand laptops.**
- Nodes can be trusted to be very well-connected, and faults can quickly be fixed by manual intervention, allowing the use of consensus algorithms which offer finality after much shorter block times.
- **If read permissions are restricted, private blockchains can provide a greater level of, well, privacy.**

Advantages of Public Blockchains

- **Public blockchains provide a way to protect the users of an application from the developers, establishing that there are certain things that even the developers of an application have no authority to do.**

- Public blockchains are open, and therefore are likely to be used by very many entities and gain some network effects.

Which Type to Choose?

- The solution that is optimal for a particular industry **depends very heavily on what your exact industry is**. In some cases, public is clearly better; in others, some degree of private control is simply necessary. **As is often the case in the real world, it depends**.

Public Blockchain Companies

HYPERLEDGER

Private Blockchain Companies

AlphaPoint

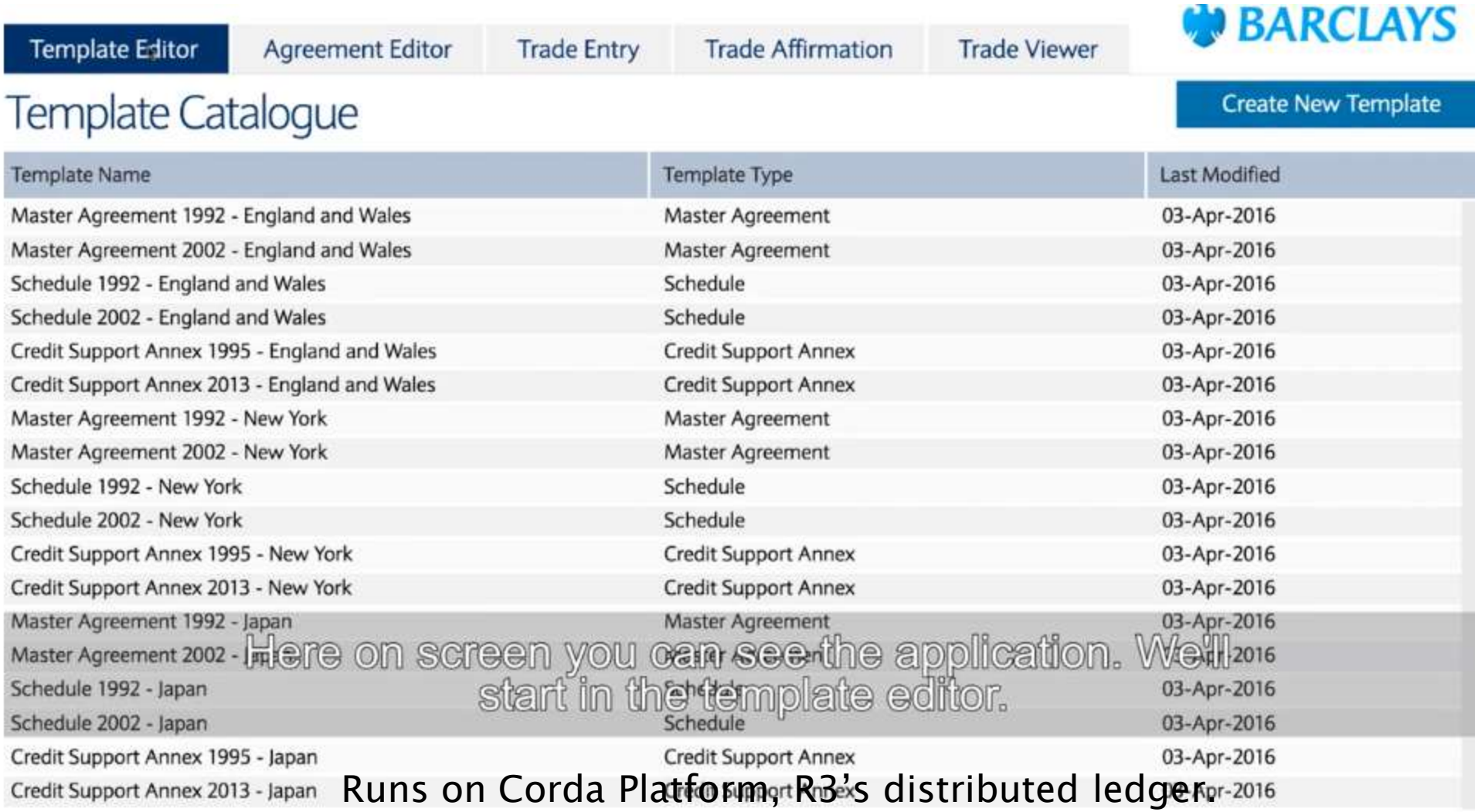
StreamCore

MultiChain

Smart Contracts

- One of the most radical ideas for blockchain technology is the **notion of digitising law**.
- **The industry jargon is "smart contracts"** — **code on a shared database that automatically executes a contract based on the fulfilment of certain real-world conditions**, just as a vending machine obeys rules to provide sweets when money is inserted.

Barclay's Smart Contract Template Catalogs



Here on screen you can see the application. We'll start in the template editor.

Runs on Corda Platform, R3's distributed ledger.
Uses CLARK language.

Cryptocurrencies

BDDK
BANKACILIK
DÜZENLEME VE DENETLEME
KURUMU

BASIN AÇIKLAMASI

Sayı : 2013 / 32 **25 Kasım 2013**

BASIN AÇIKLAMASI

Son dönemde bazı basın yayın kuruluşlarında ve internette "Bitcoin" hakkında çeşitli haberlerin çıktığı görülmektedir. Bilindiği üzere, 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun" (Kanun) 27.06.2013 tarih ve 28690 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Kanunun Geçici 1 inci maddesine göre bu Kanunda öngörülen yönetmelikler Kanunun yayımı tarihinden itibaren bir yıl içinde hazırlanarak yürürlüğe konulacaktır. Kanunun Geçici 2 nci maddesine göre ise Kanunun yürürlüğe girdiği tarih itibari ile ödeme hizmetleri sunan ya da elektronik para ihraç eden ve bu Kanun kapsamında ihdas edilen ödeme veya elektronik para kuruluşu kategorisine dahil edilebilecek olan kuruluşlar Kurumumuzca çıkarılacak ilgili yönetmeliklerin yayımı tarihinden başlayarak bir yıl içinde Kurumumuza başvurarak gerekli izinleri almak ve uygulamalarını bu düzenlemelerde yer alan hükümlere uygun hale getirmek zorundadır. Herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin, mevcut yapısı ve işleyişi itibarıyla Kanun kapsamında elektronik para olarak değerlendirilmemekte, bu nedenle de söz konusu Kanun çerçevesinde gözetim ve denetimi mümkün görülmemektedir. Diğer taraftan, Bitcoin ve benzeri sanal paralar ile gerçekleştirilen işlemlerde tarafların kimliklerinin bilinmemesi, söz konusu sanal paraların yasadışı faaliyetlerde kullanılması için uygun bir ortam yaratmaktadır. Ayrıca Bitcoin, piyasa değerinin aşırı oynak olabilmesi, dijital cüzdanların çalınabilmesi, kaybolabilmesi veya sahiplerinin bilgileri dışında usulsüz olarak kullanılabilmesi gibi risklerin yanı sıra yapılan işlemlerin geri döndürülemez olmasından dolayı operasyonel hatalardan ya da kötü niyetli satıcıların suistimalinden kaynaklı risklere de açıktır. Herhangi bir mağduriyet yaşanmaması adına, yukarıda belirtilen hususların duyurulmasında ve bu çerçevede Bitcoin ve benzeri sanal paraların barındırdığı muhtemel risklerin kamuoyuna hatırlatılmasında fayda mülahaza edilmektedir. Kamuoyuna saygıyla duyurulur.

Epilogue for Cryptocurrency

- **One valuable blockchain outcome we exposed is the emergent crypto economy**, the sum of the economic realizations resulting from applying the blockchain's potential. This crypto economy is a trust economy that is decentralized at birth, both politically and architecturally; and it lends equal access and lower barriers of entry to all.
- **As we prepare to get on board the crypto economy, undoubtedly it looks fuzzy, foggy, buggy, risky, uncertain, and unproven. Then suddenly, it will blossom and grow with more benefits than disadvantages.→** ***this might be true!***

Bitcoin

- The bitcoin protocol initially stipulated that the block reward was 50 bitcoin per block. However, every 4 years the block reward is halved. Currently the reward is sitting at 12.5 bitcoin per block. The next halving is around mid 2020. This 4 year halving continues forever. The total supply of bitcoin is initially quite inflationary but over time will eventually settle down to 21 million and no more. This protracted period will only conclude in around 2140. Satoshi Nakamoto, the creator of bitcoin, stipulated that the choice for this halving was to mimic the natural supply of gold since he/she/they wanted bitcoin to resemble a type of digital gold.

Bitcoin

Crypto-Currency Market Capitalizations

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾ Search Currencies

All ▾ Currencies ▾ Assets ▾ USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$10,206,507,019	$640.86	15,926,316 BTC	$48,686,600	-0.26%	
2	Ethereum	$1,011,822,863	$11.90	85,058,582 ETH	$4,724,580	-0.66%	
3	Ripple	$286,856,394	$0.008086	35,475,773,335 XRP *	$1,437,980	-0.80%	
4	Litecoin	$186,448,088	$3.88	48,023,554 LTC	$1,569,610	-0.39%	
5	Ethereum Classic	$91,856,159	$1.08	84,967,818 ETC	$5,449,880	8.39%	

Crypto-Currency Market Capitalizations

Bitcoin Addresses

- **Your Bitcoin address** is typically an identifier of 26 to 34 alphanumeric characters — **for example,1JDQ5KSqUTBo5M3GUPx8vm9134eJRosLoH**, represented like this string of characters or as a QR code.
- Your Bitcoin address is like your email address; people with your email address can send you email; **people with your public-key wallet address can send you Bitcoins**.
- When the wallet is initialized or set up for the first time, an address, public key, and private key are automatically generated. **Bitcoin is based on public-key encryption, meaning that you can give out the public key freely but must keep the private key to yourself.**

Cryptocurrency Clients

How to Get Started

There are two types of client software:

Lightweight Client

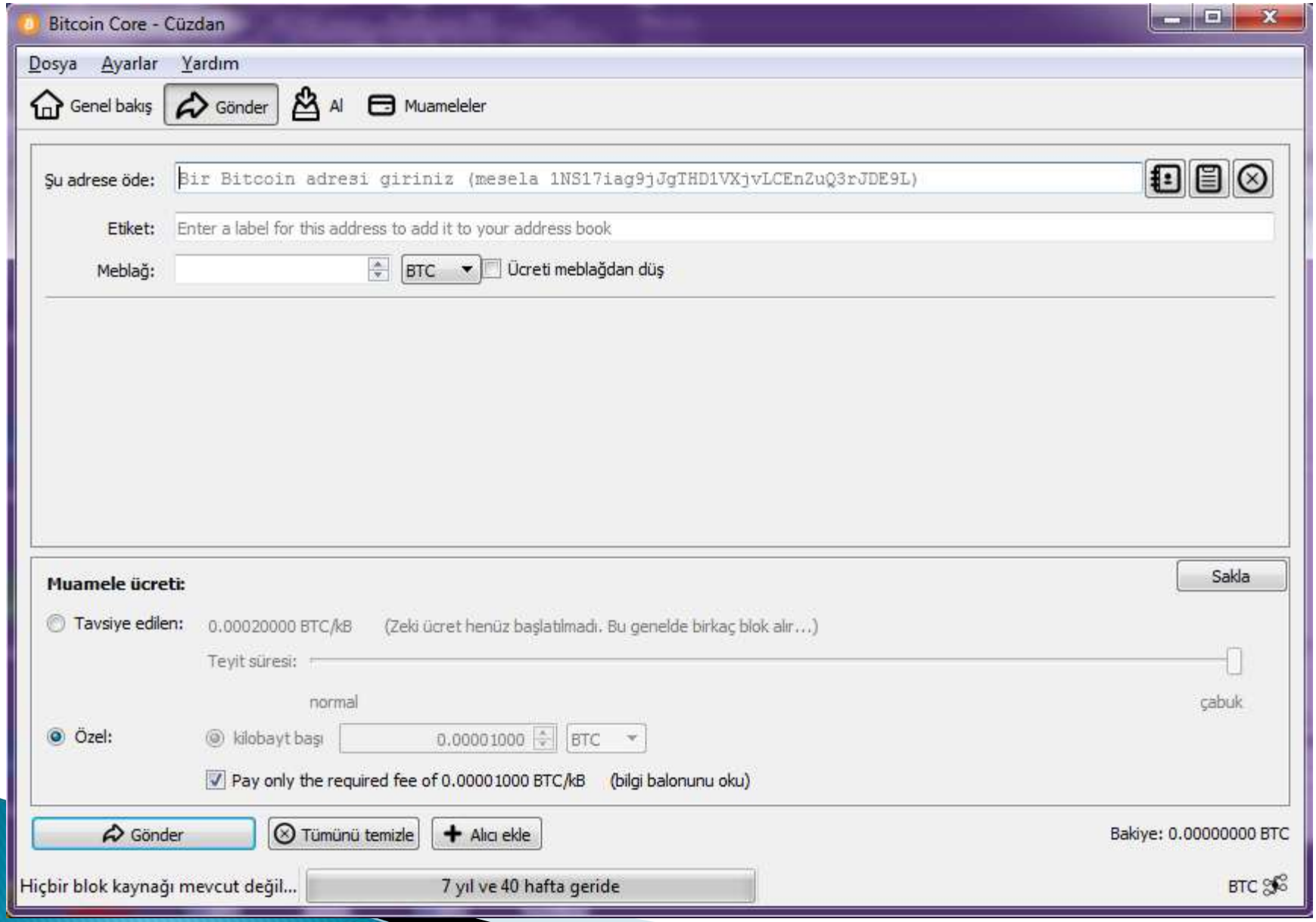
Doesn't download the entire blockchain, connects to other nodes and only collects information on transactions to it's own addresses

Full/Core Client

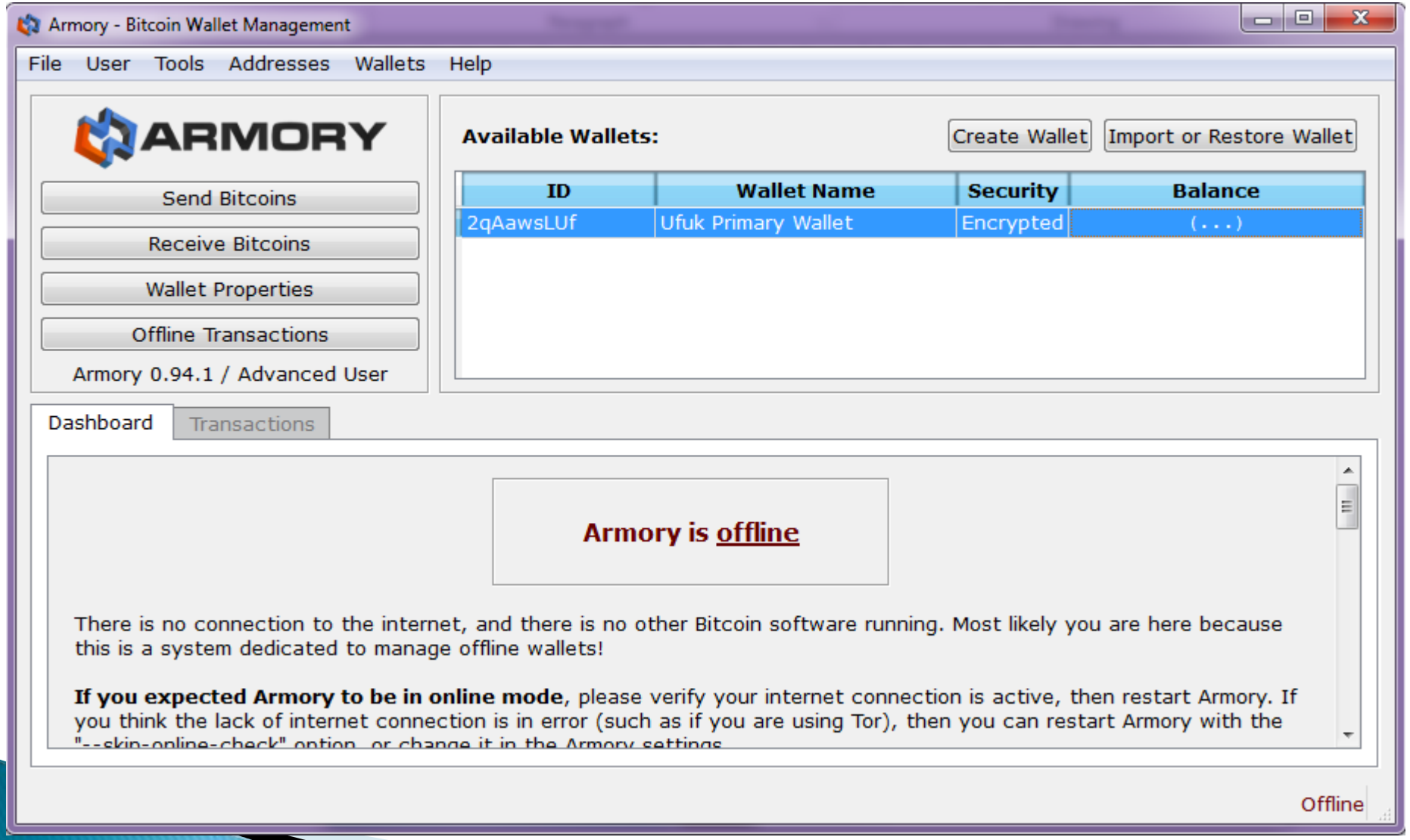
Runs as a full node on the network, downloads entire blockchain

https://bitcoin.org/en/choose-your-wallet

Bitcoin Core – Wallet

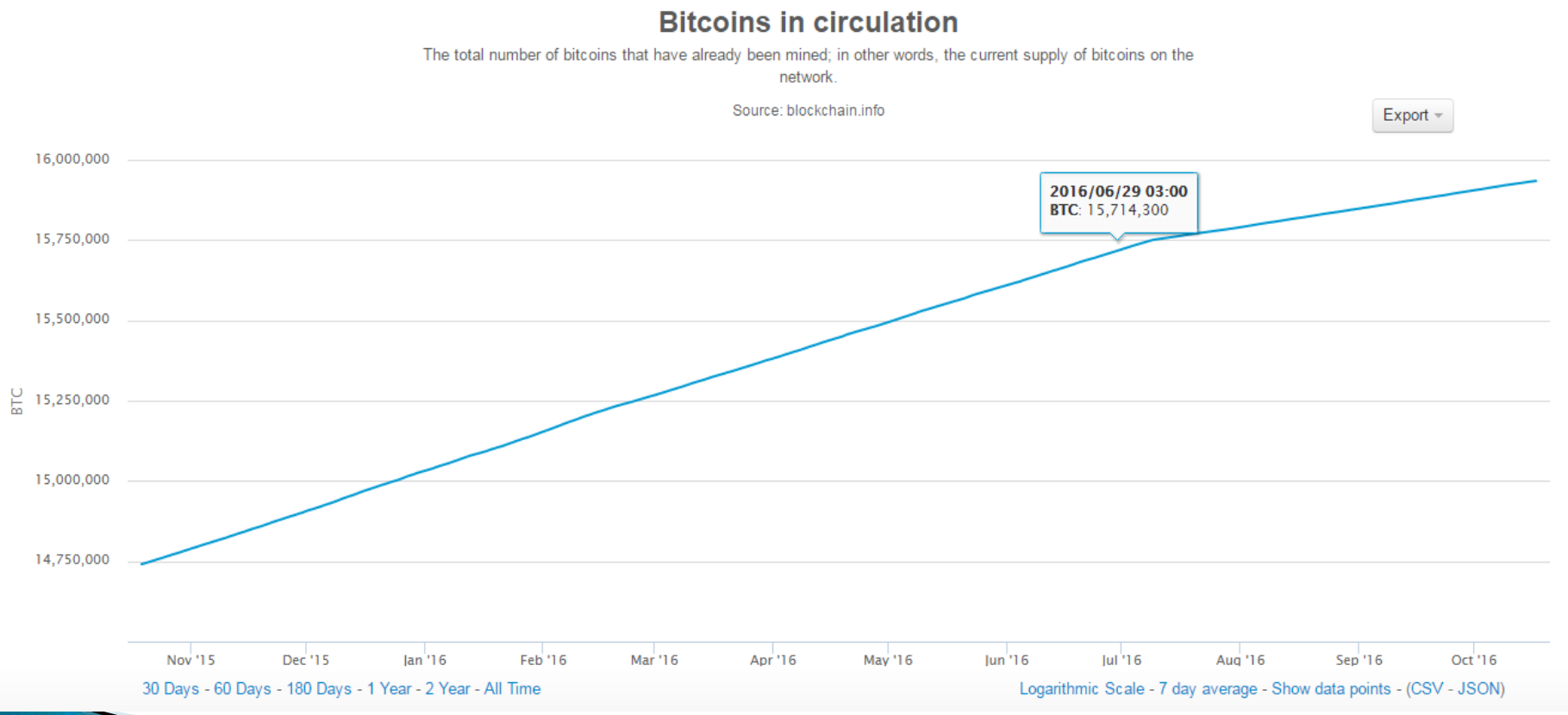


Armory – Wallet



Bitcoin Blockchain Charts

- https://blockchain.info/charts

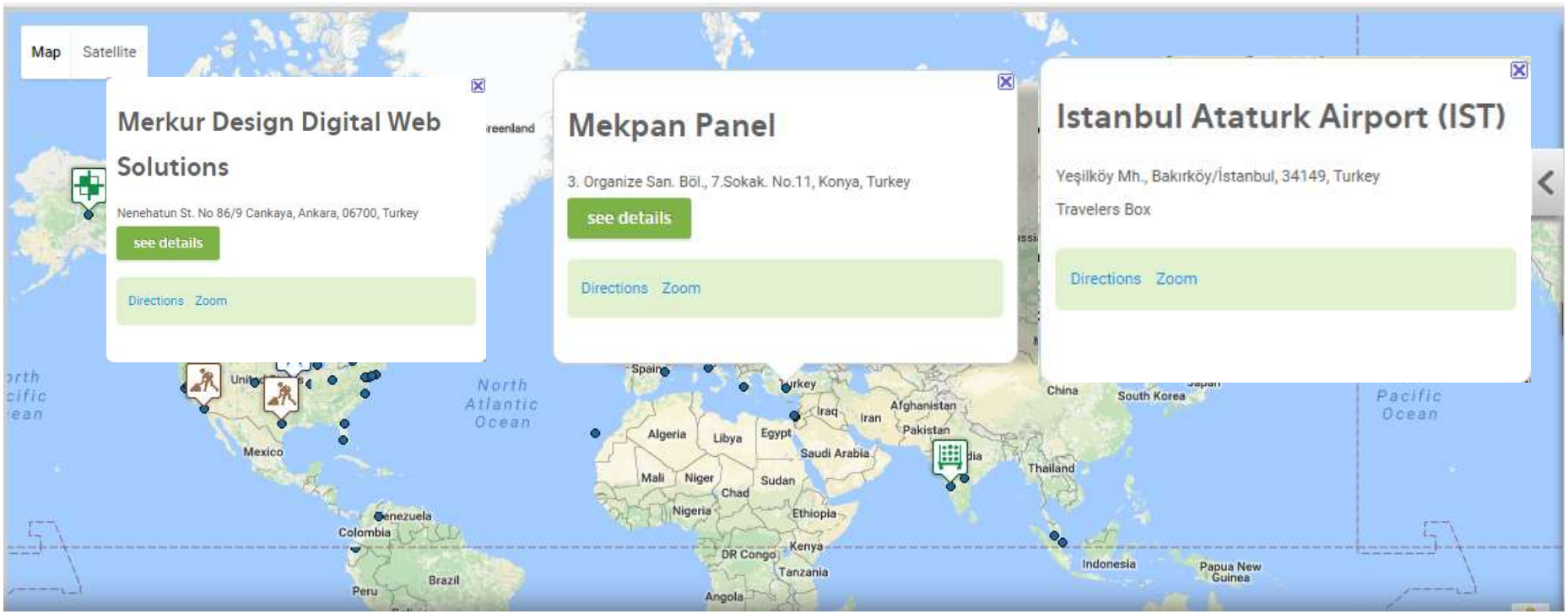


Where to Use Bitcoins?

Use Bitcoins in the real world

Where to Use Bitcoin?

Where to Use Bitcoins in Turkey?



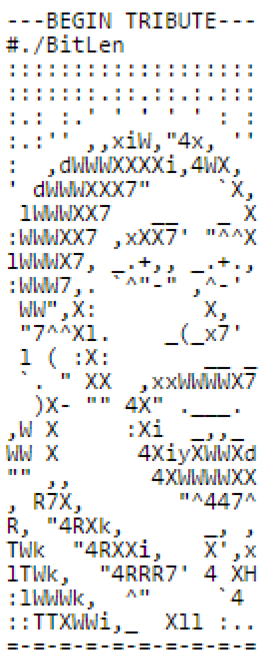
Where to Use Bitcoin?

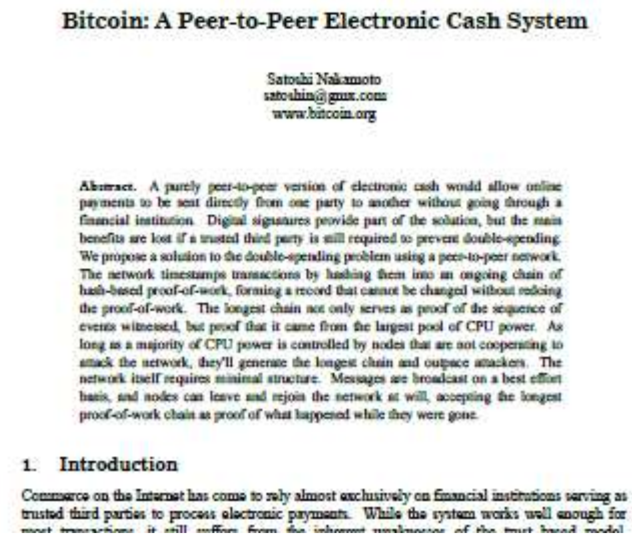
Hidden Surprises in the Bitcoin Blockchain

- **Nelson Mandela, Wikileaks, photos, and Python software**
- Secret message in the first Bitcoin block
  'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks'
- **Bitcoin logo**
- **Prayers from miners**
- A tribute to cryptographer Len Sassaman was put in the Bitcoin blockchain a couple weeks after his death by Dan Kaminsky.
- **Valentine's day messages**

The possibility of someone being able to permanently, publicly store data is going to make the future a very interesting place.

Hidden surprises in the Bitcoin blockchain





Bitcoin: A Peer-to-Peer Electronic Cash System

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

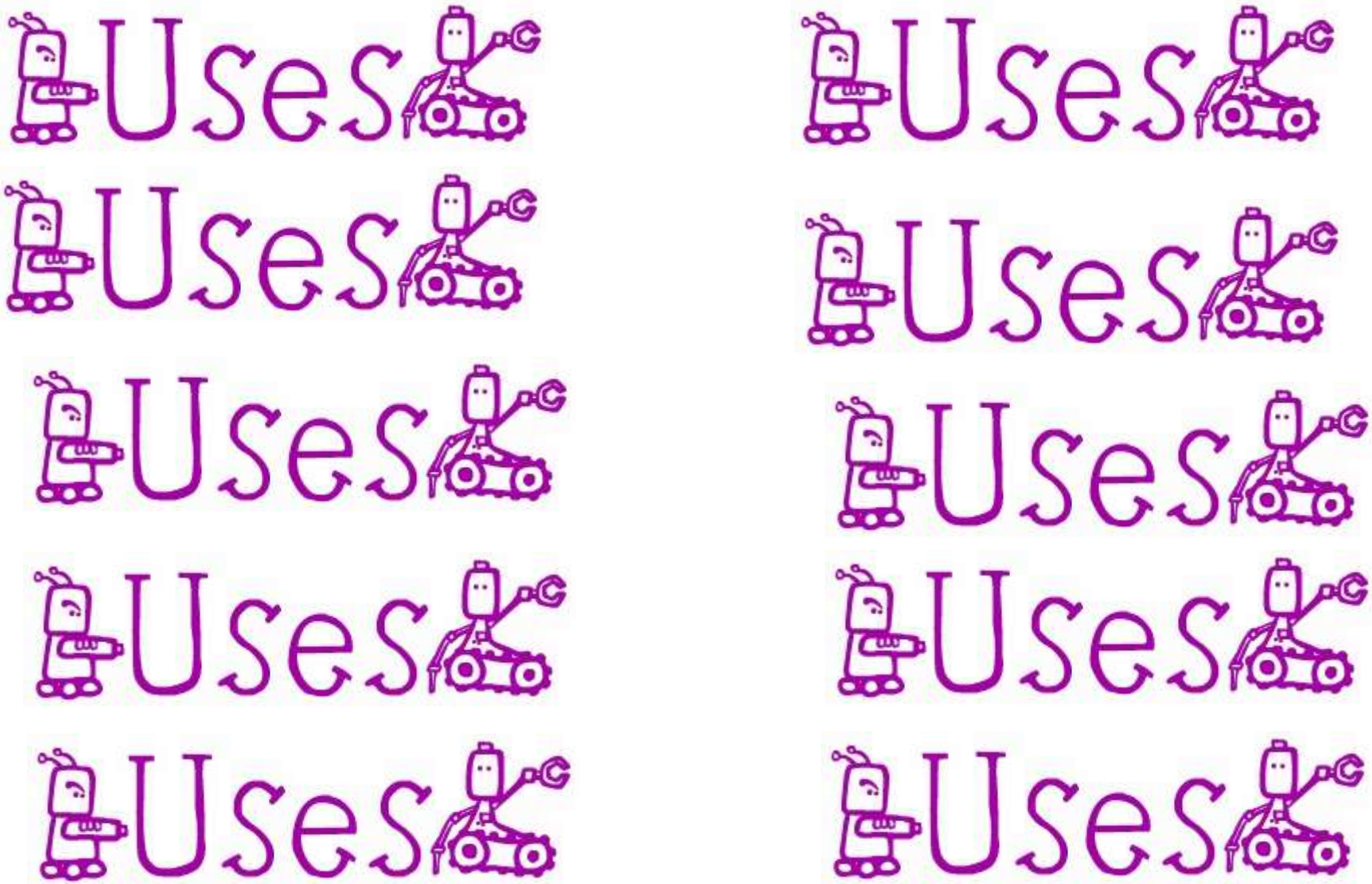
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required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

bitcoin

Blockchain Use Cases



Avoiding the Pointless Blockchain Projects

«Big company hears that blockchains are the next big thing. Big company finds some people internally who are interested in the subject. Big company gives them a budget and tells them to go do something blockchainy. Soon enough they come knocking on our door, waving dollar bills, asking *us* to help *them* think up a use case. Say what now?»

Avoiding the pointless blockchain project

How to Determine If You've Found a Real Blockchain Use Case

1. The database

- **If your requirements are fulfilled by today's relational databases, you'd be insane to use a blockchain.**
- Blockchains are a technology for **shared databases**.

2. Multiple writers

- Blockchains are a technology for **databases with multiple writers.** In other words, there needs to be more than one entity which is generating the transactions that modify the database. Do you know who these writers are? In most cases the writers will also run "nodes" which hold a copy of the database and relay transactions to other nodes in a peer-to-peer fashion.

How to Determine If You've Found a Real Blockchain Use Case

3. Absence of trust

- If multiple entities are writing to the database, there also needs to be some degree of *mistrust* between those entities. In other words, blockchains are a technology for **databases with multiple non-trusting writers**.

How to Determine If You've Found a Real Blockchain Use Case

4. Disintermediation

The problem is enabling a database with multiple non-trusting writers. And there's already a well-known solution to this problem: **the trusted intermediary.**

But the question you need to ask is: **Do you want or need this disintermediation?** Given your use case, is there anything wrong with having a central party who maintains an authoritative database and acts as the transaction gatekeeper? **Good reasons to prefer a blockchain-based database over a trusted intermediary might include lower costs, faster transactions, automatic reconciliation, new regulation** or a simple **inability to find a suitable intermediary.**

How to Determine If You've Found a Real Blockchain Use Case

5. Transaction interaction

In the fullest sense, this means that transactions created by different writers often depend on one other. For example, let's say Alice sends some funds to Bob and then Bob sends some on to Charlie. In this case, Bob's transaction is dependent on Alice's one, and there's no way to verify Bob's transaction without checking Alice's first. Because of this dependency, the transactions naturally belong together in a **single shared database**.

How to Determine If You've Found a Real Blockchain Use Case

Conclusion

- If your project does not fulfill **every single one of these conditions**, you should not be using a blockchain. In the absence of any of the first five, you should consider one of: (a) regular file storage, (b) a centralized database, (c) master-slave database replication, or (d) multiple databases to which users can subscribe.
- And if you do fulfill the first five, there's still work to do. You need to be able to express the rules of your application in terms of the transactions which a database allows. You need to be confident about who you can trust as validators and how you'll define distributed consensus. And finally, if you're looking at creating a shared ledger, you need to know who will be backing the assets which that ledger represents.

Blockchain Use Cases

Bitcoin ATM

Türkiye'nin İlk (dünyanın ikinci) Bitcoin ATM'si İstanbul Atatürk Havalimanı'nda Kullanıma Açıldı **02 Aralık 2013**

Atatürk Havalimanı dış hatlar terminalinde bulunuyordu bitcoin atm'si fakat kaldırıldığı söyleniyordu.

https://www.youtube.com/watch?v=fVUFwGqsqiA

Bitcoin ATM Map

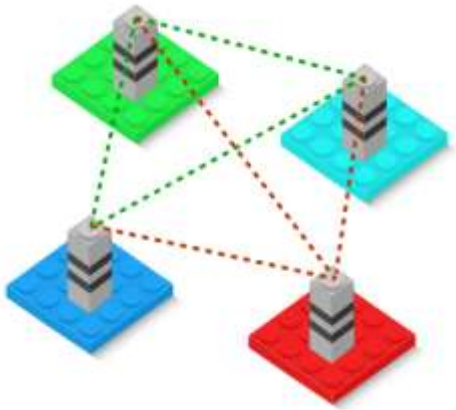
Bitcoin ATM Map

Current Cryptocurrency Distribution on Earth

Blockchain Use Cases

- Voting system
- Proof of existence
- Smart Contracts
- Decentralized DNS (Namecoin). DNS is a ledger bookkeeping domain names.
- Trustless public key encryption (i. e. https without these untrustworthy Certificate Authorities)
- Ownership records. The ledger bookkeeps the objects and their owners.
- Contracts and escrows (kefil kullanma). The ledger bookkeeps the participants and the wording of the contracts.

Blockchain Use Cases

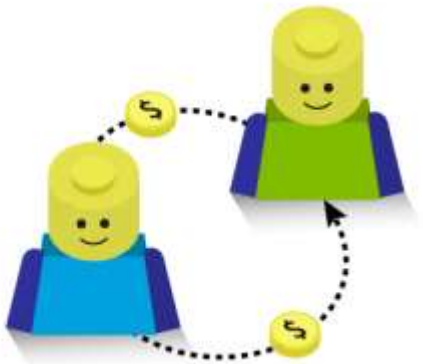


Decentralized Capital Markets

A frictionless capital markets system; enabled by digital tokens stored on the blockchain to represent existing financial instruments. Securities clearing, ownership records management, and corporate actions are self-executing and traceable processes

Peer to Peer Payments

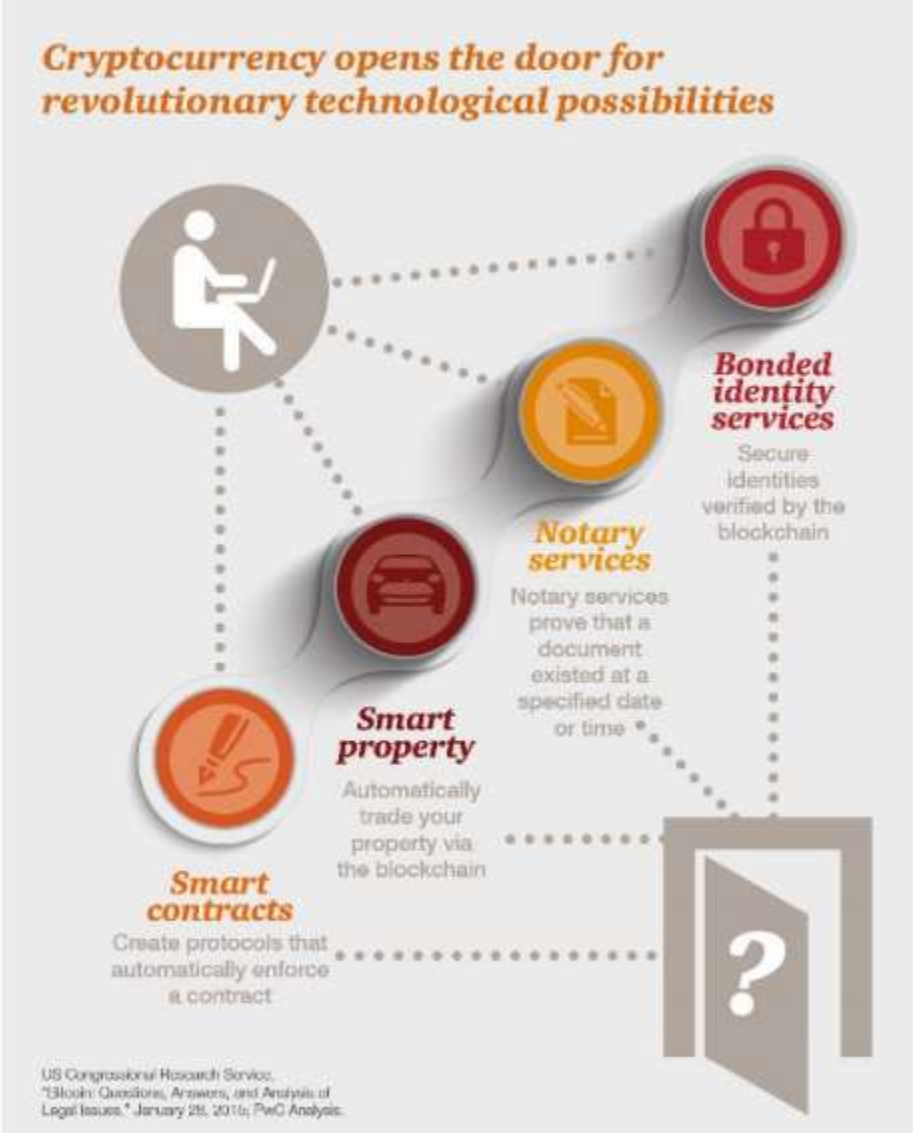
A distributed ledger shared by financial institutions equipped to handle large or small sum transfers. Records management and settlement between financial institutions is simplified by leveraging a tokenized system



Health Data Management

A distributed medical records system to store medical records across multiple parties and jurisdictions, creating an auditable trail of medical procedures completed. The use of smart contracts ensures data privacy while providing necessary stakeholders with permissioned data access

Blockchain Uses Cases



Blockchain Use Cases: Comprehensive Analysis & Startups Involved

blockchain use cases and initiatives taken by financial services industry

Blockchain & Banking

- Now much of the conversation has moved on from bitcoin and cash, to blockchain and what shared database technology might mean for the financial system. The hype and investment have moved to blockchain start-ups that promise to decrease settlement times and cut back-office bank costs.
- Unlike bitcoin, which has been running since 2009, ***uses of blockchain in banking remain largely experimental***. One vision is for a single database maintained and accessed by the biggest banks to execute and settle trades.
- Simon Taylor, who leads the team looking at blockchain and distributed ledger at Barclays, says **there are industry discussions about how each bank would maintain its own privacy in a shared database**. **There are also questions about how much access regulators should have, he adds**.
- "If a shared ledger has the golden source record of everything that's happening, under what circumstances can the regulator see it? What's the appropriate regulatory input into that system? And are they ready for that level of automation? Are they ready for a software-driven regulation?" he says.

FINANCIAL NEWS

Friday, 21 October 2016

Banks break new ground with blockchain trade test

By Anna Irrera

20 January 2016

A group of 11 banks – including the UK's Barclays, HSBC and Royal Bank of Scotland – have traded assets as part of a test of new blockchain technology. It marks one of the first known examples of banks successfully using a distributed ledger to trade with each other.

Why Banks Bother with Blockchain?

- Blockchains has potential to change the world. Startups (Blockchains Startups), Big banks and some governments are implementing blockchains as distributed ledgers to revolutionize the way information is stored and transactions is conducted. Their goals are laudable—**speed**, **lower cost**, **security**, **fewer errors**, and the **elimination of central points of attack and failure**. These models don't necessarily involve a cryptocurrency for payments.

Where Banks Use Blockchains

- **Cross border banking/trade** activity,
- **payments**,
- **settlement and clearing,**

In the shorter term, clearing and settlement is proving to be the most active use case area for blockchain in banking, mainly because it gives a short-term win with real cost savings. Clearing and settlement costs billions and, according to Santander's 2015 report LINK, it is estimated that moving this into a digital record, near real-time and over the internet, will save the industry $20 billion a year in more in overhead costs

- **fixed income markets**,
- **funds transfer** (like to compete with SWIFT), and account information across divisions of the bank like HSBC NY being able to communicate and easily transmit client information to HSBC Singapore (which is something that is more difficult to do than people realize today).

Many of these on this list are why nearly every multinational bank today is looking at or already has a blockchain project in motion.

Where Banks Use Blockchains

- **Cross border banking/trade** activity, **payments**, securities
- settlement and clearing,

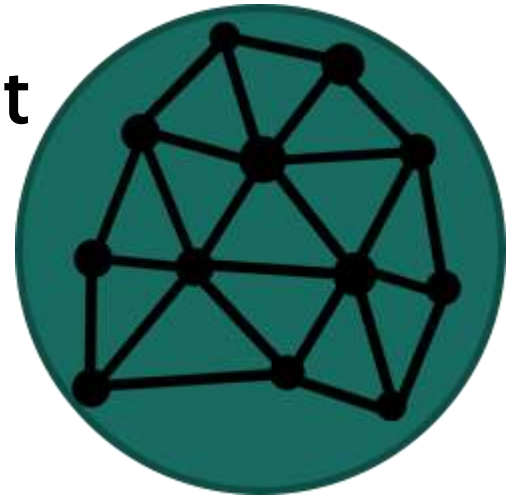
In the shorter term, clearing and settlement is proving to be the most active use case area for blockchain in banking, mainly because it gives a short-term win with real cost savings. Clearing and settlement costs billions and, according to Santander's 2015 report LINK, it is estimated that moving this into a digital record, near real-time and over the internet, will save the industry $20 billion a year in more in overhead costs

- fixed income markets, funds transfer (like to compete with SWIFT), and account information across divisions of the bank like HSBC NY being able to communicate and easily transmit client information to HSBC Singapore (which is something that is more difficult to do than people realize today).

  Many of these on this list are why nearly every multinational bank today is looking at or already has a blockchain project in motion.

R3 CEV Consortium

- R3 is a financial innovation firm that leads a consortium partnership with **over 50 of the world's leading financial institutions**. »We work together to design and deliver advanced distributed ledger technologies to the global financial markets.»
- Distributed ledger technology has the potential to **change financial services** as **profoundly as the Internet changed media and entertainment.**



The Banks in The R3 Consortium

Blockchain

Winner: R3 CEV

Parties involved: R3 CEV and banks: Banco Santander, Bank of America, Barclays, BBVA, BMO Financial Group, BNP Paribas, BNY Mellon, CIBC, Commonwealth Bank of Australia, Citi, Commerzbank, Credit Suisse, Danske Bank, Deutsche Bank, , Goldman Sachs, Hana Financial Group, HSBC, ING Bank, Intesa Sanpaolo, Itaú, JPMorgan, Macquarie Bank, Mitsubishi UFJ Financial Group, Mizuho Financial Group, Morgan Stanley, National Australia Bank, Natixis, Nomura, Nordea, Northern Trust, OP Financial Group, SBI Holdings, Scotiabank, State Street, Sumitomo Mitsui Banking Corporation, Royal Bank of Canada, Royal Bank of Scotland, SEB, Société Générale, TD Bank, UBS, UniCredit, US Bancorp, Wells Fargo and Westpac.
Technology providers: Eris, Microsoft, Ethereum, Intel, IBM, Amazon and Chain

Launched in September 2015, the strength of R3 has been in pulling together the largest global financial institutions to find practical applications for distributed ledger technology (DLT), commonly called blockchain.

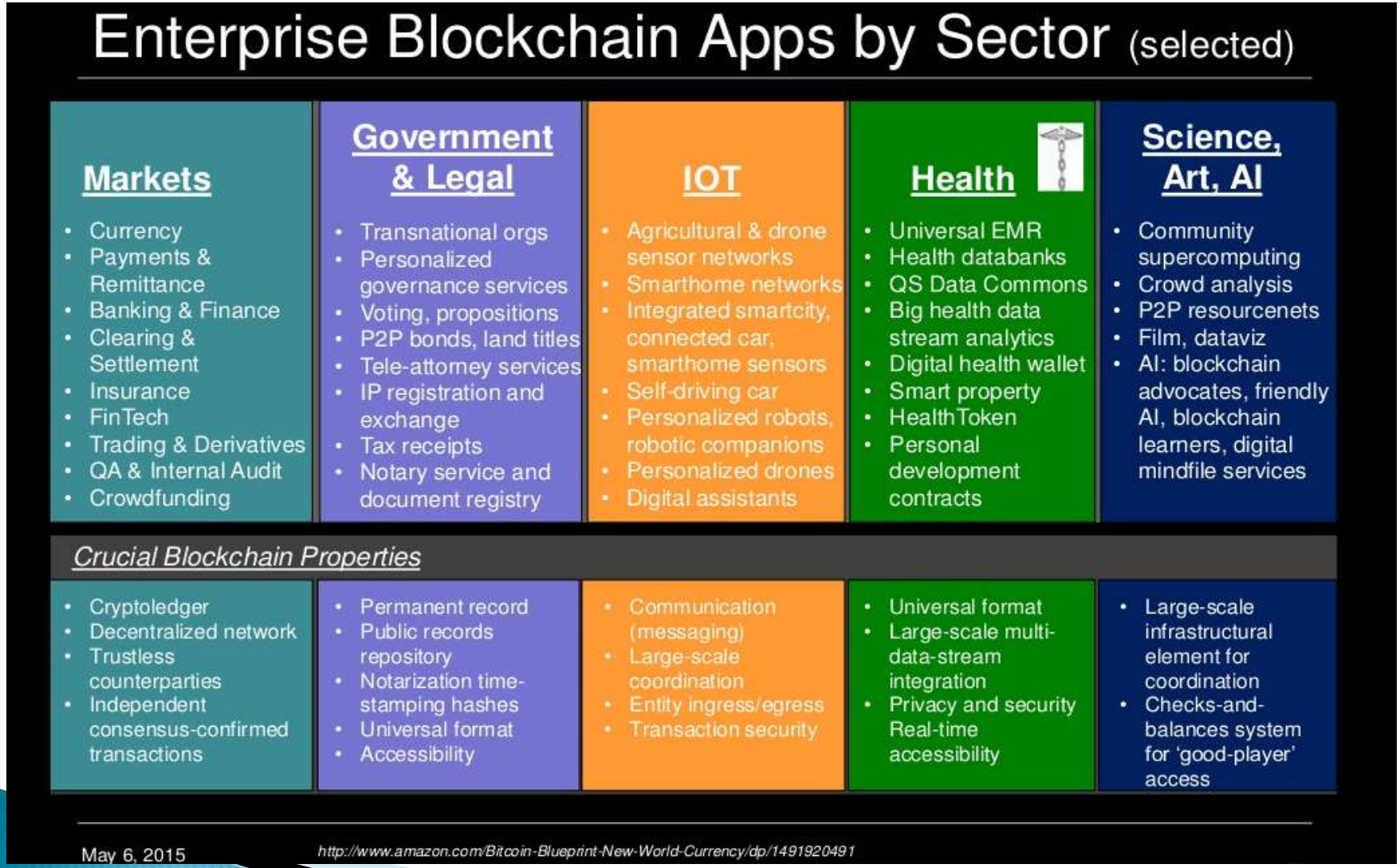
DLT, which grew out of the cryptocurrency world, is envisaged to transform how financial transactions are recorded, reconciled and reported, and in the process add greater security, lower error rates and realise significant cost reductions.

Rather than building a blockchain or DLT in isolation and then taking it to the financial community, R3 decided to work with the banks from the outset to identify specific industry issues and develop solutions accordingly – as well as increase the 'network effect'.

"We believe the key to developing these technologies in a way that would be meaningful and efficient was to work in collaboration with the industry, pooling resources rather than spending time focusing on individual projects that would then effectively require to be duplicated across institutions. Our members agreed with that vision and enthusiastically signed on," says R3 CEO David Rutter.

In January 2016, R3 and 11 consortium members ran their first trial, dubbed Project Zero. They connected on an R3-managed private peer-to-peer distributed ledger, underpinned by Ethereum

Enterprise Blochain Apps by Sector



Blockchain & the Financial Institutions

- 1. Bank of America
- 2. NASDAQ
- 3. Citi
- 4. Visa
- 5. Royal Bank of Canada
- 6. R3CEV

Blockchain's Capabilities

- Rethinking intermediaries
- Bundling services
- Unbundling services
- New flows of value
- Decentralized governance
- New legal frameworks
- Running smart contracts on the blockchain
- Sharing a distributed ledger
- Creating/Issuing digital assets
- Embedding trust rules inside transactions and interactions
- Time-stamping

Blockchain's Capabilities

- Implementing digital signatures
- Notarizing data/documents to produce proof
- Creating records of a business process, event, or activity
- Verifying authenticity of data/ownership/documents/assets
- Confirming authenticity of transactions
- Ensuring that contractual conditions are undeniably met
- Reconciling accounts
- Finalizing financial settlements
- Embedding digital identity in applications
- Providing escrow or custodial services
- Enabling smart things to transact securely

How do You Organize Internally?

- **Some companies are funding a "Blockchain Labs"** These labs typically have an internal focus to "show and sell," or educate the blockchain's possibilities to other business units and departments within the organization.

- **Some other organizations have formed an internal blockchain task force** comprised of the various business unit stakeholders, who meet and communicate on a regular basis.

- **Another approach is to discover ideas within the various groups via a common process,** but to develop the proofs of concepts for them in the labs, then proceed to implementing the best candidates with the business units.

What to Expect in Near Future?

- **What is certain is that the pace of activity around distributed ledger will continue onto 2016. We will see more established Financial Institutions and vendors announcing initiatives and will probably see a small number of early trial services in areas such as remittance and securities trading. While I'm sure we will get a greater understanding on the technical promise of the blockchain over the next 12 months I'm not convinced we will get clarity on one of the major outstanding questions, regulatory policy.**

- **A Very Big Development for Bitcoin is to add on the top of this as Japan governmental financial organisations consider to Make it a Legal Currency.** Will this make Bitcoin explode as one of the global biggest economies and currencies and take Bitcoin to a new legal, official credibility definition?


The Final

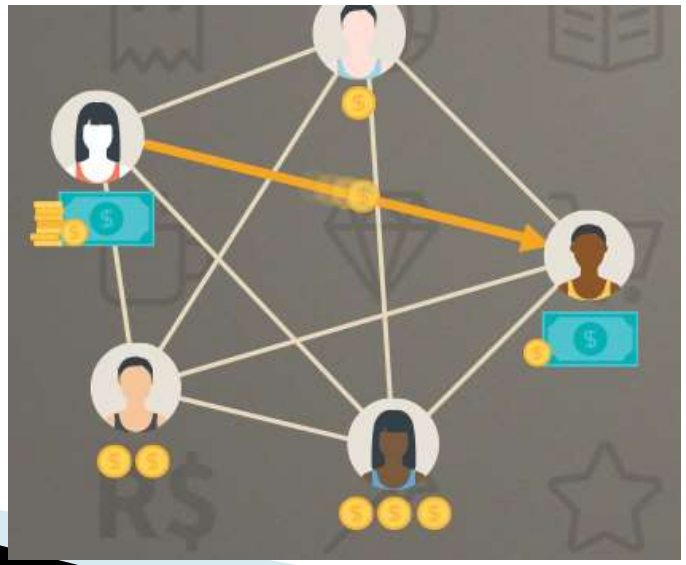
Get The Hands Dirty

http://www.multichain.com/getting-started/

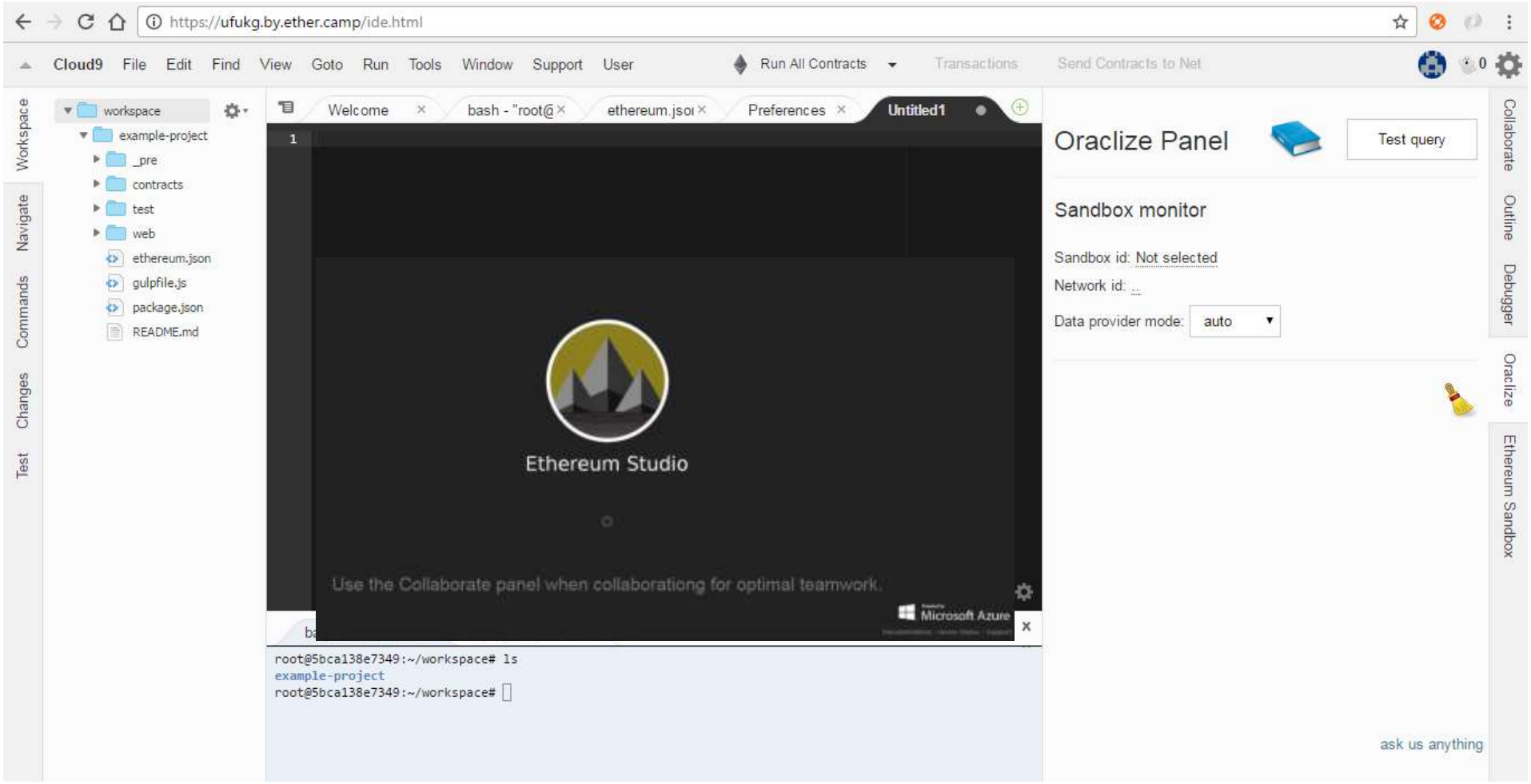
Open platform for blockchain applications

Download MultiChain

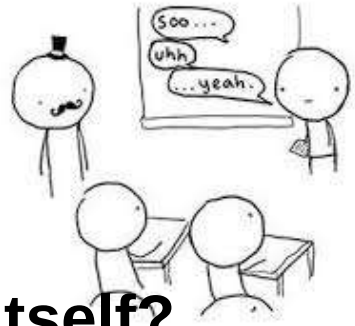
CREATE YOUR OWN CRYPTO-CURRENCY WITH ETHEREUM



Ethereum Studio



Conclusion



is It a Bigger Revolution Than the Internet Itself?

To me it shall be a big revolution (if it can evolve into a better direction), but not as big as internet itself though.

Shall It Ruin Banks!?

Though at the moment it is a very difficult question to answer whether it can ruin banks,

yes, it is possible, if the banks continue to operate as it is today, but it seems they shall dive into this bandwagon and don't let a new technology ruin them. But one thing is for sure, the life shall never be the same for the financial institutions, they need to adabt.

I think there is time for the blockchain's biggest promise to get rid of the intermediaries, since no goverment on earth would accept to give up any of it's controlling power.

Conclusion

The blockchain will redefine the role of existing intermediaries (if they accept to change), while creating new intermediaries, therefore it will disrupt the traditional boundaries of value.

How to Adopt Blockchain Development?

With the blockchain, one could adopt a **conservative approach and wait until the technology matures**, then get involved when all uncertainties are removed. As the saying goes, **the early bird would get the worm, but the second mouse gets the cheese**. **Some companies will undoubtedly follow that route**, **while others will be more attracted to being pioneers and innovators who are willing to trade risks for greater or earlier rewards.**

Final Words

- There seems to be a great potential in Blockchain that it can make a big change in life.
- Since it is not well known, nor a mature thing yet, everyone is trying to see what can be done with it.
- So, I think keeping the eyes on it and creating experimental projects to better grasp and see the opportunities it can create is the best thing to do at this point.
- Lets create an experimental project using blockchain technology.

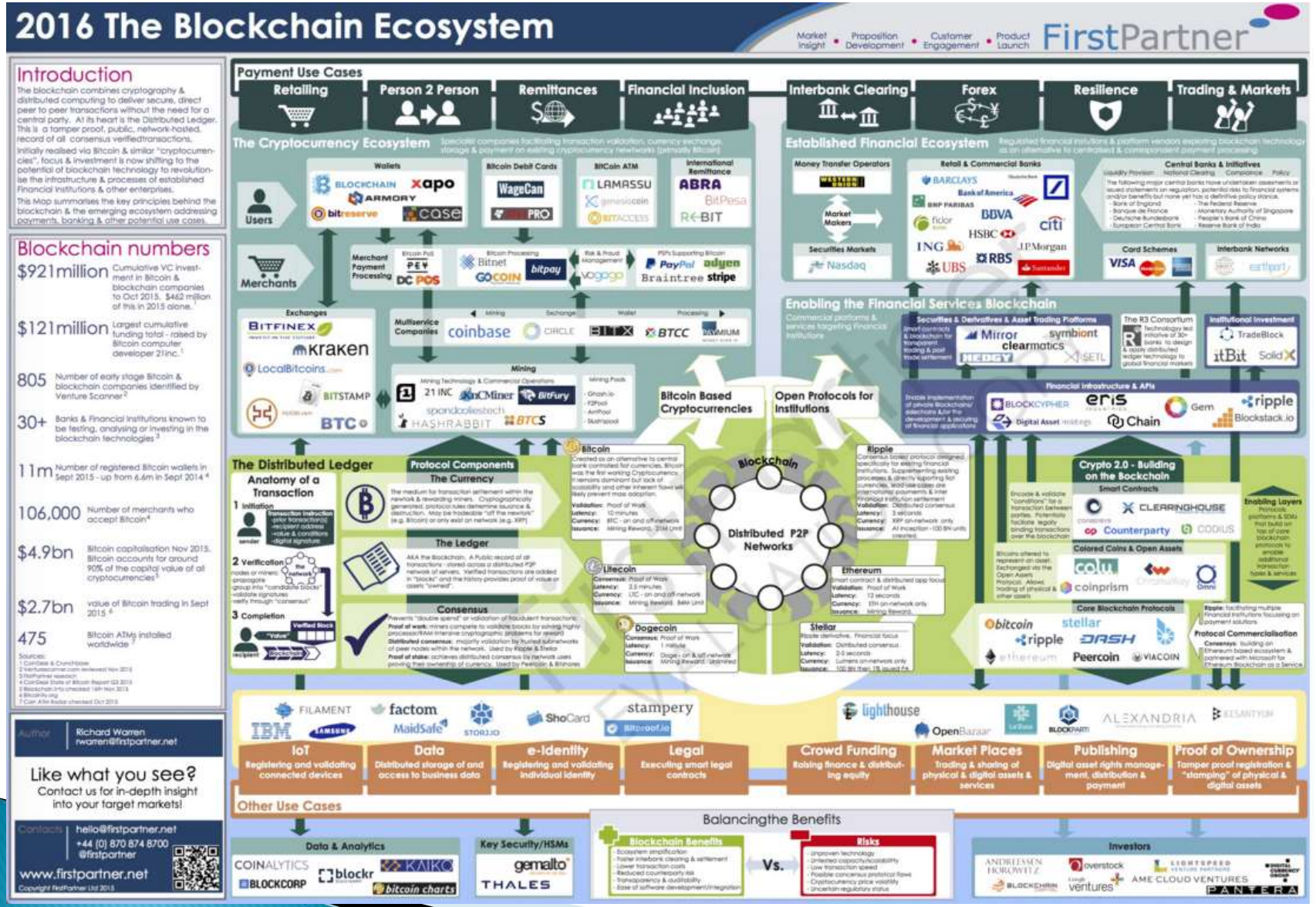
Questions & Answers

So, you still have questions huh? ☺

Appendices

The blockchain Ecosystem 2016

The Blockchain Ecosystem 2016



How are Transactions Broadcast to the Rest of the Network?

Generally bitcoin nodes will connect to at least 8 other (random) nodes. This is enough You pick geographically separate nodes to get a true sense of the network's state. Nodes are responsible for relaying information about new transactions and blocks to their peers.

Want More?

Please see the «Links & Videos Section» in «the Blockchain Document»

What is blockchain? (2 mins video)