

Blockchain Primer

APRIL 13, 2018

DAN DESKO, SENIOR MANAGER, IT RISK ADVISORY – SCHNEIDER DOWNS

Agenda

- What is Blockchain?
- What is Bitcoin?
- Blockchain in Financial Services
- Common Misconceptions/Myths
- Blockchain Challenges and Risks

Blockchain in a Nutshell



What is Blockchain

Blockchain is technology that enables shared databases.

What is Blockchain

*But this isn't your granddaddies' shared database. They enable a whole new kind of shared databases. With superpowers**

**Not really true, no superpowers are involved. Just a lot of math.*

What is Blockchain

So what makes it so special?

What is Blockchain

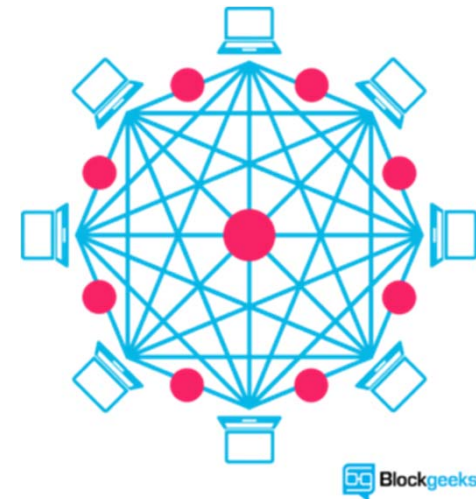
Traditional

Centralized Database Structure



Blockchain

Decentralized and Distributed Database Structure

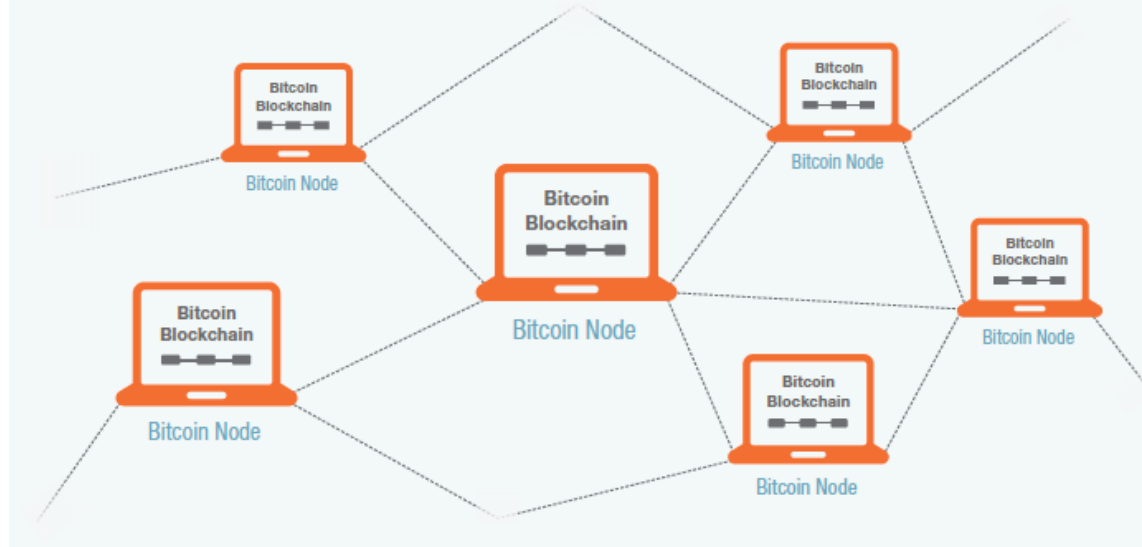


What is Blockchain

The Blockchain creates a peer-to-peer distributed and synchronized ledger, that is currently the foundation of the Bitcoin cryptocurrency.

Much of the context we will use today will be related to the Bitcoin Blockchain.

Figure 3—Bitcoin Blockchain Peer-to-Peer Network



© 2017 ISACA. All Rights Reserved.

What is Blockchain

Other Characteristics

- ✓ Transaction summaries are stored in a “block” which is essentially a grouping of transactions that is marked with a timestamp and the cryptographic fingerprint of the previous block.
- ✓ Chronological sequence of transactions, where each block of transactions is linked to the previous block.
 - ✓ Hence, BLOCKCHAIN...
- ✓ Cryptographically verified and sealed, essentially preventing future editing.
- ✓ Consensus based, a transaction on the Blockchain can only be executed if the network verifies it.
- ✓ Copies of the Blockchain and its underlying transactions are stored/distributed on every participant node.
- ✓ The destruction or hacking of one node cannot disrupt the entire network.
- ✓ Increased transparency, all transactions can be viewed at any time.
 - ✓ Try this Bitcoin Blockchain viewer: <https://blockchain.info/blocks>

BLOCKCHAIN

WALLET

DATA

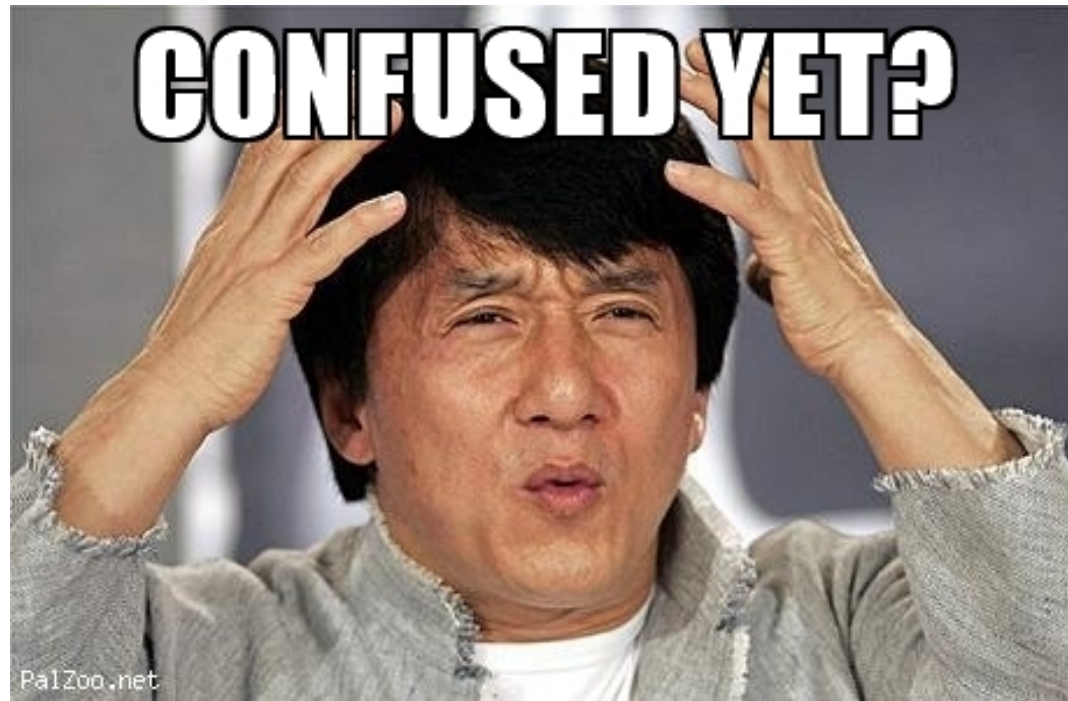
API

ABOUT

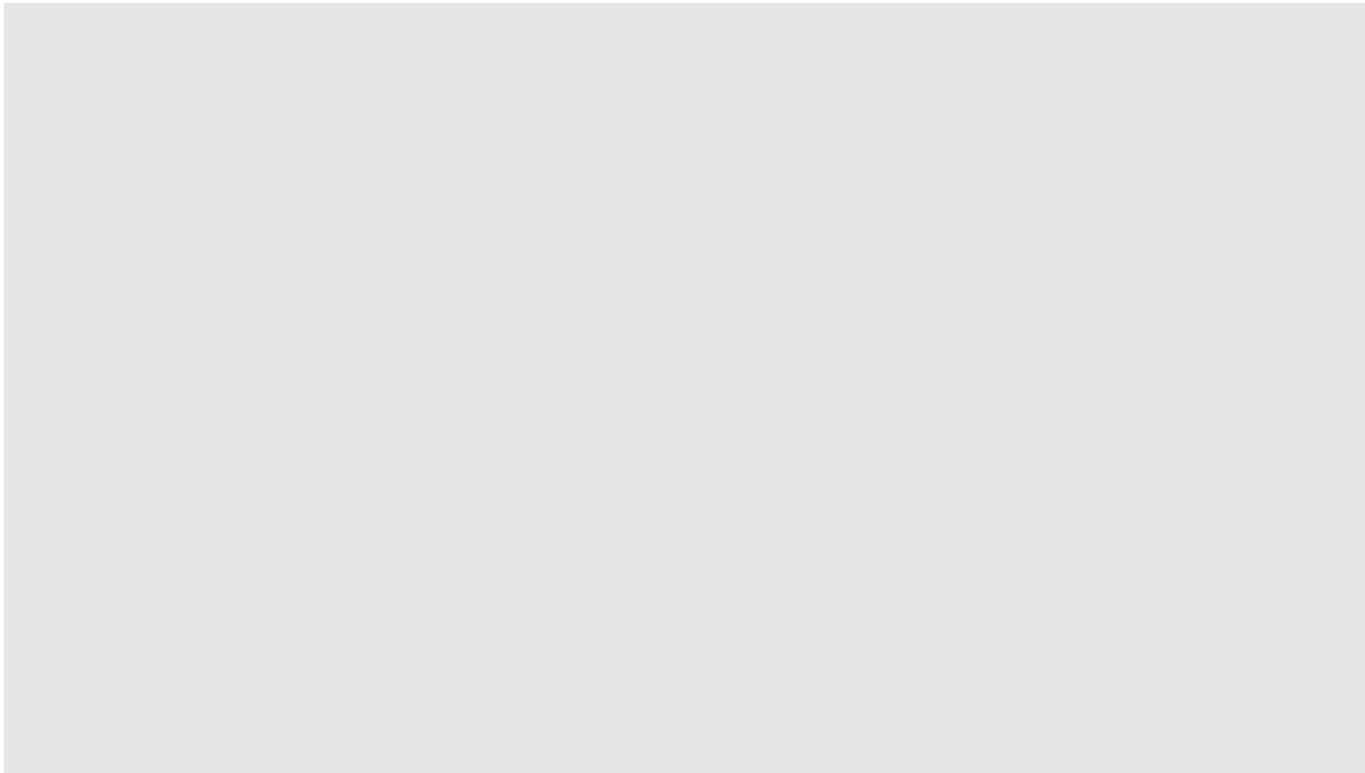
Summary	
Height	503260 (Main chain)
Hash	0000000000000000000000083435d70bf1c74e5ac023030b3ddcc3f422af2daeb4b75
Previous Block	00000000000000000000007979d7f1c6be97d32b19a0a5a957813d3c8232f9dd22dc
Next Blocks	000000000000000000000010ecd0940a4422cc83de9daf3cd8fd1139a18c60aa01df
Time	2018-01-09 01:27:10
Received Time	2018-01-09 01:27:10
Relayed By	BTC.com
Difficulty	1,931,136,454,487.72
Bits	402690497
Number Of Transactions	2768

- | | | |
|------------------------------|--|---|
| Output Total | 42,996.8793744 BTC | |
| Estimated Transaction Volume | 1,799.27057858 BTC |  |
| Size | 1057.367 KB | |
| Version | 0x20000000 | |
| Merkle Root | 0e85a73643c384f24d0ddb611783ce7b7967c6983a2b69bdfa2f71e59355485a | |
| Nonce | 1070444503 | |
| Block Reward | 12.5 BTC |  |
| Transaction Fees | 4.6844718 BTC | |

Let's Add Some Context



What is Bitcoin?



What is Bitcoin?

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.

- Not tied to any one political system, central bank or government.
- Virtual money used to buy and sell things, mimics real world resources (e.g. Gold).
- No need for an account at a bank, all you need is a smartphone with a Bitcoin wallet.
- Encrypted in a way that prevents it from being copied or spent more than once.
 - The Blockchain is essential to this.
- Transactions are recorded to the Bitcoin Blockchain.
- Owners have an address, which is a derivative of a public key (cryptographic term).

What is Bitcoin?

Bitcoin is being adopted worldwide and starting to be accepted as a form of payment by major corporations such as the below. However, there has been some trepidation due to recent price surges. Microsoft, which once accepted Bitcoin, has recently pulled back the Bitcoin payment option.

Bloomberg

 overstock.com®

 newegg®

 **zynga**®

 Expedia®

 dish

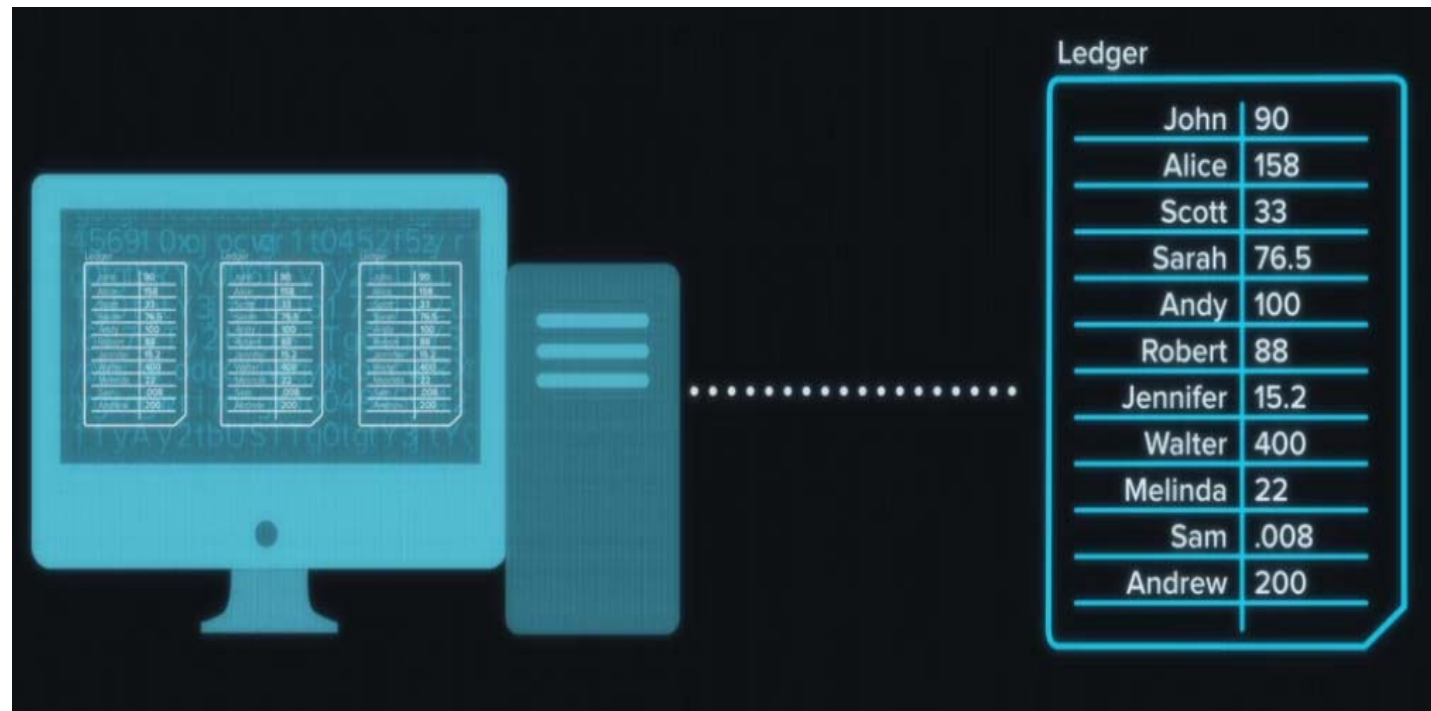
 eGifter

REEDS
Jewelers

What is Bitcoin?

Let's think of an example. Here is the traditional example of a centralized model, similar to that of a Bank.

- Every user has an account that has their account value tied to it.
- The bank is the central trusted source of this information.



What is Bitcoin?

With Bitcoin, that same database or ledger exists, however, rather than a name or account #, each person has an “address” which is mathematically tied to a private/public key pair, where the private key is known only by the owner and the public key is a derivative of the private key.

Ledger

1D1074B11625D	90
5EB639I34MS1P	158
Y33LX45-ONG2Z	33
A576BVB26UWB	76.5
2F72DKO83N4C	100
SG7PABE0682W1	88
D39HX251JF1M	15.2
K55X38K215Z9D	400
4Y10S3M6003U1	22
6CJ5R4451B19Z	.008
T238PX7051C1E	200

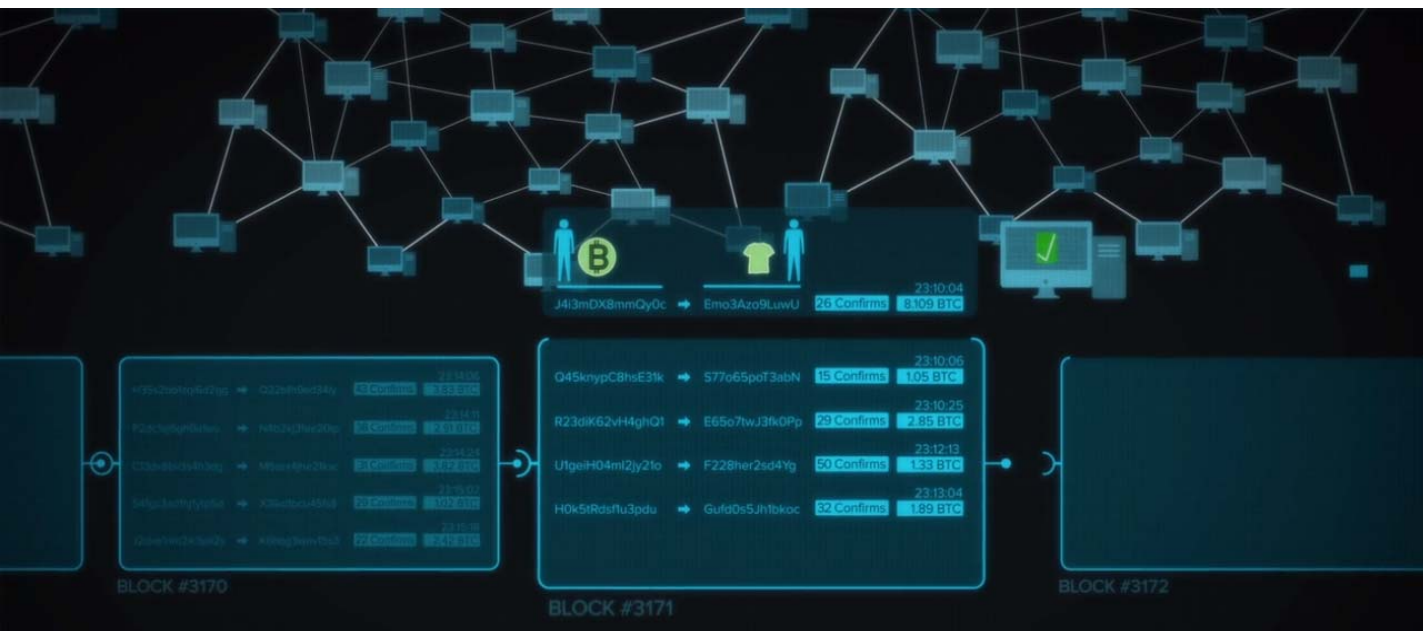
What is Bitcoin?

With the Bitcoin Blockchain, all the nodes in the Blockchain have a copy of this ledger.

- When transactions occur, “miners” verify the transaction through consensus. They conclude if the transaction is legitimate by verifying that the user saying they are spending/transferring a coin, actually owns that coin and has the right to spend it.
- There is no central trusted source of this information, it is distributed and open.
- Users remain anonymous as the cryptographic address cannot be tied back to them directly.



What is Bitcoin?



As transactions are verified by miners, they are added to a block within the Blockchain. The miners are simply racing to solve a mathematical problem.

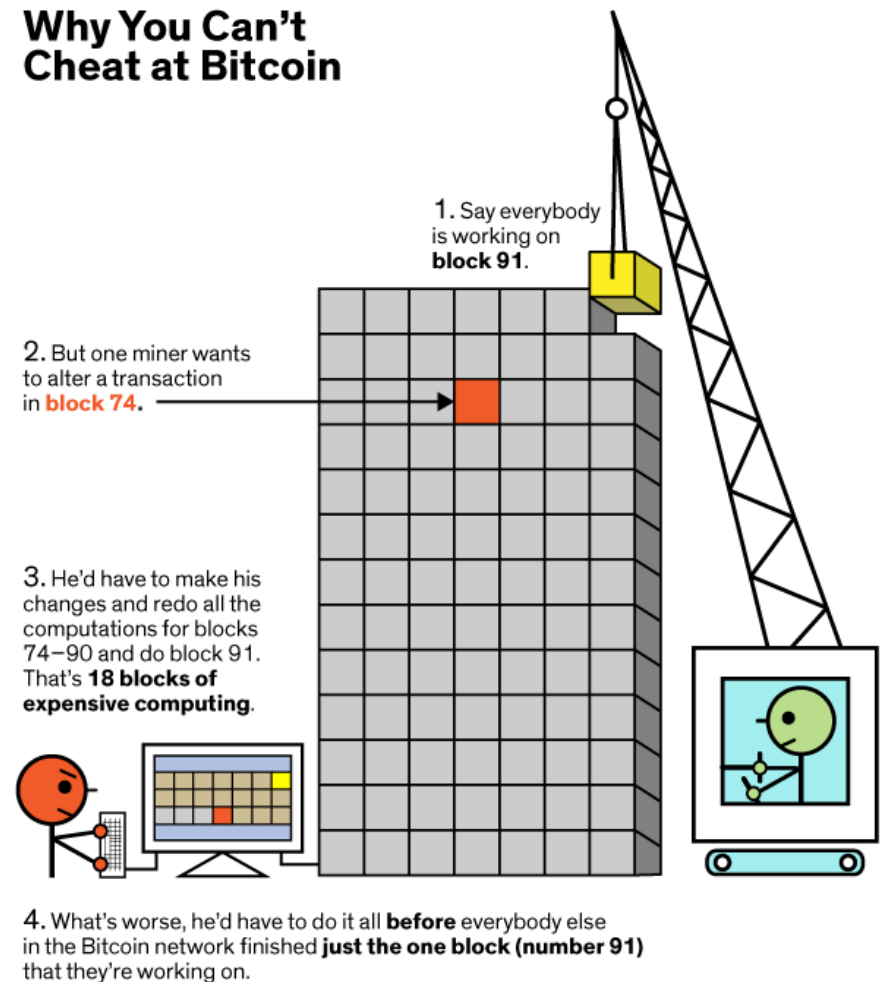
Once the block fills up with transactions, it is sealed with a one-way solvable cryptographic function.

The output of this function is then used to start the next block, thereby linking the block together in the chain, the BLOCKCHAIN.

What is Bitcoin?

The chaining and sequence of transactions is what makes it so difficult to cheat. The computational power used to create and verify these transactions is so great that it is said to be computationally impossible to go back and alter a previous block before the next block is written across all nodes on the Blockchain.

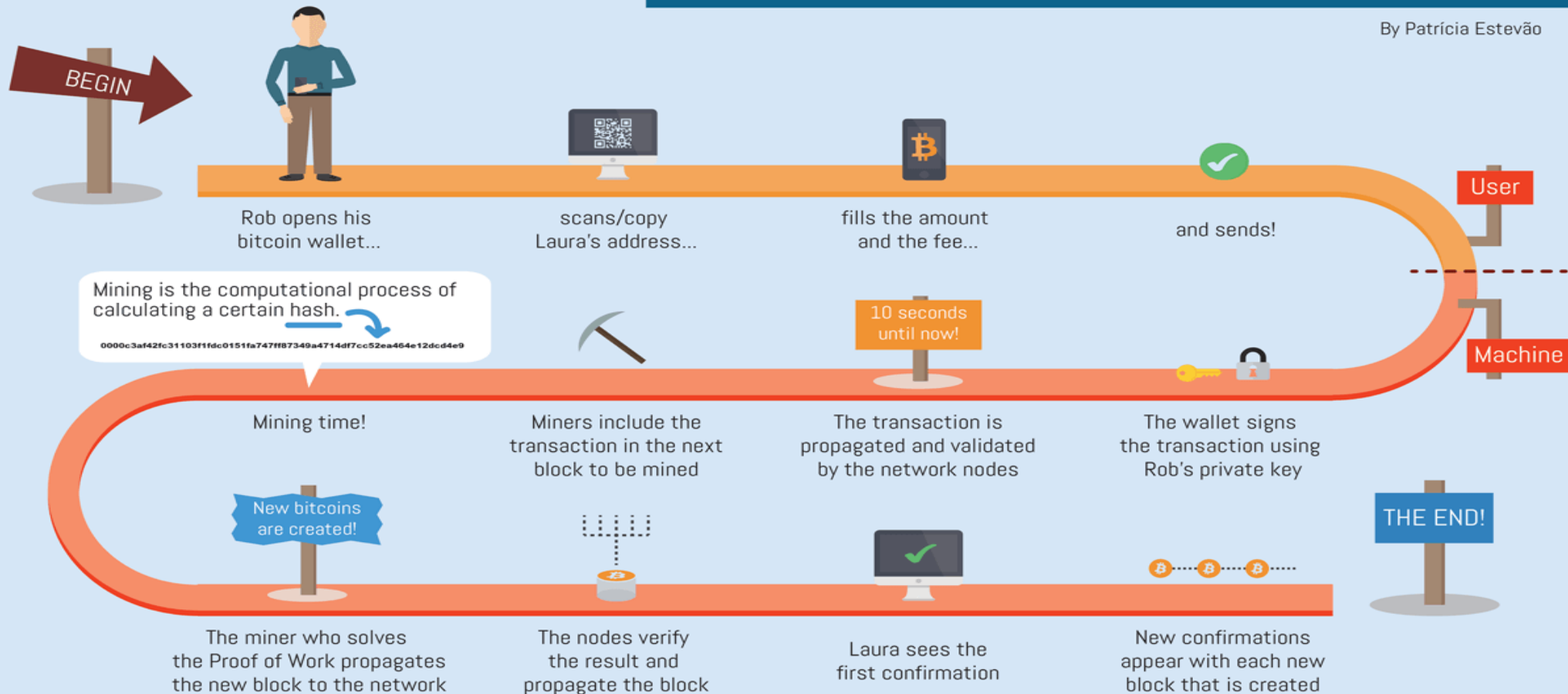
Why You Can't Cheat at Bitcoin



THE BITCOIN TRANSACTION LIFE CYCLE

Rob's quest to send 0.3 BTC to his friend Laura

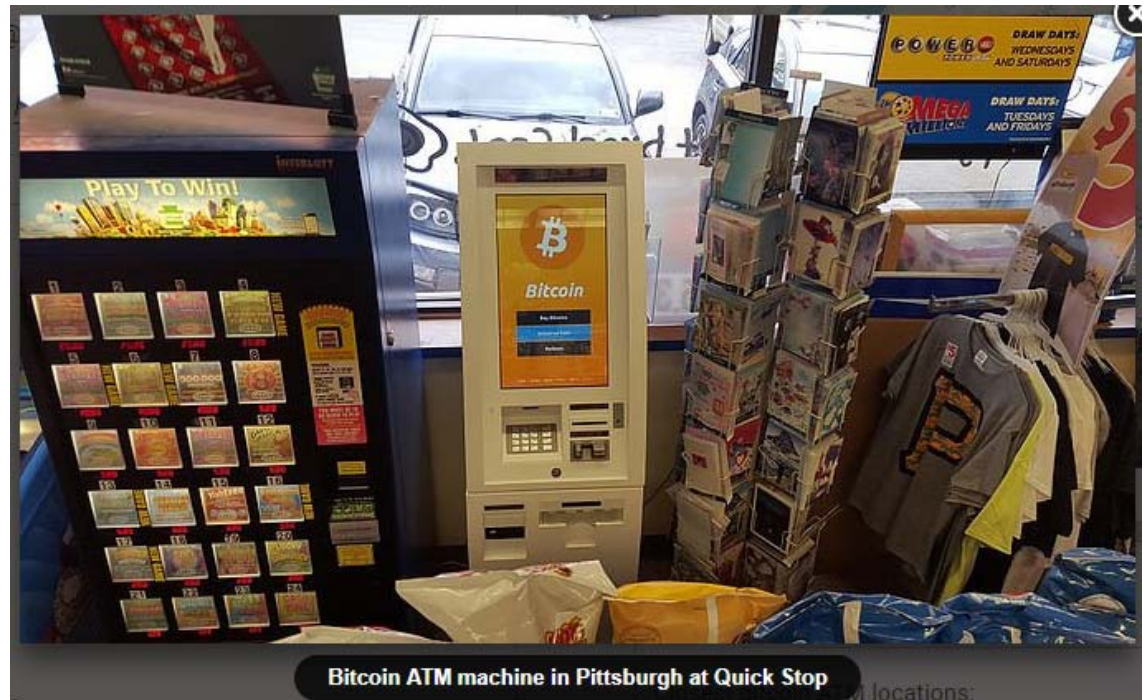
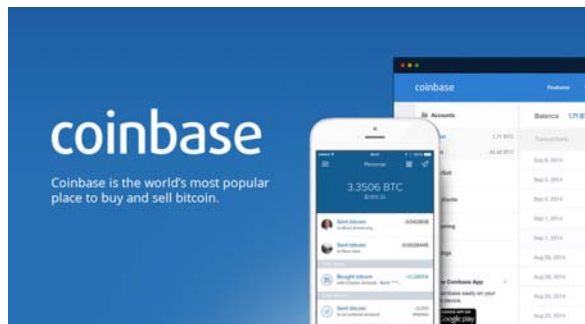
By Patrícia Estevão



What is Bitcoin?

Want to get Bitcoin?

- Insert cash at a Bitcoin ATM like this one.
- Alternatively, you can use a Bitcoin exchange to transfer dollars to Bitcoin. For example, coinbase.com.



Common Misconceptions/Myths

MYTH: Blockchain is the same as Bitcoin.

- Blockchain is the technology that enables the Bitcoin cryptocurrency. One cannot survive without the other however.

MYTH: There is one single/all powerful Blockchain!

- Sorry, there is no single “Blockchain” that holds all records of every transaction that ever existed.

MYTH: The Blockchain is immune from hacking.

- This is also false. The Bitcoin Blockchain cannot be altered so long as the good CPU processing exceeds the bad CPU processing. In other words, the majority of CPU processing on the network must be honest nodes, or else we are in trouble. This could change as computing power increases, e.g. quantum computing.

MYTH: Bitcoin and cryptocurrency is for thieves and miscreants only.

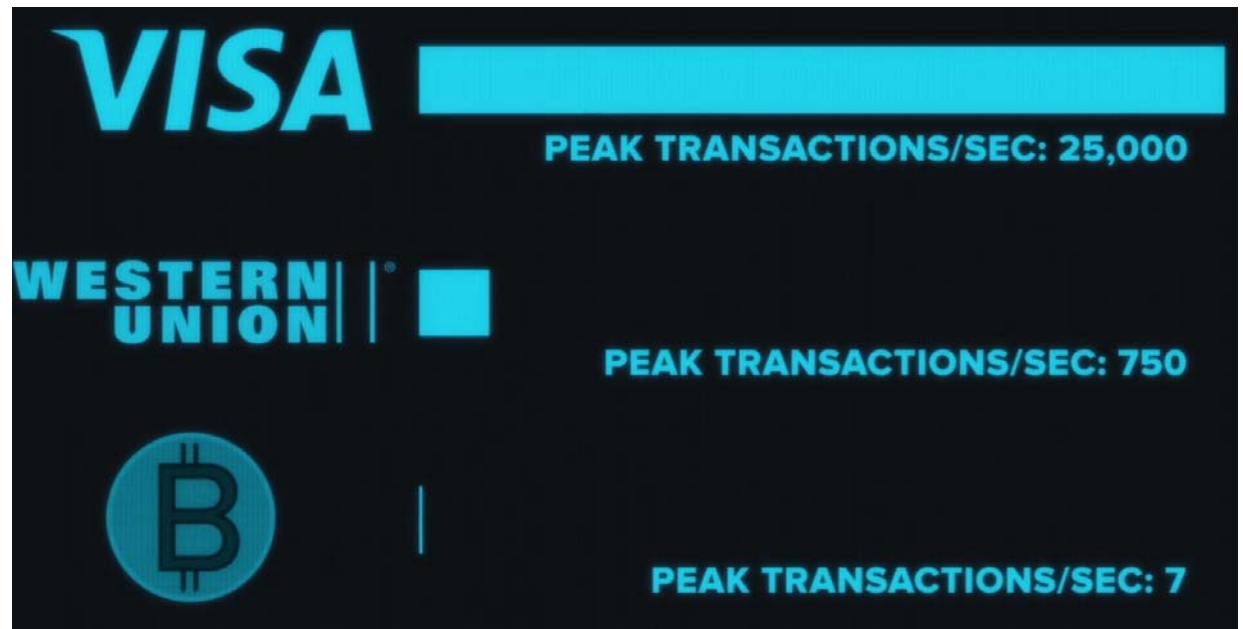
- Currency does not judge how citizens use it. And while some of the first uses were used for bad, not all is bad.

MYTH: The Blockchain can be used for anything and everything!

- Well perhaps, but does it need to be? In most cases a traditional database will do.
- The question to ask is: What is more important, transparency and disintermediation (Blockchain), or confidentiality and performance (Traditional Database)?

Blockchain Challenges and Risks

- Peer-to-peer networks have their challenges. They are often slow compared to other centralized systems.
- This will pose challenges to the Bitcoin currency in certain use cases, such as equity trading or retail transactions, as customers expect a much faster clearing time.



Banking on Bitcoin; Netflix.

Blockchain Challenges and Risks

- You need participation for a Blockchain to work, sometimes participation may not work if there is no incentive for parties to participate.
 - The miners doing all the heavy lifting ensuring the Bitcoin Blockchain works, they get rewarded BTC for doing that!
- The whole idea of the Blockchain is transparency, this causes a confidentiality problem. Imagine publically displaying confidential organizational transactions in a Blockchain.
- Well, what about a private Blockchain!?
 - The idea sounds great in theory, however, there are many issues in the implementation. Who will do the work? The Bitcoin public Blockchain requires something called “proof-of-work”. Essentially, a piece of data that requires significant computational time/energy to find. This “proof-of-work” is essential in the Bitcoin Blockchain, as solving this is essential to writing to the Bitcoin Blockchain.
 - Miners are rewarded for finding the “proof-of-work” with Bitcoin. This goes back to the incentive argument! There may be no incentives in a private Blockchain.
 - If the “proof-of-work” component is missing in a private Blockchain, you have nothing more than a distributed database!

Blockchain Challenges and Risks

- The technology is complex and there are very few who currently understand it. Similar to the .COM boom when the world had very few JAVA and HTTP developers, right now there are very few Blockchain developers.
- The regulatory landscape is a big unknown. The thought is that governments will find a way to tax cryptocurrencies or outright ban them altogether.
- Environmental concerns are abundant. As there is more competition on the Bitcoin network, Bitcoin mining becomes more difficult, by program design; and this consumes A LOT of power.
 - According to one widely cited website (digiconomist.net) that tracks the subject, the Bitcoin network is consuming power at an annual **as comparable to the power for entire country of Denmark**. By the site's calculations, **each Bitcoin transaction consumes enough to power to power a home for nine days**.

Crypto-Risk in Financial Services

Annual Report Quotes

Item 1A - "Risk Factors" includes information about the most significant risks that apply to the company or to its securities. Companies generally list the risk factors in order of their importance. In practice, this section focuses on the risks themselves, not how the company addresses those risks. Some risks may be true for the entire economy, some may apply only to the company's industry sector or geographic region, and some may be unique to the company.

WesBanco - "[B]anks and other financial institutions may have products and services not offered by WesBanco such as **new payment system technologies and cryptocurrency**, which may cause current and potential customers to choose those institutions."

Crypto-Risk in Financial Services

Bank of America

Geopolitical Risk - "Emerging technologies, **such as cryptocurrencies**, could limit our ability to track the movement of funds."

Increased Competition – "Further, clients may choose to conduct business with other market participants who engage in business or offer products in **areas we deem speculative or risky, such as cryptocurrencies.**"

Inability to Adapt – "In addition, the widespread adoption of new technologies, including internet services, **cryptocurrencies and payment systems**, could require substantial expenditures to modify or adapt our existing products and services...[cont'd]"

Crypto-Risk in Financial Services

IberiaBank Corporation

Our success depends on our ability to respond to the threats and opportunities of fintech innovation.

*"Fintech developments, **such as bitcoin**, have the potential to disrupt the financial industry and change the way banks do business. Investment in new technology to stay competitive would result in **significant costs and increased risks of cyber security attacks**. Our success depends on our ability to adapt to the pace of the rapidly changing technological environment, which is crucial to retention and acquisition of customers.*

Crypto-Opportunity in Financial Services

JP Morgan Chase's Quorum



Quorum™ is an **enterprise-focused** version of [Ethereum](#).

Quorum is ideal for any application requiring **high speed** and **high throughput** processing of **private transactions** within a **permissioned** group of known participants. Quorum addresses specific challenges to **blockchain technology** adoption within the financial industry, and beyond.

Crypto-Opportunity in Financial Services

JP Morgan Chase's Quorum

- Quorum is a consortium based Blockchain, meant for interbank payments, with the Royal Bank of Canada and the Australia and New Zealand Banking Group.
- Variation of the Ethereum protocol developed by JP Morgan Chase.
- Able to process dozens, to hundreds, of transactions per second.
- It is a private permissioned Blockchain, meaning that this network isn't open to all. It is also a consortium Blockchain, meant to be implemented between participants pre-approved by a designated authority.
- Prevents all, except those party to a transaction, from seeing sensitive data.

Crypto-Opportunity in Financial Services

The screenshot shows the GitHub repository page for `jpmorganchase/quorum`. At the top, the repository name is displayed with icons for Watch (252), Star (2,024), and Fork (405). Below this is a navigation bar with links for Code, Issues (67), Pull requests (10), Projects (0), Wiki, and Insights. A large banner for "Join GitHub today" is present, stating that GitHub is home to over 20 million developers and includes a "Sign up" button. Below the banner, a description reads: "A permissioned implementation of Ethereum supporting data privacy" with a link to <https://www.jpmorgan.com/quorum>. A series of tags (blockchain, ledger, privacy, ethereum, consensus, go) are shown. At the bottom, repository statistics are listed: 7,937 commits, 13 branches, 11 releases, 113 contributors, and the license LGPL-3.0. Action buttons for "Branch: master", "New pull request", "Find file", and "Clone or download" are visible.

jpmorganchase / quorum

Watch 252 Star 2,024 Fork 405

Code Issues 67 Pull requests 10 Projects 0 Wiki Insights

Join GitHub today
GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.
[Sign up](#)

Dismiss

A permissioned implementation of Ethereum supporting data privacy <https://www.jpmorgan.com/quorum>

blockchain ledger privacy ethereum consensus go

7,937 commits 13 branches 11 releases 113 contributors LGPL-3.0

Branch: master New pull request Find file Clone or download

Crypto-Opportunity in Financial Services

JPMorgan Reportedly Mulls Spinning Off Quorum Blockchain Project



Crypto-Opportunity in Financial Services



Ripple provides one frictionless experience to send money globally using the power of Blockchain. By joining Ripple's growing, global network, financial institutions can process their customers' payments anywhere in the world instantly, reliably and cost-effectively. Banks and payment providers can use the digital asset XRP to further reduce their costs and access new markets.



Questions

