TRENTON SYSTEMS®

Blogs by Trenton Systems

Blockchain Explained: The Complete Guide [2018 Update - Part 1]

by **Yazz Krdzalic**, on Apr 20, 2018 11:08:25 AM

It seems the web is flooded with questions around blockchain technology. Blogs, posts, articles, infographics, YouTube videos, you name it, all trying to answer one question: What is blockchain?

Based on last year's hype, you'd think that we already kn
but that's nowhere near the truth.

People are actually still confusing 'bitcoin' with 'blockchain'.

I intend to put a stop to the confusion, clear the muddy waters, and provide you with enough info so that you too can stand toe-to-toe with a blockchain expert and carry a conversation.

Here's what I'll cover in the first part of this series:

- Who started it all?
- What's a Bitcoin?
- What is Blockchain?
- Types of Blockchains
- Blockchain Use Cases
- What's next for Blockchain?

To answer these questions, let us first journey back through time.

Blockchain Genesis: The Beginning

Date: October 2008

Location: www.metzdowd.com

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

What is it? First ever cryptography whitepaper describing bitcoin digital curren

Author: Satoshi Nakamoto

This is the very first *known* post on bitcoin to hit the internet.

[*You can download the original whitepaper in PDF format at the bottom of this post*]

Who is this Satoshi Nakamoto?

A name without a face.

The true identity of Satoshi Nakamoto has yet to be revealed. Of course, if you want your article to shoot to the top of Google, simply claim to know Satoshi Nakamoto's identity. You should get plenty hits. **WARNING:** Your popular vote may plummet.

Once you start reading the story behind this mysterious man, it's honestly a lot like being a Gunter looking for Anorak's Easter Egg. #ReadyPlayerOneReference

How do we know Satoshi Nakamoto is a man, and not a woman, or some other life form for that matter?

Well, we don't.

But, on a Peer to Peer (P2P) Foundation profile - an organization that studies the impact of P2P technologies and impacts on society - Satoshi claimed to be a man hailing from Japan who was born on April 5, 1975.

Many coders have gone out and analyzed the data of 'his' activities, traced it back to time-zones only to find out the sleep patterns aren't 'normal' for a person living in Japan.

The frenzy continued as people dissected the language used within Satoshi's code as well as posts to virtually every online page Satoshi commented on, to definitively say, this 'man' is not of Japanese origin.

Whether or not Satoshi Nakamoto is Japanese, or a man, or is 43 years old is irrelevant. There IS one thing we can all agree on: Satoshi Nakamoto is a mysterious mastermind.

Upon creating the Bitcoin (and thus Blockchain Technology), he (or she, or they) made it open source.

Now, everyone contributes to making this revolutionary technology even better.

As of December of 2010, roughly 2 years after original release date, Satoshi Nakamoto gave all ownership of the Bitcoin/Blockchain world to the people and has been inactive since.

Thank you Satoshi.

Let's pause here to cover some basic terminology.

Let's start with cryptography.

Cryptography (aka. Cryptology) is a way of studying techniques for secure communication in the presence of 3rd parties or adversaries.

Let's try that in English: a way to keep your private communication out of the hands of unauthorized users.

Google defines it as "*the art of writing or solving codes*".

Here's an example to help you put everything into perspective.

> You and a friend make up a secret language that only the two of you understand. Next time, in the presence of others, you are able to talk openly about private matters without worrying about anyone being able to crack the code you two created. Essentially, you've practiced the art of writing and solving codes: cryptography.

Out of this, we can easily define 'cryptocurrency'. It is a digital currency that is encrypted. That was easy enough.

Now allow me to introduce a term that confuses most people today: bitcoin.

What is a bitcoin? It's the world's first decentralized cryptocurrency.

Wait, you mean to tell me bitcoin is not blockchain?

Correct - it's NOT blockchain...*but more on that later.*

In its simplest form, a bitcoin is a digital currency that operates in a financial ecosystem WITHOUT a central bank.

For this to make any sense, you must first understand how today's banking system works.

Here's your quick breakdown.

When you initiate a transaction using your debit/credit card, it communicates this desire to your financial institution (bank, credit card company, etc.).

Simultaneously, a computer code is activated to approve the transaction. It checks all accounts involved and available funds, the transaction takes place, and historical data is stored on the bank's server.

You can then log into your bank account and check your private ledger (recorded transactions) and view any pending or processed activity.

These activities remain part of your financial institution's database and these ledgers are reported back to home base: the central bank.

In the United States, we call it the Federal Reserve System (the Fed). It's an institution that manages our currency, interest rates, and much more.

Think of the central bank as the owner of our financial ecosystem. Therefore, each financial institution within our system must abide by the rules and regulations of the central bank - you and I included.

But, why? *I thought you'd never ask.*

As a people, we decided to put our trust in a central bank to keep our best interest as priority numero uno. Place a mediator between our transactions and things simply cannot go wrong.

[*enter stage right*] Financial Crisis of 2008.

The trust we placed into the current financial system deteriorated drastically since 2008. People and businesses alike began to question how to move away from a central banking system while maintaining our financial security and privacy as a top priority.

Back to bitcoin...

A bitcoin bypasses the central system and uses what we call a distributed ledger technology, or DLT.

I know what you're thinking: Why would I want my private ledger, all my top secret financial data, distributed?

It's not like it sounds - well...maybe a little...

Once you grasp this next concept, you'll understand the hype behind bitcoin and cryptocurrencies alike.

How a Distributed Ledger adds to your privacy

Imagine each transaction you initiate gets checked by multiple users on a network, not just by one central administrator.

No one person can alter your data since these users, located across various geographies, simultaneously confirm that your transaction has taken place.

How do they know it's me?

Your information is securely stored using cryptography and can only be accessed using digital keys and cryptographic signatures.

These keys are NOT stored on the network.

You hold full responsibility in keeping this information safe and sound.

What if I lose my key?

If you lose the key, you lose access to your account and all funds therein, no questions asked.

Part of what makes the Bitcoin so secure.

Where can I safely store my private key?

There are ways to store your private key in a 'wallet'.

A Cryptocurrency Wallet is a collection of private keys but can also refer to software that manages those keys on the distributed ledger network.

Either way, it's up to you to decide how secure you want t

This my friend, is what a distributed ledger technology (DLT) is all about.

A means by which a bitcoin (or any other form of cryptocurrency) travels from one user to another - using independent computers (called nodes) to record, share, and sync transactions to their respective ledgers for your security and privacy concerns.

[mind blown]

Now that I've touched on Bitcoin, Cryptocurrencies, Wallets, and Distributed Ledger Technology, I think we're ready to dive into Blockchain.

Blockchain Explained: What is Blockchain?

Since you've learned what cryptography, cryptocurrency, bitcoin, and distributed ledger technology means, understanding blockchain will be a breeze.

How so?

Here's a little test to prove to yourself how far you've come. Ready?

Blockchain is a type of distributed ledger in which transactions made (in Bitcoin or other cryptocurrency) are recorded chronologically (chained together) and organized into blocks.

Surprised by how much of that you actually understand? Great!

How does Blockchain work? Your very first Bitcoin.

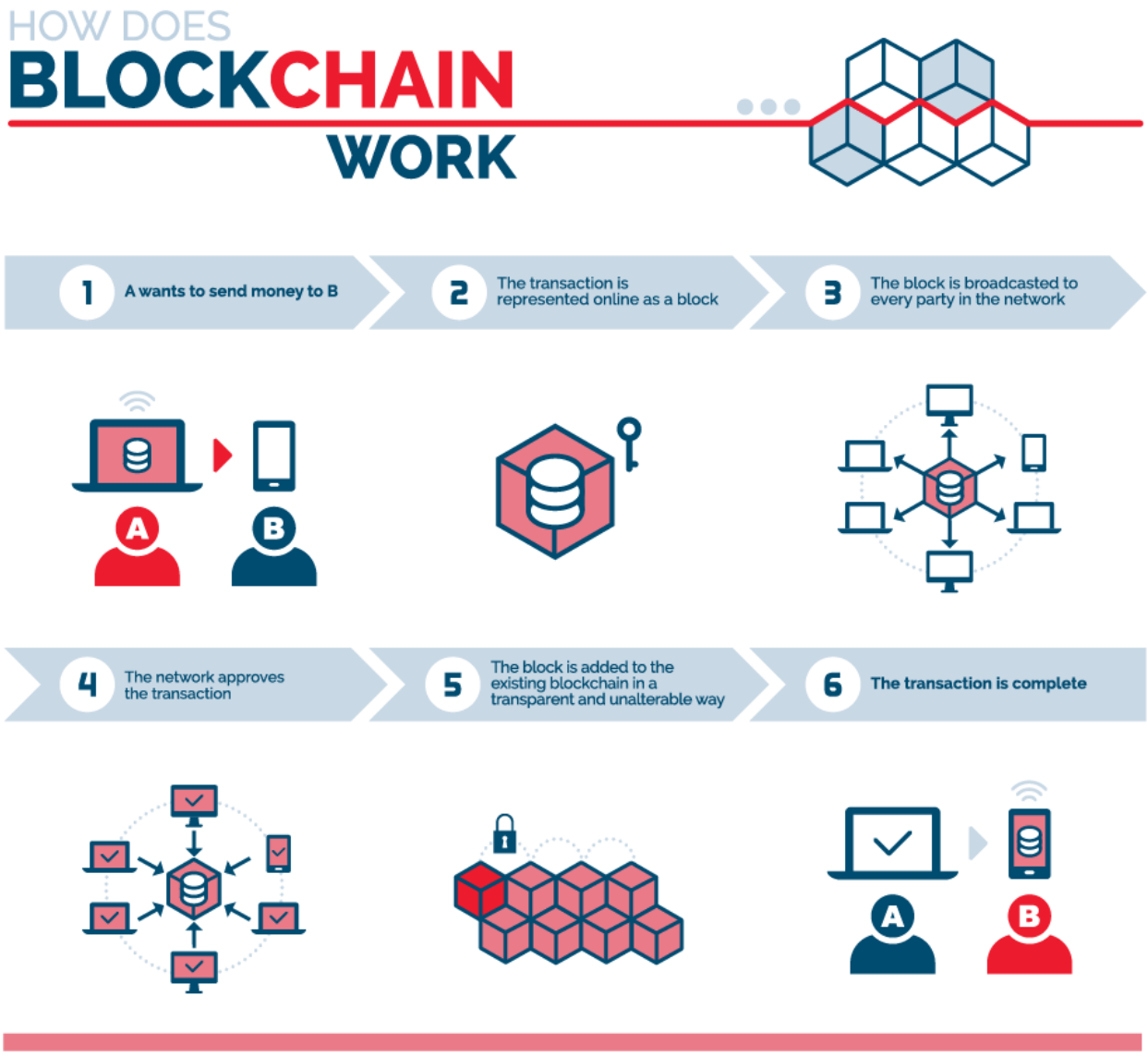
One of the best ways to understand how blockchain technology works is by an illustration.

My goal: Transfer 1 Bitcoin to you, the reader.

Cryptocurrency of choice: Bitcoin

DLT used: Blockchain

This is how our transaction is going to look like on the blockchain network.



You officially own one *imaginary* Bitcoin thanks to Blockchain Technology. Congrats!

Why Blockchain gets confused wit

Hopefully the example above gave you a basic understan
that it is the underlying Distributed Ledger Technology used to move a cryptocurrency (like Bitcoin) across a decentralized system.

Blockchain, in essence, is a network of computers that allows a Bitcoin to move from one person to another.

See, that wasn't too difficult.

Let's dig a little deeper to broaden our understanding on the types of blockchain technologies available.

Public Blockchain vs. Permissioned Blockchain

A traditional blockchain, the public blockchain, is a network where anyone can use cryptographic keys, their computer as a node in the network, and become a cryptocurrency miner.

These miners can join, leave, come back whenever they choose. Just follow the public blockchain rules, and you're good to go.

As blockchain technology use cases evolve from cryptocurrency to various applications (we'll cover this in a second), the 'public' feature of blockchain seems to become less appealing.

The solution? Permissioned Blockchain.

At the core, permissioned blockchain technology is identical to the public blockchain, with one added layer of security: access restrictions.

In order for you to join this network of nodes or make any changes within the network, you have to be granted special rights.

Think of it as a gated distributed ledger.

How a Permissioned Blockchain wo

Transaction validators are pre-selected, not just generated openly.

These validators are in charge of confirming transactions within a private blockchain environment. The same as miners *BUT* pre-selected.

Also, participants in a permissioned ecosystem can be restricted to perform any or all transactions within the network. Access is clearly defined.

Time for your second Bitcoin of the day.

I'd like to send you one more Bitcoin for making it this far in our blockchain lesson.

Since you are now part of a select few individuals, I'd like to invite you to join my permissioned blockchain network. It's an honor to have you.

As you enter your access code, my transaction validators will confirm your identity and grant access.

Once in, the same steps as before will take place.

Validation. Approval. Transaction Completion.

But before that happens, I decided that on my network, I only trust you to be the holder of this specific Bitcoin.

I agreed to only open this chain to you and noone else.

From this moment forward, the specific blockchain we are creating with our transaction is only visible to me, you, and the list of pre-selected validators.

Unless both of us agree to expand those rights to other p[illegible] party will have access to our blockchain.

Congrats! You officially received a special Bitcoin over a p[illegible]

Since the need for permissioned blockchain technology came about as use case[illegible] blockchain technology started expanding, it's only fair we discuss a few so you ca[illegible]

understand the global hype.

Let's discuss some non-cryptocurrency applications of blockchain

I held out mentioning one other key term in the cryptocurrency and blockchain world: Smart Contracts.

Until now.

In short, smart contracts are pieces of code on the blockchain that execute a contract between parties while also enforcing obligations.

It eliminates the need of a third party. YES!

Think about it this way, instead of waiting on a middleman to validate your contract then execute it (like a lawyer would), the code automatically has these conditions built into it.

It executes everything flawlessly without compromise. Plus it stores the history into the non-editable, highly secure blockchain so that you always have a point of reference.

Genius!

I am sure your head is spinning with the number use cases you can come up with where this would be useful.

Medical records, transferring deeds, food production, sup
banking...honestly any widget you can think of that is of i

But...

What are some blockchain use cases for 2018 and beyond?

#FinTech (Financial Technology)

Let's kick things off with the finance sector.

Blockchain technology is looking to streamline payments processing with ultra high efficiency. Not only within national borders, it also looks into to eliminating the known lag with cross-border transactions.

Blockchain in FinTech can minimize auditing complexities for ledgers across all financial institutions. The historical data built into the system allows for much greater insight into a transaction's history and status.

Ultimately, any individual or business would be able to send money anywhere in the world and it would take seconds. Compare this to today where it could essentially take days or weeks with regulatory bodies standing in the middle of our transactions.

We are currently working on a project that is poised to enter the FinTech sector.

For a behind the scenes look at the hardware running blockchain technology, check out the blockchain supercomputer in the making.

Medical

Picture all your health records stored securely on a blockchain netwo herever you go, you simply grant the medical staff access to your everything you have done in the past up until today.

All this without waiting on approvals, e-mailing copies, calling doctors that may no longer exist. Everything they need, within seconds, just like that (snaps fingers).

How many blockchain use cases are there today?

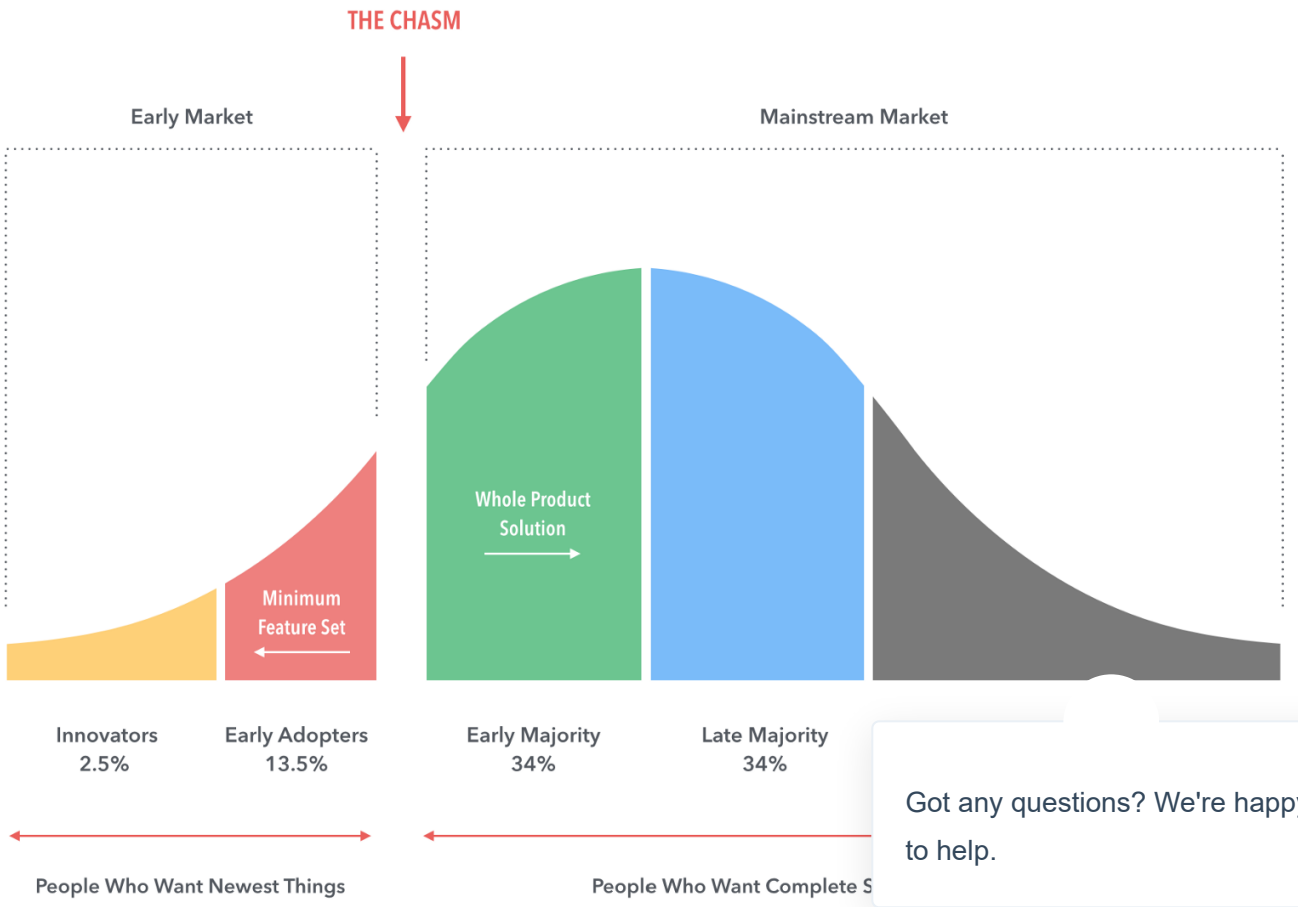
The list is growing by the minute. More and more people (and businesses) are buying into the technology.

When is blockchain going to take over the world?

Part of the problem with mass-adoption is the learning curve. There's a lot more to blockchain technology than Bitcoin. A LOT more.

We've barely scratched the surface in this post (of many more to come).

But to answer the question, I'd say we are in the early-adopters stage of the Adoption Curve. (see below)



https://www.google.com/search?q=adoption+curve&rlz=1C1SQJL_enUS787US787&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjtmIaAkcfaA8KHZKoBI8Q_AUICigB&biw=1914&bih=947

What does that even mean?

It means that we are on the brink of mass-adoption - the chasm (pictured above).

We have to first take care of a few roadblocks standing in the way, but once that is out of the way, we will be off to the races.

What can we do to speed things up?

Learn then share the knowledge.

It's part of my mission here.

I'm searching for all the information on blockchain technology I can find to summarize in bite-sized pieces for easy digestion.

This is a revolutionary technology poised to take global adoption, and I for one, want you to know what's going on.

Now what?

Knowledge is power and sharing is caring.

Leave a comment below. Share this post.

Teach us a thing or two.

Contribute.

Consider this your invitation to my permissioned blogcha

I look forward to learning from you. We all do.

Make sure to read Part 2 of the Blockchain Explained Guidebook!

Cheers!

Comments

Michael Thompson 4/25/2018, 4:15:04 PM

Interesting Stuff

Reply to *Michael Thompson*

akeo tech 10/30/2018, 3:35:40 AM

Very good post. It explains all the important points related to blockchain. Indeed a great post.

Reply to *akeo tech*

Solulab Official 8/27/2021, 2:32:27 AM

Informative!

Reply to *Solulab Official*

First Name*

Last Name

Email*

Website

Comment*

protected by reCAPTCHA
Privacy - Terms

SUBMIT COMMENT

Trenton Systems Blog

Our blogs cover the latest ruggedized computing news a

Got any questions? We're happy to help.

Recent

PCIe Gen 4 vs. Gen 3 Slots, Speeds

Huge List of Computer Stress Test Software [Rugged Computing]

PCI Express Interface

Topics

Archive

Subscribe to Updates

Complete the form below to subscribe to our company blog.

Email*

SUBSCRIBE

Got any questions? We're happy to help.

Trenton Systems

1725 MacLeod Drive
Lawrenceville, GA 30043
Call us: (770) 287-3100
sales@trentonsystems.com

Blog

Use Cases

Who We are

Careers

Rugged Servers

Rugged Workstations

Blade Servers

Storage Solutions

Subscribe to our blog

Email*

SUBMIT

Got any questions? We're happy to help.