Cryptocurrency and Validated Transactions

By Bob Primak
For The Chicago Computer Society
South Suburban Computer Club
May 17, 2022

NOTE: I am not a financial advisor. This presentation is not selling or endorsing any financial instruments or techniques.

For investment advice, consult your own financial adviser.

Some of what is presented here is controversial and may differ from the opinions of others.

Cryptocurrency and Validated Transactions

We will be discussing cryptocurrency.

What is it? How does it work?

What is Blockchain, and how are Blockchain transactions validated?

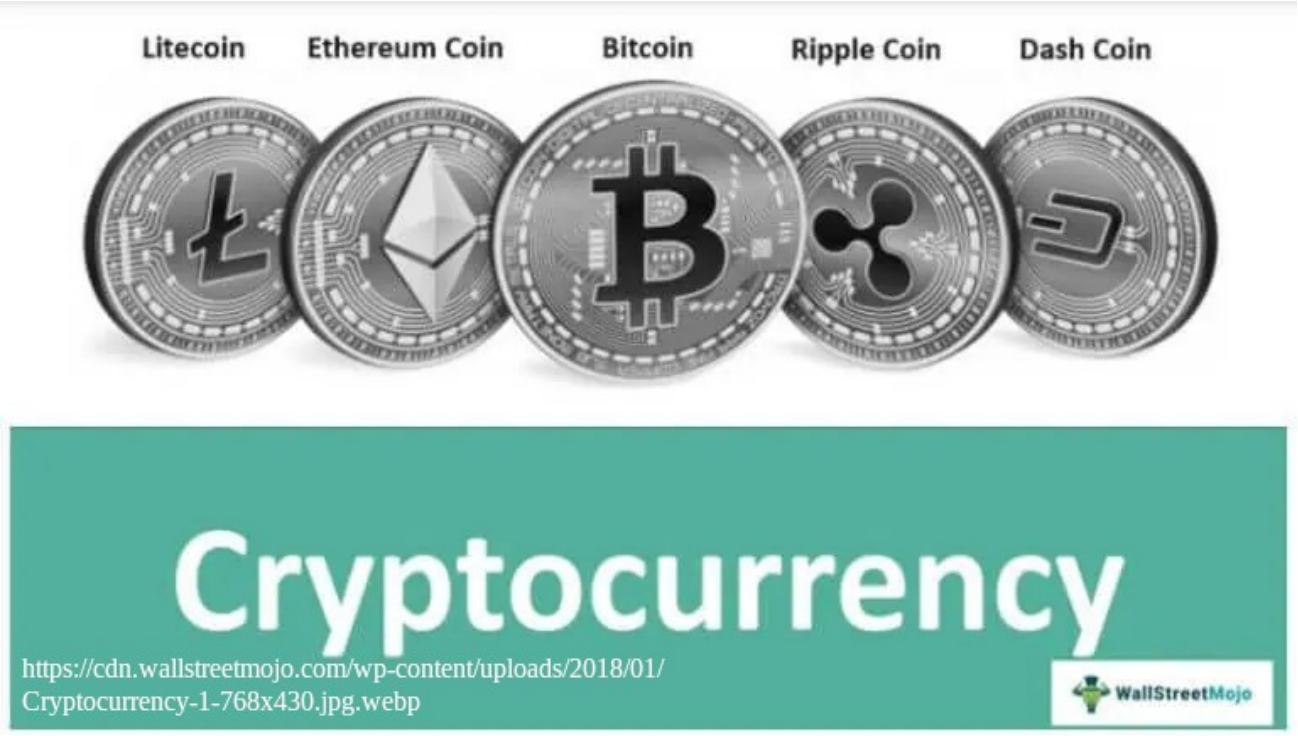
What is Proof of Work, and Proof of Stake?

Can we actually use Bitcoin to pay for stuff?

What happens if we want to cash out our Bitcoins?

Cryptocurrency and Validated Transactions

What is cryptocurrency?



Cryptocurrency and Validated Transactions

What is cryptocurrency?
Here's what you need to know about blockchain, coins and more.
It's important to understand the basics of cryptocurrency before investing.
https://www.cnbc.com/select/what-is-cryptocurrency/

At its most basic, a cryptocurrency is a digital asset that utilizes computer code and blockchain technology to operate somewhat on its own, without the need for a central party — be that a person, company, central bank or government — to manage the system.

Cryptocurrency and Validated Transactions

Cryptocurrency and Validated Transactions

Bitcoin, the first cryptocurrency created, was developed initially to act as a payment mechanism native to the online world. Faster, cheaper, censorship resistant and not beholden to any government or central bank's whims.

Today, there are thousands of cryptocurrencies. These still act as payment mechanisms but have also been developed for other use cases, such as lending and borrowing or digital storage. And one of the broadest use cases for this technology is speculation, buying in the hopes that the price will go up and the holders can make a profit.

Most of what I'll be dealing with this evening is about Bitcoin. Some cryptocurrencies work differently from Bitcoin. One of these, Ethereum, has become tied with Nonfungible Tokens (NFTs). I will be going into more details about that area of cryptocurrency at a future CCS meeting.

Cryptocurrency and Validated Transactions

How does it work?

While the definition is fluid, there are several features that typically make up a crypto asset:

6) Cryptography -- All cryptocurrencies rely on security features, including encryption, to maintain their integrity and to provide some degree of privacy in transactions. This is not the same as providing absolute anonymity. We shall see later why crypto transactions are and must be inherently traceable from end to end.

7) Transparency -- use of open source protocols, but more importantly: Every crypto transaction is timestamped to the blockchain, which creates a public provenance or chronology of ownership or custody of the assets. This makes every transaction traceable. But it is in place to allow people to trust that the cryptocurrency is valid and that its value is agreed upon in some way.

Cryptocurrency and Validated Transactions

8) Incentives -- Bitcoin miners must use computer power to verify blocks of transactions. To compensate for the work miners do, newly minted coins are automatically distributed to miners when they verify a block of transactions. This is called Proof of Work.

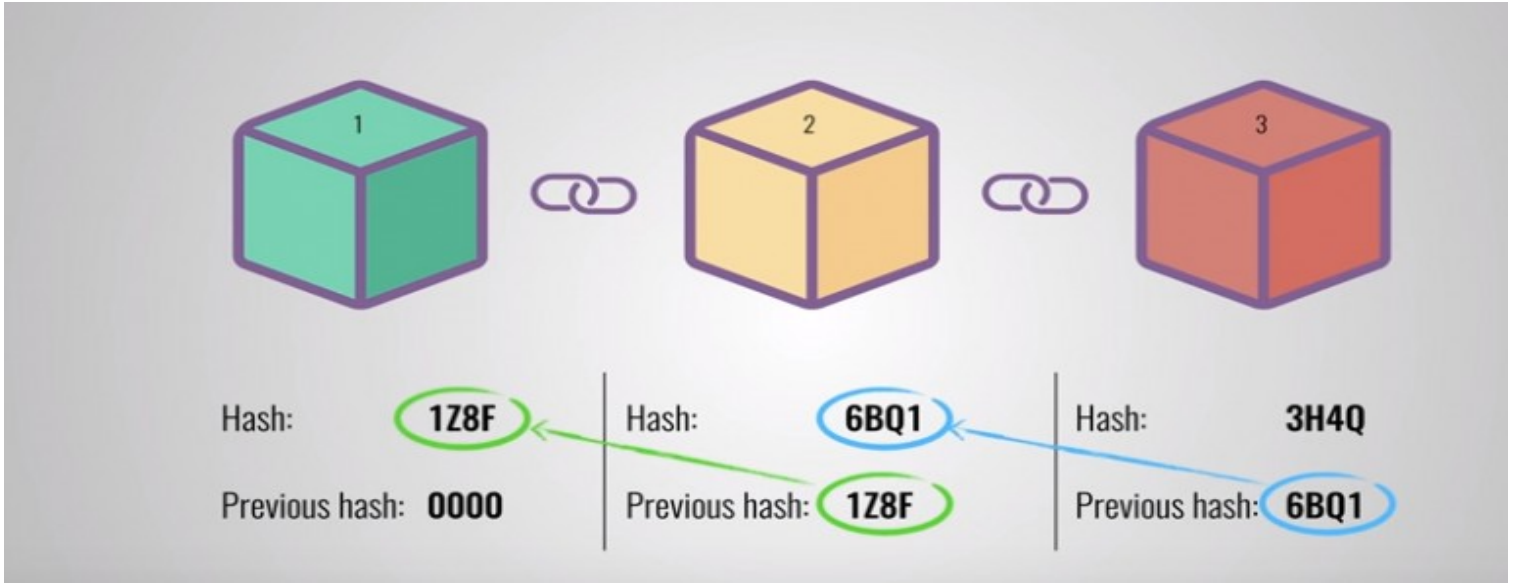
There are other ways to use Proof of Work, and some of these ways can get problematic, as we shall see in August when I present about Ethereum and its ties with the Metaverse of in-game economies and tokens which have no existence in the material world. Read more at CNBC:

https://www.cnbc.com/select/what-is-cryptocurrency/

Cryptocurrency and Validated Transactions

What is Blockchain?

What are cryptocurrencies, and how do they work?
https://www.cbsnews.com/news/what-is-cryptocurrency-bitcoin-ethereum-blockchain/



https://www.calsoftinc.com/blogs/wp-content/uploads/2018/09/2-768x347.png

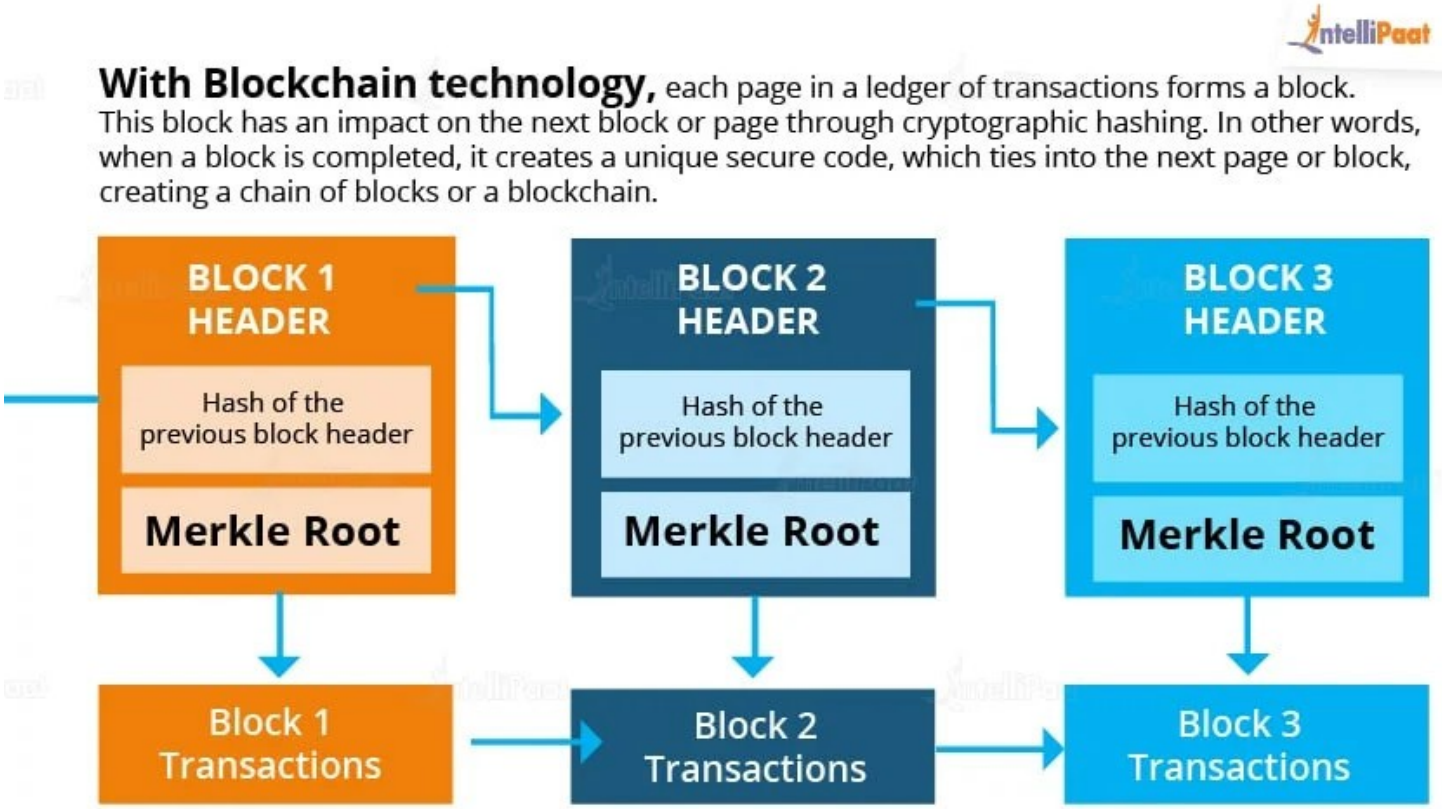
Cryptocurrency and Validated Transactions

A blockchain is a type of database. Different cryptocurrencies are built on different blockchains.

Some cryptocurrencies or tokens are built on top of other cryptocurrency blockchains. Tokens (NFTs) for example are built on cryptocurrency blockchains, like that of Ethereum.

Blockchains are a type of public ledger. Blockchains record cryptocurrency transactions in encrypted, digital records that live on servers all around the world. Blockchains can also be used to record other types of information — like property records or the origins of a food item. Most credit cards use blockchain technologies to make a secure, public ledger of the transactions they handle.

Cryptocurrency and Validated Transactions



https://intellipaat.com/mediaFiles/2019/02/Blockchain-08.jpg

Cryptocurrency and Validated Transactions

An accounting ledger is an account or record used to store bookkeeping entries for balance-sheet and income-statement transactions. Accounting ledger journal entries can include accounts like cash, accounts receivable, investments, inventory, accounts payable, accrued expenses, and customer deposits.
(Accounting Ledger -- https://www.sageintacct.com/resources/accounting-financials-glossary/accounting-ledger
)

The blockchain works as a ledger, tracking every Bitcoin transaction, and is self-verifying, meaning that the entire network of nodes — different computers participating in the network — will constantly check and secure every movement. This is a type of peer to peer network. Validation is achieved in essence through a consensus among the participants in the network.

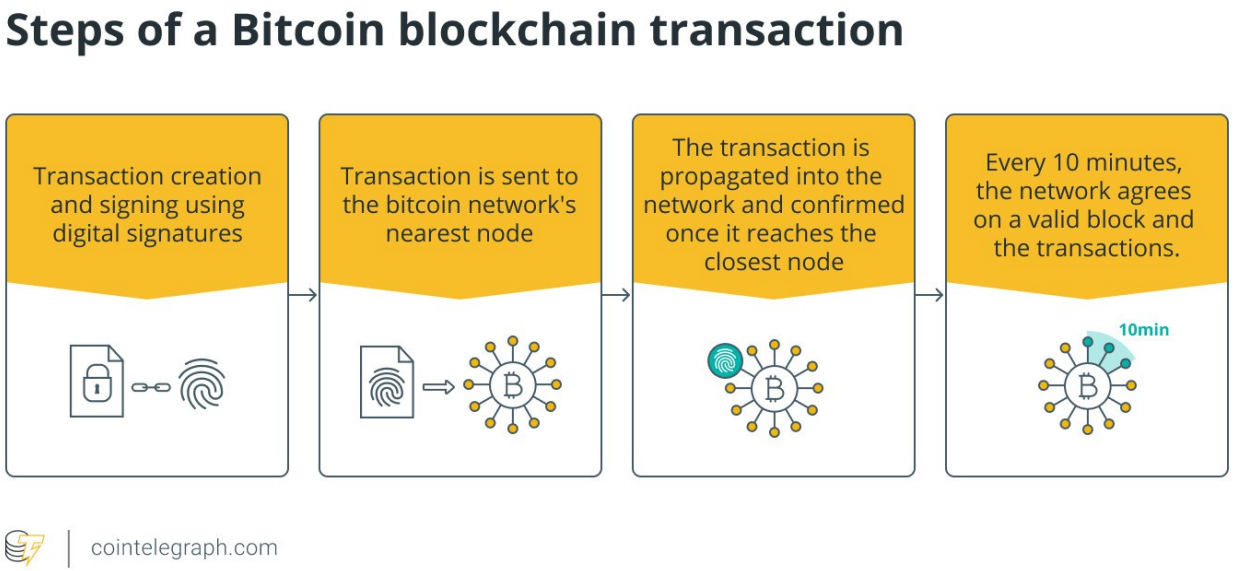
Cryptocurrency and Validated Transactions

A traditional ledger for accounting.

https://www.wikihow.com/images/thumb/0/0b/Write-an-Accounting-Ledger-Step-17.jpg/aid1332366-v4-728px-Write-an-Accounting-Ledger-Step-17.jpg.webp

Cryptocurrency and Validated Transactions

What is the Bitcoin blockchain? A guide to the technology behind BTC



Cryptocurrency and Validated Transactions

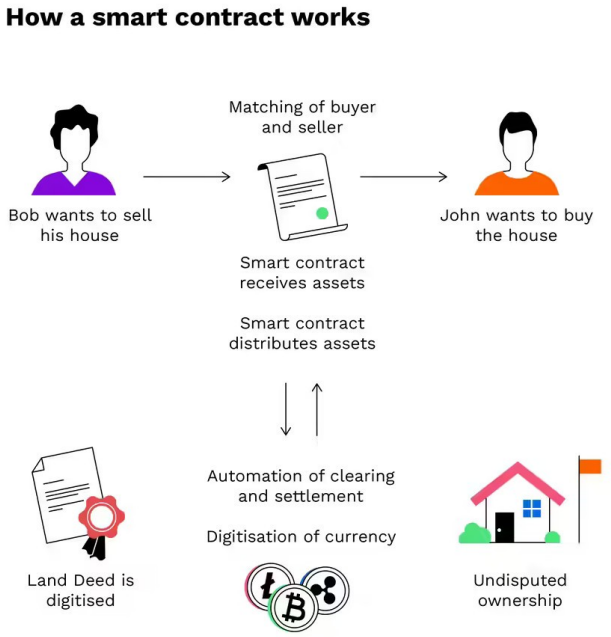
https://s3.cointelegraph.com/storage/uploads/view/9f3e567803b4c29aaf63c50bf50fe946.png

There are 4 steps illustrated in this image. (Previous slide.)

The blockchain works as a ledger, tracking every Bitcoin transaction, and is self-verifying, meaning that the entire network of nodes — different computers participating in the network — will constantly check and secure every movement. This is a type of peer to peer network. Validation is achieved in essence through a consensus among the participants in the network.

A peer to peer ledger is also known as a distributed or decentralized ledger.

Cryptocurrency and Validated Transactions



https://bitpanda-academy.imgix.net/null27888504-6500-47de-9a48-af940ad52551/bitpanda-academy-intermediate-11-smart-contract-infographic.png?auto=compress%2Cformat&fit=min&fm=jpg&q=80&w=900

Cryptocurrency and Validated Transactions

What Is a Smart Contract?

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met.

What are smart contracts on blockchain?
https://www.ibm.com/topics/smart-contracts

A smart contract, like any contract, establishes the terms of an agreement. But unlike a traditional contract, a smart contract's terms are executed as code running on a blockchain like Ethereum. Smart contracts allow developers to build apps that take advantage of blockchain security, reliability, and accessibility while offering sophisticated peer-to-peer functionality — everything from loans and insurance to logistics and gaming.

Cryptocurrency and Validated Transactions

What makes smart contracts “smart,” however, is that the terms are established and executed as code running on a blockchain, rather than on paper sitting on a lawyer’s desk.

Smart contracts expand on the basic idea behind Bitcoin — sending and receiving money without a “trusted intermediary” like a bank in the middle — to make it possible to securely automate and decentralize virtually any kind of deal or transaction, no matter how complex. And because they run on a blockchain like Ethereum, they offer security, reliability, and borderless accessibility.

What is a smart contract?
https://www.coinbase.com/learn/crypto-basics/what-is-a-smart-contract

Real-World Use Cases for Smart Contracts and dApps
https://www.gemini.com/cryptopedia/smart-contract-examples-smart-contract-use-cases

(Skip next 3 slides for South Side.)

Cryptocurrency and Validated Transactions

(I will digress here to tie in with future talks on High Frequency Trading and the "Flash Boys", and NFTs and the Metaverse, all of which involve programmed trades and smart contracts.)

Smart Contracts are tied more to gaming and NFTs and use the Ethereum Blockchain. So they are beyond the scope of this presentation. But it should be noted that some examples of Smart Contracts are similar to the automatic high-speed trading programs used by brokerages in traditional stock and securities markets for decades. And they can carry all of the problems of high-frequency, high-velocity trading programs.

I will be giving a talk about an old story from Wall Street at another computer user group meeting in June. This is the story told in the book "The Flash Boys". It shows actual large-scale market manipulation using programmed trading and taking advantage of very small physical differences in computer networks. Front running is the ability of one trader to preempt trades of other traders by getting ahead of them in an electronic cue, often exploiting these small time differences within the network.

Cryptocurrency and Validated Transactions

Front running may be possible with Smart Contract programs as well, though there have been no complaints of these practices in the articles about cryptocurrencies I've seen so far. So, can someone preempt your coin mining submissions in a similar way to how the Flash Boys did their front running scheme? No one seems to be talking about this. The SEC regulates traditional American securities transactions. Who regulates the Blockchain?

Smart Contracts also can dilute the value of Proof of Work (explained later in this presentation). This has caused issues with Ethereum's blockchain, and raises issues of the value of work and the definition of work under labor rules.

Some people (especially gamers in such places as the Philippines and Southeast Asia) have literally worked for less than local minimum wages, which has attracted the attention of law enforcement and labor authorities in several countries.

Cryptocurrency and Validated Transactions

But is gaming, is coin mining, really work, as defined under the local laws? This controversy has parallels in the "gig economy" of delivery and ride sharing services. Are gig workers really employees? How are "hours worked" defined when you don't punch a time clock? Is being paid per unit produced really legal? The alternative, Proof of Stake, has its own problems, as we shall see later.

(End of digression.)

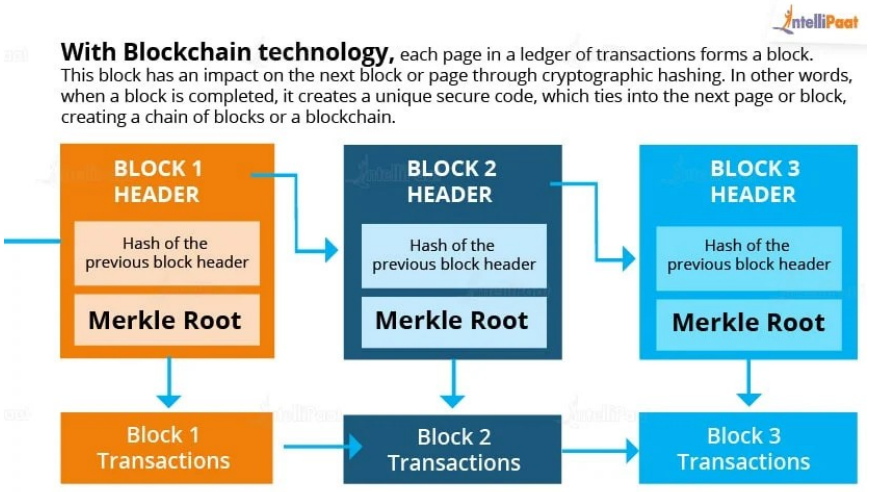
“High Frequency Trading and The ‘Flash Boys’” to be given at the Lexington Computers and Technology Group (LCTG) June 22, 2022. (Daytime meeting)
https://wiki.toku.us/doku.php?id=lexingtoncomputergroup#future_meetings_schedule

“NFTs, Ethereum and the Metaverse” to be given at the August 4, 2022 meeting of The Chicago Computer Society West Side Computer Club. (Evening meeting)
Email to <1ccsadmin@comcast.net> for CCS meeting schedules and announcements.

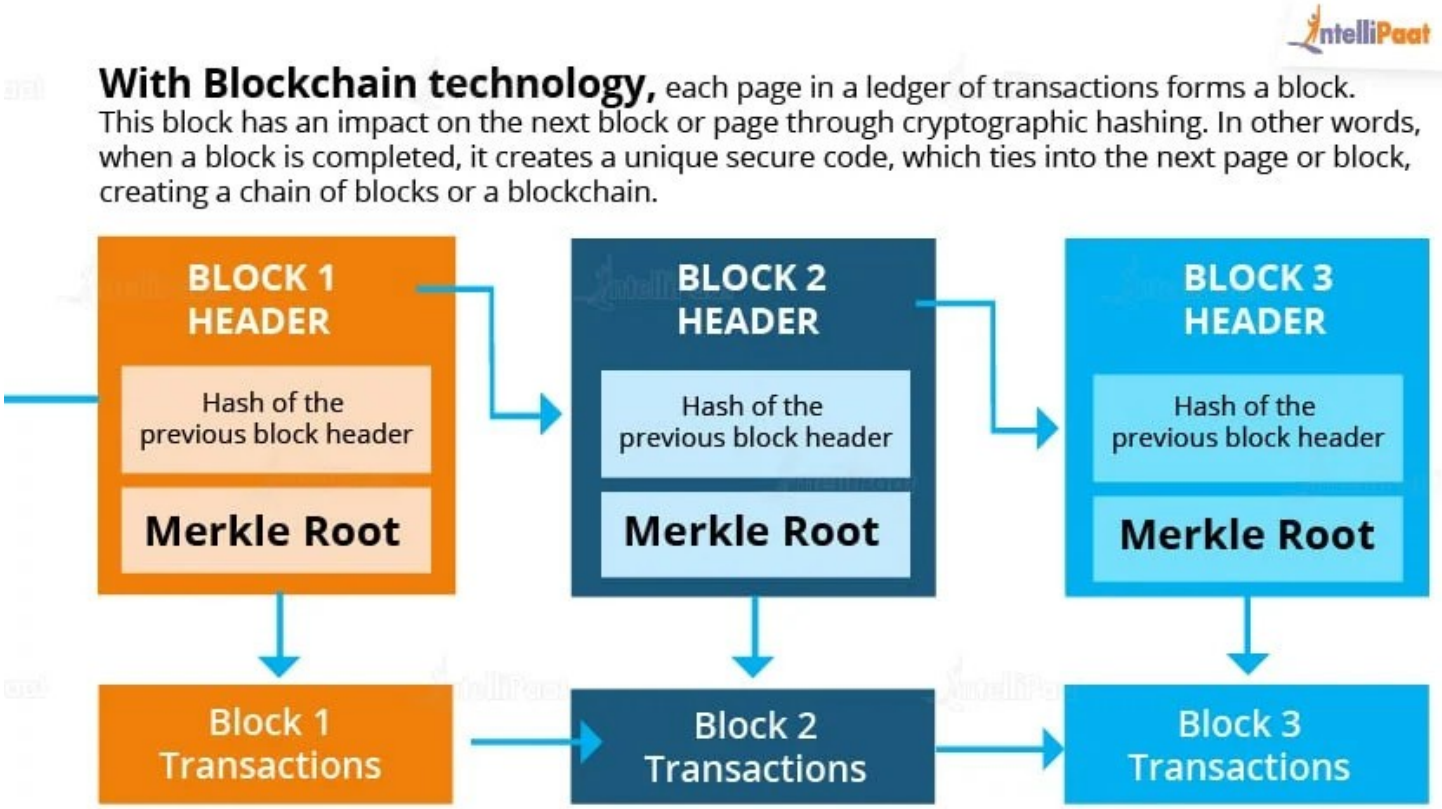
Cryptocurrency and Validated Transactions

How are Blockchain transactions validated?

What is the Bitcoin blockchain? A guide to the technology behind BTC
https://cointelegraph.com/bitcoin-for-beginners/how-does-blockchain-work-a-beginners-guide-to-blockchain-technology



Cryptocurrency and Validated Transactions



https://intellipaat.com/mediaFiles/2019/02/Blockchain-08.jpg

Cryptocurrency and Validated Transactions

We have seen how the blockchain is built, and how it is validated. A blockchain is a type of database which is a collection of information stored on a computer system electronically.

A database structures data into tables, while a blockchain collects information into groups, known as blocks, that hold data sets. Each block has a specific storage capacity that is chained onto the previous filled block when it gets filled, forming a chain of data. That's why it's called the blockchain: Millions of blocks filled with data are chained together.

This system means that every blockchain is a database that is more complex since it creates an irreversible chainline of data when implemented in a decentralized system. The goal of the blockchain is to allow digital information to be recorded and distributed, but not edited. This differs form most databases.

Cryptocurrency and Validated Transactions

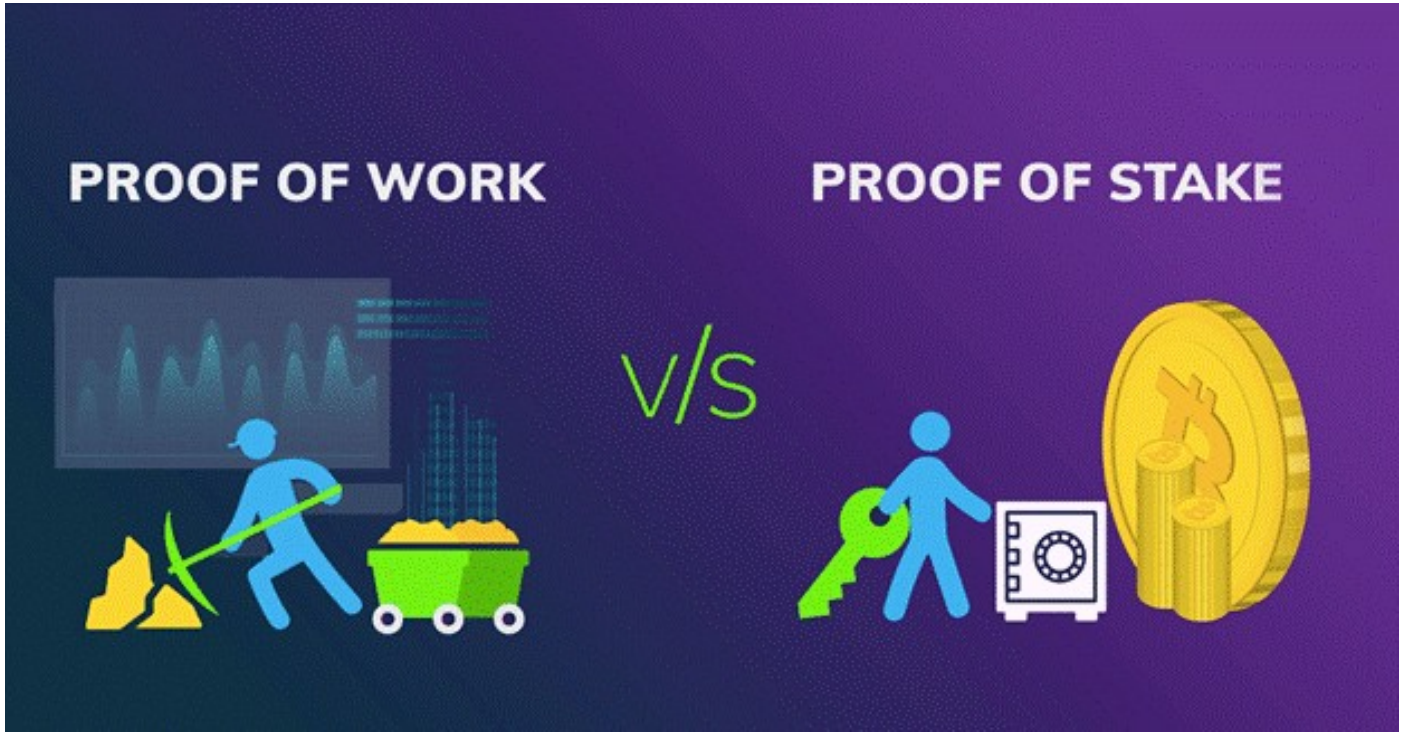
Transactions that are part of the blockchain have to be approved by thousands of thousands of computers. This removes all human involvement in the verification, which means there are fewer human errors, as well as a more accurate record of information. Any member of the Bitcoin network can check and verify the blockchain at any time.

Although anyone with an internet connection can see the list of the network's transaction history and access details about transactions, no one can access identifying information about the users that are making those transactions. Every time a transaction is recorded, it is verified by the network.

What is Proof of Work?

What is "proof of work" or "proof of stake"?
https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake

Cryptocurrency and Validated Transactions



https://www.c-sharpcorner.com/article/proof-of-work-vs-proof-of-stake/

Cryptocurrency and Validated Transactions

“Proof of work” and “proof of stake” are the two major consensus mechanisms cryptocurrencies use to verify new transactions, add them to the blockchain, and create new tokens. Proof of work, first pioneered by Bitcoin, uses mining to achieve those goals. Proof of stake — which is employed by Cardano, the ETH2 blockchain, and others — uses staking to achieve the same things. (Proof of Stake is part of the my future presentation, as Bitcoin does not use Proof of Stake.)

Proof-of-work blockchains are secured and verified by virtual miners around the world racing to be the first to solve a math puzzle. The winner gets to update the blockchain with the latest verified transactions and is rewarded by the network with a predetermined amount of crypto.

Proof of Work is an energy-intensive process that can have trouble scaling to accommodate the vast number of transactions smart-contract compatible blockchains like Ethereum can generate. And so alternatives have been developed, the most popular of which is called proof of stake.

Cryptocurrency and Validated Transactions

What is Proof of Stake?

What is "proof of work" or "proof of stake"?
https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake

While the Bitcoin blockchain mostly just has to process incoming and outgoing bitcoin transactions, much like a vast checkbook, Ethereum's blockchain also has to process a vast array of DeFi (decentralized finance) transactions, stablecoin smart contracts, NFT minting and sales, and whatever innovations developers come up with in the future. (Don't worry about what all these terms mean, as they are part of the August presentation.)

Their solution has been to build an entirely new ETH2 blockchain — which began rolling out in December 2020 and should be finished in 2022. The exact details vary by project, but in general proof of stake blockchains employ a network of "validators" who contribute — or "stake" — their own crypto in exchange for a chance of getting to validate new transactions, update the blockchain, and earn a reward.

Cryptocurrency and Validated Transactions

The network selects a winner based on the amount of crypto each validator has in the pool and the length of time they've had it there.

Once the winner has validated the latest block of transactions, other validators can attest that the block is accurate. When a threshold number of attestations have been made, the network updates the blockchain.

All participating validators receive a reward in the native cryptocurrency, which is generally distributed by the network in proportion to each validator's stake.

Complaints include that this system gives all the power to a few "whales" -- big, wealthy investors. While pools can allow smaller investors to have collective power, it is still believed by many that this system favors larger investors, so smaller investors have been discouraged from participating. This has implications for the value of NFTs, which goes beyond the scope of this presentation.

If anyone tries to validate a block in a Proof of Stake blockchain and their decision is not accepted, a portion of their stake is "burned" -- written out of the blockchain. This can also be problematic.

Cryptocurrency and Validated Transactions

Can we actually use Bitcoin to pay for stuff?

https://i0.wp.com/www.rarerecords.net/wp-content/uploads/bitcoin_ethereum_400a.jpg?w=400&ssl=1

Cryptocurrency and Validated Transactions

Can we actually use Bitcoin to pay for stuff?

How Can I Buy Something With Bitcoin?

The easiest and most convenient way to make purchases using bitcoin or other cryptocurrencies is with a cryptocurrency debit card. These cards, which are available from major crypto exchanges and other providers, also allow the holder to withdraw cash from participating ATMs. Many participate in major networks, such as Mastercard and Visa.
(What Can You Buy With Bitcoin?)
https://www.investopedia.com/what-can-you-buy-with-bitcoin-5179592

Electronics, luxury watches, and even cars are among the items that cryptos can purchase.

Even Real Estate can be paid for with crypto, provided the seller's financing arrangements can accept it as payment.

Cryptocurrency and Validated Transactions

Crypto Just Became Real Estate's Hottest New Thing
https://www.forbes.com/sites/petertaylor/2022/05/07/crypto-just-became-real-estates-hottest-new-thing-heres-what-the-bitcoin-revolution-means-for-buyers-sellers-and-developers/?sh=325d9d8d388b

Crypto boom opens door to a new class of landlords
https://www.nbcnews.com/tech/crypto/crypto-real-estate-investment-landlords-rcna20029

So yes, there are getting to be companies which will accept and even facilitate real estate transactions using cryptocurrencies and smart contracts. Remember, the price of crypto is very volatile, so the value of your purchase in crypto can fluctuate wildly.

El Salvador becomes first country to adopt Bitcoin as an official currency
The cryptocurrency will be legal tender alongside the US dollar
https://www.theverge.com/2021/9/7/22660457/el-salvador-bitcoin-legal-tender-currency-cryptocurrency-chivo-wallet

Cryptocurrency and Validated Transactions

So there's that. Many in the international finance community are very skeptical of the viability of this concept. But note -- El Salvador already does not have a local official currency. This is in part because the country's economy is almost entirely made up of moving goods and services, acting only as a waypoint in the flow of commerce. Very unusual type of economy.

https://forkast.news/wp-content/uploads/2021/08/FF_Chivo-610x343.jpg

Cryptocurrency and Validated Transactions

https://www.coindesk.com/markets/2021/06/25/athena-to-install-1500-atms-in-el-salvador-following-bitcoin-law/

What happens if we want to cash out our Bitcoins?

How to sell Bitcoin: 5 ways to "cash out" your BTC holdings
https://cointelegraph.com/bitcoin-for-beginners/how-to-sell-bitcoin-5-ways-to-cash-out-your-btc-holdings

Note: Not all of these methods will work for all cryptocurrencies.

Cryptocurrency and Validated Transactions

Cryptocurrency exchanges: Despite having several disadvantages, exchanges are a one-stop solution when it comes to trading Bitcoin. In the case of selling the cryptocurrency, exchanges act as an intermediary, holding sellers' and buyers' funds.

It is important to remember that despite offering wallet services, exchanges are by no means a secure, reliable place to store your funds. They can be targeted by hackers. Some have shut down leaving their depositors with no recourse to recover the funds they held.

Direct trades (person-to-person): Bitcoin buyers post listings on these platforms, noting their desired price, their preferred payment option, etc. Interested parties then find listings they like and complete the sale by following the instructions provided by the platform. These sales involve a high degree of trust. Things can go very wrong.

Cryptocurrency and Validated Transactions

Face-to-face transactions: You just arrange to meet with someone and exchange your cryptocurrency for cash (or goods or services). Potential dangers exist when trading Bitcoin in person with strangers, similar to the risks that come with other in-person financial transactions.

Bitcoin ATMs: You set up a wallet or debit card, and you can draw from it as you would do in a traditional ATM setting. There are some parts of the world where crypto ATMs do exist, but they are rare to nonexistent in other areas. In the US there are crypto ATMs, but they are not anywhere near as common as US Dollar ATMs.

Cryptocurrency and Validated Transactions

That's as far as I'm going to go this evening. I hope everyone has learned something about cryptocurrencies, blockchain technology and the roles these and related technologies are playing in our lives. I can't answer in-depth questions, and I don't give out investment advice, but I may be able to fill in more details if there's time for questions and answers.

More on NFTs and the Metaverse in August at the CCS West Side meeting.

(My “Flash Boys” Presentation in June at LCTG will also be interesting.)

Presenter: Bob Primak, for the Chicago Computer Society.
South Suburban Computer Club. May 17, 2022.

If there’s time, we can have questions and discussion.