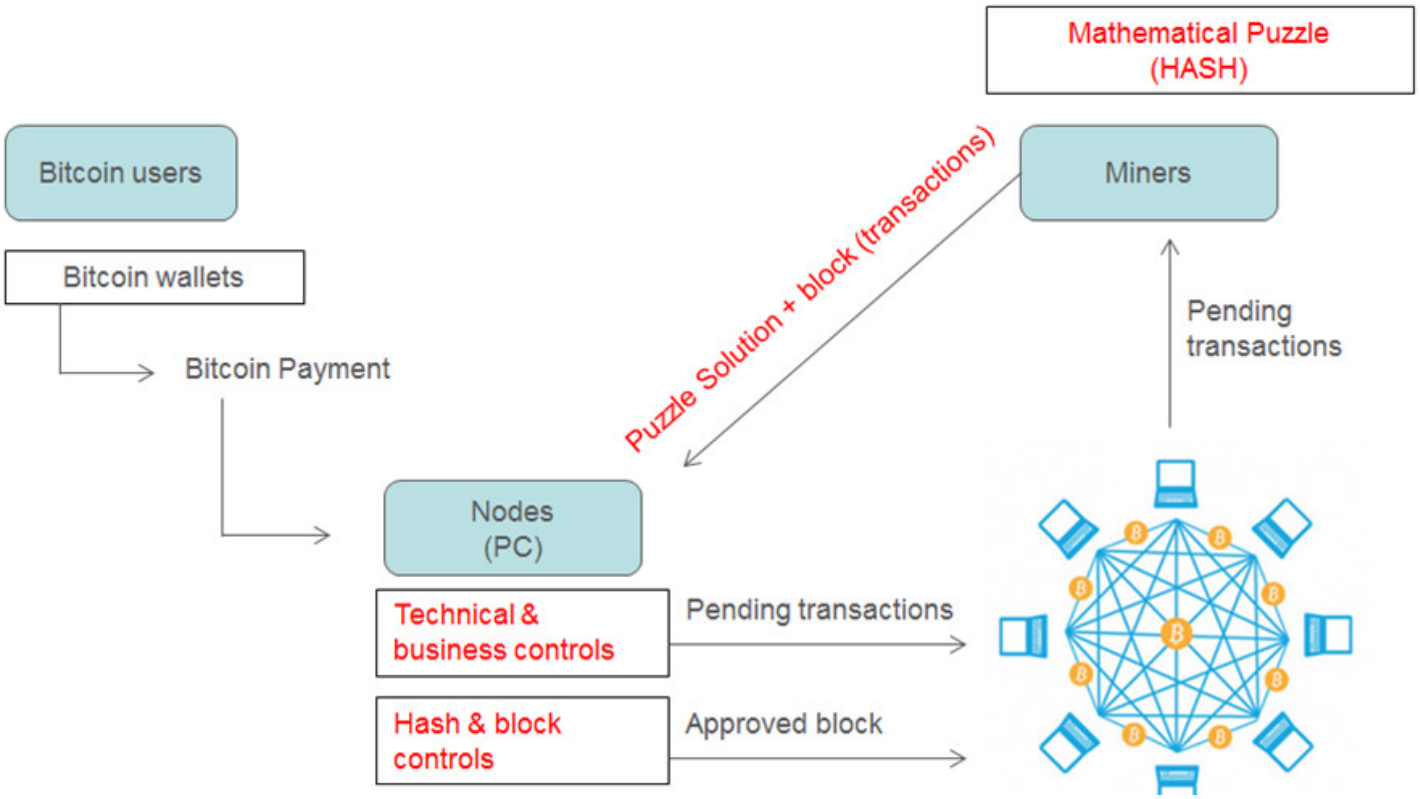


End to end Bitcoin Blockchain explanation with examples

Published on May 27, 2017

Onur Deler | Follow
Enterprise Architect at TEB (BNP Paribas JV)

379 18 109

Recent years' most popular question is "**What is bitcoin or blockchain?**" I was one of them that asking to google what are they? Working as business architecture, many resources about this new technology has been too technical for me. I had to drink a lot of coffee to understand them. By the way still learning process continues with the help of coffees. Best way of learning is to tell, try to describe. Hope these series of writing will make all of us learn more.

Generally in internet; before starting to describe bitcoin, first definition of money and later digital money, finally cryptocurrency is being told. There are great videos and essays that describe them, especially Andreas M. Antonopoulos videos are worth watching. For that reason I will just skip through and jump directly to our popular questions.

If internet was a country, bitcoin would be both its central bank and its currency. United States has dollar, Europe has Euro and Japan has Yen. These countries have central

issues its currency as Bitcoin.

> *In 2008 an unknown person with a Satoshi Nakamato nickname, publish an essay and bitcoin journey has started. IMO, Bitcoin has been created for one purpose and this is "no one, no central bank, no country, no dictator or a thing can stop me to spend my money"*

If I have 'a paper money' in my pocket, I can use it without asking any approval from any system to spend it. I would go to supermarket, restaurant or cinema and directly pay it with my cash. Directly, peer to peer, without any 3.party in the middle, without relying on any intermediary between me and the service/good provider. But rather than cash money, if I want to use any other 'paperless money', asking for approval of enough balance, limit or credit and asking for that I am eligible to spend my money. After a few seconds, if I get these approvals, I can do my transaction.

But for the first time, 'paperless money' behaves just like a "paper money" and this is Bitcoin. If you have bitcoin, you don't need to take approval from any intermediary to spend. This requirement would be only done within a system where there is no intermediary.

But how bitcoin is different from other paperless money? What makes it so special? Is a new technology created for that? Bitcoin uses existing technologies; it gathers all these old technologies together and names it blockchain. In fact, name would be the 'distributed ledger technology'. But as I said, it will be series of writing, and it would be unfair to use many unknowns at first article. Clarification will be done later.

So if bitcoin uses existing technologies under the blockchain name, why we have waited it for such a long time. Because, those existing technologies are like lego pieces and no one has been used legos to build a car before. Well, in fact legos have been used before to build a car many times. Bitcoin is not the first cryptocurrency, but it is for the first time going on the highway with other cars. It is the first time bitcoin; our precious paperless (cryptocurrency) money can be used like a dollar, euro and yen.

So asking the same question, "**how bitcoin is different from other paperless money?**" Let's take one step into details.

There are central banks, local banks, Swift, MasterCard, Visa, Facebook, Airbnb or any other intermediary in the middle. There are, because we need them, because we need to trust someone to hold our money or our data securely, because we don't trust each other. So if there is no trusted intermediary now, who will we trust? The answer is no one!

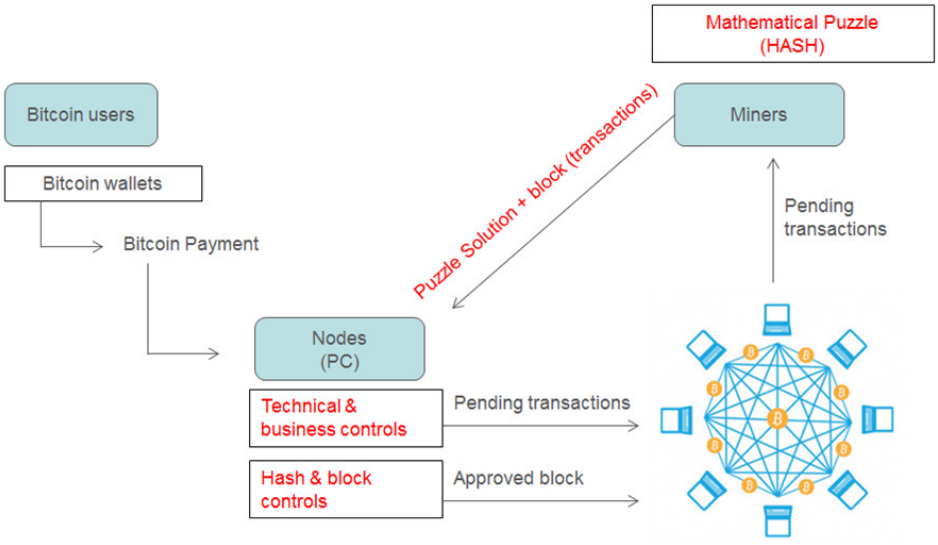
technology aka blockchain.

Our trust need has not changed, but also we want more. New request is “no one can stop me to spend my money”, remember? So we have requirements. Clearly, what are those requirements? Are these requirements doable without a trusted part? Let’s write the requirements step by step and later answer them in blockchainish.

Here are some quick questions we will cover now:

- Would not there be a double spending if there is no centralized structure?
- So there will be no bank. Who will securely hold my money, data?
- Will it be spread to all over the world? Same data is everywhere. Is my account info on someone else's computer?
- Is it really the correct person, who spends the money?
- If the transaction is held on someone else's computer, what if they change the transaction data later?
- How will blockchain know that I have enough funds in my account?

To answer them all, first let’s look at the big picture. Later on find the answers.



This is the big picture of bitcoin blockchain. Also there are different types of blockchains which are configured for different purposes.

In bitcoin blockchain, there are 3 different roles.

- Nodes,
- Miners.

It is free; you can be any of them or all of them. There is no restriction.

Bitcoin users have bitcoin wallets. There are many different wallets on internet; you don't need to share personal information to have it. It is free; you can have as many as you want. There is no limit.

When you have a wallet, you can do a bitcoin payment transaction. But where did this bitcoin come from, how do you have it? Short answer is; miners are creating bitcoins and you can buy those bitcoins on internet by exchange. As you exchange your dollar to euro, there is no difference.

Wallets are like mobile banking app, and they hold passwords for you to use the bitcoins. When you do a bitcoin payment, you send the transaction order to the nodes.

What is a node?

Nodes are just a PC, and their owners are the only volunteers in that system. So far there are around 6000 nodes all over the world. Their owners are the people who believe in bitcoin philosophy. If these node owners are not miners at the same, they are just volunteers or revolutionary, they are doing it for free.

When a node receives an order, they do many controls and check that if this transaction is valid, like banks do it now. If transaction order is valid, they send it to other 7 nodes to check it, too. In a few seconds, this transaction order spreads all over the world to 6000 nodes.

Ok, now I do bitcoin payment from my wallet and send it to 6000 nodes. This transaction order status is pending, waiting for miners to work on them.

What is a miner?

Miners are just like gold miners, they are working hard to find the gold. They are creating money from thin air but not thick rocks. Bitcoin miners don't dig, but solve mathematical puzzle called hash puzzle. (Will explain later)

Miners are listening to the bitcoin blockchain and they are collecting those pending transactions. They can select any transactions from that pending transaction pool, but there is max 1 mb size limit. All of the miners may have different set of transactions. The miner who solves the hash puzzle first, shouts "I FOUND IT, I FOUND IT!!" and broadcast to all network.

of the puzzle, transactions themselves, signatures, version numbers, etc. This is a trustless environment, no one trusts to each other. For that reason, everything like transactions, their signatures, puzzle itself, block size and many other controls are being done. These controls are being done by every node. This means, one block is being controlled by around 6000 nodes.

When a node approves the block, saves it. That event is continuously being done in every 10 minutes. When a block is saved in node, it attaches to the previous block which was saved 10 minutes ago. Saved blocks are creating a chain, blockchain. After a block is saved and added to the chain, you cannot change even one dot, one character inside it. Otherwise all block integrity changes.

This is the all process for the above figure. But still questions haven't been answered, yet. It is time to answer the questions! First questions for the client side.

How my account number will be created? Who will create it?

Bitcoin is a self-service system. You will create your address. There is no identity control, just connect to internet, and download your bitcoin wallet, and click the button "create an address"

Address will be your account number. When you click that button, you will have 2 long string. One will be your address (account) and the other will be your private key (password).

Do I need wallet for creating an address and private key?

BITCOIN WALLET	
Address	Private Key (usually hidden from screen)
1KrieA3KyYVrLJbSynkML9rriBLZpkPvDR	5J7ZWKWJE1fMSjQSTyeBqD4cxickKKA7xFdYHZDeXVbmoPBLrey
1KKGgesMtkWW52SEyd88kBkSijhVps7nJJ	5JwGTvMJumhMtxNBSj5QdYZVSck5W8PqAC5mtEUnRA1xHpL9g5x
14wKRvadKMq6Lthg9HAic5iebKWGSY2w75	5JphsyRvz3Goves7GVzntJ4bVpTWnmExXsjK3fHe6zhRqrgZoDT

This figure is copied from https://bitsonblocks.net, there is great info, worth to visit.

No, but you need to enter the private key when you do a payment. Wallets make you define your own password, as facebook does. Instead of entering around 50 characters, you can use your own 8 chars. password. Private key is not changing, but wallet makes you feel as it does.

Don't lose your password or private key. There are different algorithms for securely storing your private key. But usage is not simple yet. If you lose private key, you literally lose.

There are many wallets on the internet, What if 2 different people have the same address? Who is controlling the uniqueness of the address - "account numbers"?

world, even, the probability is less than this. By the way, wallets are the weakest point in this system. For that reason, generally hacking events are being around the wallets.

Where is my money, does wallet hold my balance, total amount?

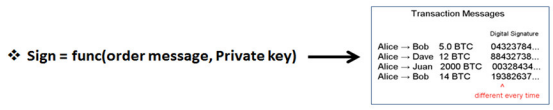
No, wallets don't hold your balance. By the way, there is no balance field in bitcoin, just there are transactions and transactions are held in nodes. (Explained later) Wallet makes you see your transactions, as if you see your balance. It makes your life simpler with its user friendly interface.

Ok now, let's ask some questions about transactions and security.

So I open my wallet, create a transaction order, and send it to 6000 nodes. Can they change my transaction order and distribute it to the network?

Today, I will answer it **"No, they cannot change it."** Later in the coming essays; I will mention about transaction malleability and segregated witness (segwit). But it is so early for segwit, now.

During your payment, you sign your transactions. There is a sign function. You create your message order; "I send Alice 0.5 BTC" and sign with your private key aka password. Wallets do it automatically and send it to nodes.



When nodes receive your order, they verify your sign. All nodes have a verification function. Nodes receive 3 data; your message order "I send Alice 0.5 BTC", your address and your digital signature. Nodes put all these data into the *verify function*. If it is not verified, it means that someone has tried to change your message order. Gotcha!

1 = ? verify (order message, address, sign)

- The same signature cannot be used to verify a different transaction!
- The slightest change in the message will invalidate the signature!

How will we know if there is enough balance in my account?

As I said before, there is no "total balance" field in bitcoin blockchain. In the account view, the "total balance" is calculated instantaneously. Let's look at the below example, I want to send Alice 5.5 BTC. To do that payment, I will use my unspent transactions (UTXO – unspent transactions output) :)

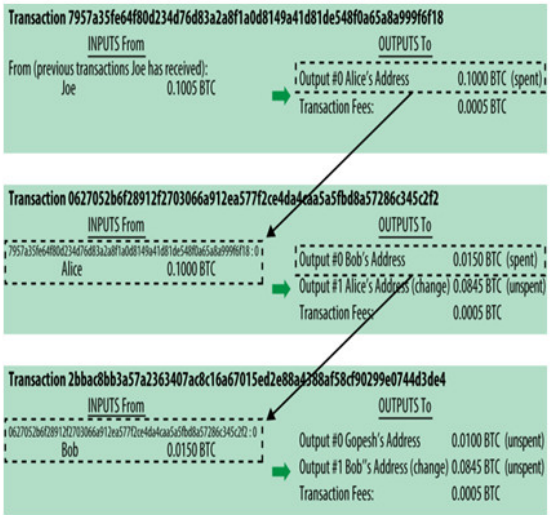
only use your unspent transactions which you have received before.

If I want to send Alice 5.5 BTC, I need to use my transactions, which have been sent to me before. When I calculate my balance instantaneously, I come up with 6 BTC. I had to use 5 transactions to gather 6 BTC. When this transaction is done, it means that I cannot use these 5 transactions anymore. By the way, at the right side of the below image, there are 2 addresses. One is Alice's address and the other is mine. So in the future, if I need to do a new payment, I can use this unspent transaction output aka UTXO.

Input and output totals are equal. If output total is less than 6 BTC, the difference would be a transaction fee for the miner. Be careful, blockchain is immutable, once it is gone, it is gone. You cannot take your money back :)

What if I insert a made up transaction, and use it to fool Alice?

No, it won't work! This is a trustless environment, no one trust each other, only trust themselves. For that reason, all nodes do controls by themselves.



When I use unspent transactions in my previous payment, nodes control them if they are really unspent. They also control, where that transaction is coming from. Even pre-previous transaction is being controlled, if it is valid or not. This control continues to the origin of that transaction, till to the genesis transaction! Sounds paranoiac, right? Well, you will be paranoiac, if you don't trust anyone! This can be called transaction chain. So it is impossible to insert a made up transaction in the middle. Even if you update all the history records in all 6000 nodes with a virus, it will not be enough. If you change one point in a block, its integrity totally changes. Just remember from Indiana jones, he takes one piece in a temple and in

it collapses.

This traceability feature is important, for the coming essays we will use this for different use cases.

How double spend control can be done?

Example: Let's look at the below example.

- I buy an ipod from Alice and pay the price with Bitcoin.
- Alice sends the ipod.
- Meanwhile, I create another order using the same transaction, and this time I send bitcoin to my second address.
- Finally nodes are spread to all over the world, one is in China, and the other is in Norway. For some nodes, the second message will arrive before the first one.
- Which transaction will be true?

Well, this answer needs a sub title. Because it will be take some time to answer.

Reconciliation in Bitcoin – Preventing Double Spend - BLOCKCHAIN

This figure is copied from https://bitsonblocks.net

We need a system that every node will agree on the order of transactions take place. Transactions in the same block are theoretically considered to be occurred at the same time. Every miner on the network can create a block from pending transactions (unapproved) transactions.

Questions again, **which block should be added to the chain?**

Answer: The miner's block, who has solved the hash puzzle first, will be added to the chain.

What is a hash?

The SHA (Secure Hash Algorithm) is one of a number of cryptographic hash functions. A cryptographic hash is like a signature for a text or a data file. SHA-256 algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one way

http://www.xorbin.com/tools/sha256-hash-calculator)

SHA256(Monday):
d618fb157a4b382e92fcd4a830c5fa8adef45a809543c524f7904e38f867dac8

SHA256(Manday):
0fdf06beb5d6547f70259bc47bb6de97d884655996f83632492bad5d4960c4f3

As you see above, one char difference changes the all hash output.

In Bitcoin blockchain, inputs used in hash functions are:

- Transactions take place in the block. *(In fact this would be the root hash of the merkle tree of all transactions in the block)*
- The hash output produced for the previous block called **block fingerprint** *(That piece is important for immutability)*
- A randomly chosen number aka **nonce.** *(This is the only number we will update during the puzzle solution.)*

What is a hash puzzle?

Miners are racing. The output of hash is totally random number. The puzzle is to find the 'hash output' below a certain number. Until to reach below that number, you continuously change the ***nonce*** number; perhaps million or billion times. Well this is random number, perhaps you are very lucky, and when you enter the nonce number, will find it at your first trial. But generally, people are not that much lucky.

Puzzle solution (hash output) <
000000000006547f70259bc47bb6de97d884655996f83632492bad5d4960c4f3

Puzzle is difficult and costly to solve. To solve the puzzle, miners are working really hard. For that reason, it is called proof of work.

- During mining in 2008, more electricity was consumed than in Bangladesh.
- It is stated that in 2020 there will be more electricity consumption during mining than in Denmark.

What if two miners solve the puzzle at the same time?

If there is such a case, it is called fork. In the blockchain technology; when there is a new release, the probability of the fork is higher. At some blockchain framework; upgrade is not allowed, because it is a pain point now. Blockchains' communities of

technology is promising. It is evolving very fast.

In bitcoin history, the longest fork had 53 blocks in August 2010, due to the Value Overflow bug. In March 12, 2013 blockchain fork started with release of v0.8 and it was 31 blocks long. *(https://bitcoin.stackexchange.com/questions/3343/what-is-the-longest-blockchain-fork-that-has-been-orphaned-to-date)*

Our question is "*what if two miners solve the puzzle at the same time?*" *upgrade/release* cases create forks but their reasons are different, which can be mentioned in future.

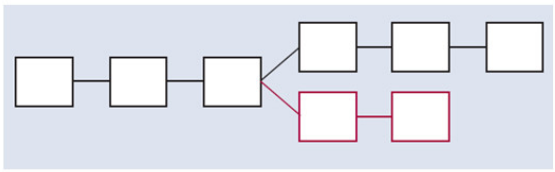
When we turn back to miners' case, difficulty of the puzzle minimizes the probability to be solved at the same time. If there is a tie, someone has to solve a new block to break the tie. ***The general rule is always 'follow the longest chain'***.

So what is happening during the fork?

When two miners solve the puzzle at the same time, they send the blocks to the nodes to verify. Nodes verify and add the block to their chain, which they receive first. When nodes accept the block, they announce to miners their last block. But nodes will announce different blocks to the miners. Miners are in a race. They don't wait for a second when they receive the last block info; they start to work (hashing) immediately.

Blocks have fingerprint.

Each block in the chain is different from each other, like a snowflake. Each block has a unique fingerprint. In hash puzzle, do you remember the second input of the hashing? It is previous block's fingerprint. When a miner finds the puzzle solution, it sends it to the nodes. When nodes receive the new block, they control many things and one of them is the fingerprint of the previous block. If it doesn't match with the one they have, they reject the solution and wait for the new block which matches. Ok, that fingerprint info is enough; let's turn back to our story.



So half of the nodes have the last block with different fingerprint and now miners are using different inputs for the hashing race. When a miner finds the solutions, sends it to the nodes. Some of the nodes will accept it, some of them will not. By the way, there is a rule in the blockchain and it is "longest chain wins". Just for the above forked chain figure, continue to our story. After a few seconds, another miner on the red chain finds the solution and sends it to the nodes. Nodes are checking the fingerprints saved in their local database. After ten minutes later, tie is broken with the black colored fork. Nodes that are on the red colored chain check the longest chain. The

and update their local database with longest chain.

Two red blocks have been released and transactions' status listed in these blocks is changing to pending again. It means that they will go through to all controls again and wait for miners to collect them during the hash puzzle race.

According to the above scenario, it seems that double spend can be done easily in bitcoin!

Double spend scenario

1. I'm buying a MacBook from Alice and pay 1 BTC to her. (2470 $ as I wrote this article)
2. Alice waits for the transaction to be approved in the blockchain. *My transaction is in block#3.*
3. After a block is added to the chain which my payment transaction is in it, Alice sent my MacBook by cargo.
4. When I take the product, I'm sending the same transaction (1 BTC) to my second address.
5. Nodes receive the transaction and check that it has already been spent, so don't accept it.
6. But I have super power computers. I take my fraud transaction in my block#3a and begin to solve the hash puzzle. During hashing, I take previous block's fingerprint block#2 , not the last one. By the way, except me; all miners are working on block#4.
7. Just assume that I find the puzzle solution quickly and broadcast my block#3a to all nodes. Nodes again don't accept, because they have that block#3 already.
8. Now I am working on block#4a and other miners are still working on block#4. Miracle happens and I find the solution before them and broadcast my block#4a.
9. The rule is clear, longest chain wins. So all nodes release block#3 and update their local database with the new chain. They add block#3a and block#4a to their ledger. And they say goodbye to block#3, goes to space :)
10. All transactions listed in the block#3 again are turning back to the pending transactions pool. But before entering in to that pool, nodes are checking if controls are ok. They check my 1 btc transaction to Alice and see that it has already spent. It is not an UTXO-unspent transaction output.

bad!

The whitepaper, Satoshi Nakamato published, says 'As long as the majority of the CPU's power is in control of those who do not cooperate to attack the network, they will produce the longest chain and kill the attackers.'

For the above scenario; if network's power was greater than mine, I would never catch and pass the longest chain.

If you do trade on bitcoin blockchain, wait for some blocks to be approved. More blocks are added to the chain, less probability that your transaction will release to space. You decide how much you will wait, if it is a cup of coffee, 10 minutes (1 block) would be enough. If it is a foreign trade transaction with 1.000.000 $ wait for 2 days!

Why miners solving the puzzle?

- Reward per block is 12 BTC ($ 29640 – March 26, 2017)
- Every 4 years a block winner falls to the half. Next reward-drop date will be 23 Jun 2020. The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12 to 6 coins.
- When the amount of bitcoin reaches 21 million, no reward will be awarded

Mining Pool System

- To achieve a steady return, many people combine their processing power into a pool.
- The income obtained is also distributed to the pool participants according to the participation rate.
- The BTC Guild mining pool managed to solve 6 blocks in a row 3 years ago.
- Ghash.io mining pool power increases up to 45% of the network. Miners voluntarily left the pool; otherwise possibly it would **destroy** the Bitcoin value by centralizing the mining.

There are many other different use cases and blockchains. They are topic of other articles.

You can read "Blockchain Evolution 2 / Off-chain, Sidechains, Ethereum & Smart Contract Explanation with a use case" in this post.

Onur Deler
Enterprise Architect at TEB (BNP Paribas JV)
3 articles

Follow

18 comments Newest

Sign in to leave your comment

Nitin Kumavat ··· 1mo
Student at Thakur college of engineering and technology

which fields of block are used to generate solution?

Like Reply

Niranjan Indavara Omkarappa ··· 6mo
Technical Lead at Evolvus Solutions Pvt Ltd

Nice article got more clarity.
Bitcoin belongs to Public blockchain type. Everyone can contribute towards mining.
In Private blockchain type. Who are in group are eligible for Mining or only limited persons in the group are eligible for Mining?

Like Reply | 1 Like • 2 Replies

Onur Deler 6mo
Enterprise Architect at TEB (BNP Paribas JV)

In private blockchain type, there is no need for mining. Generally in private chains, specific nodes (members) have right to create blocks (aka validation & approvement of transactions). PBFT consensus model is generally being used for that kind of cases. Hyperledger fabric is a good private blockchain type to analyse. At this link there is more details about consensus mod
… See more

Like Reply | 1 Like

Niranjan Indavara Omkarappa 6mo
Technical Lead at Evolvus Solutions Pvt Ltd

Onur DelerThank you.

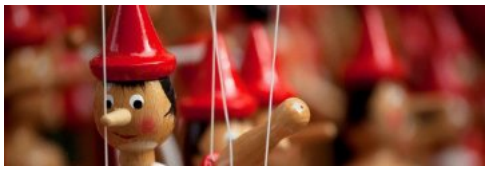
Like Reply

There are 16 other comments. Show more.

Top stories from Editors' Picks

Artificial intelligence could completely transform patient care. So why are nurses so skeptical about it?

Beth Kutscher on LinkedIn



The one crucial element of a healthy workplace that every company, in every industry, can provide

Jeffrey Pfeffer on LinkedIn

Melinda Gates says VC is still a boys' club. This entrepreneur has an innovative solution to that

Glenn Leibowitz on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories