Does blockchain represent a fundamental shift in human transactions?

- Blockchain's origin
- Cryptocurrencies and storage
- Truth-free data management

BLOCKCHAIN’S ORIGIN

CYPHERPUNKS, SECURITY AND PRIVACY

- The **Cypherpunks** (a mashup of “cypher” from cryptography, and “cyberpunk” from the science fiction genre) formed in the Bay Area in the early 1990’s. This group of programmers began to work on cryptography for everyone – not just the government. **They were renegades.** Some of their ideas and discussions were enunciated in **The Cypherpunk Manifesto** by **Eric Hughes**. They promoted privacy and anonymous systems and transactions, and wrote computer code to enable creation of practical, anonymous systems.

> **“…privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system…An anonymous system …is the essence of privacy.**
>
> Eric Hughes, A Cypherpunk’s Manifesto

Cypherpunks followed and utilized the earlier work of **Phil Zimmerman**, creator of PGP (Pretty Good Privacy) encryption, who successfully resisted government attempts to own encryption technologies.

Sources 1. https://www.activism.net/cypherpunk/manifesto.html 2. https://www.internethalloffame.org/inductees/philip-zimmermann 3. https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1

CURRENCY AND CONSTRUCTION

FROM BLOCKCHAIN TO CURRENCY

- The Cypherpunk movement sparked the birth of blockchain, the underlying technology required for execution of the peer-to-peer cash systems, and cryptocurrencies. Bitcoin, the first publicized cryptocurrency, was developed by Satoshi Nakamoto, a still-mysterious programmer who publicly shared a paper describing both.

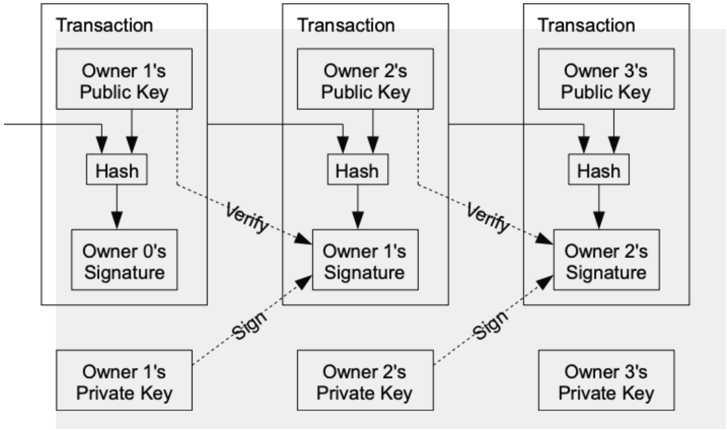
SATOSHI NAKAMOTO is the still-unidentified programmer who first developed Bitcoin, and the first Blockchain.

- The innovation resulted from a combination of known cryptographic techniques and a big idea: transactions could simply be conducted peer-to-peer, without an authority figure (see Nakamoto's figure at right).

> **"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.**
>
> Satoshi Nakamoto, Author, Bitcoin White Paper [4]

CONSTRUCTING BLOCKCHAIN

- In order to construct a fully peer-to-peer system, wherein there is no authority over all transactions, a set of cryptographic methods are used to allow contact and verification among "Owners," or peers. **This scheme fundamentally alters the verification and oversight of transactions.** Four key tenets of a blockchain – a shared, replicated, permissioned ledger are: **consensus, provenance, immutability, and finality**



Sources: 1. https://satoshi.nakamotoinstitute.org/emails/cryptography/1/#selection-33.0-35.42 2. https://blockonomi.com/who-is-satoshi-nakamoto/ 3. https://bitcoin.org/bitcoin.pdf 4. https://www-01.ibm.com/events/wwe/grp/grp307.nsf/vLookupPDFs/1.%20IBM%20Blockchain%20Explained/$file/1.%20IBM%20Blockchain%20Explained.pdf

CHARACTERISTICS, MINING, AND VERTIFCATION

CHARACTERISTICS OF A BLOCKCHAIN

- Not all networks are blockchains – blockchains have these fundamental characteristics:
  1. **consensus** parties agree transaction rules were followed
  2. **provenance** ledger contains all relevant historical information
  3. **immutability** participants cannot modify a transaction
  4. **finality** there is a single ledger for any blockchain network
- These tenets enunciate the general rules of a blockchain network. But who are these peers, who verify transactions – and what's in it for them? **In the operation of blockchain, self-interested parties verify transactions.**

> **There are four constituencies that participate in expanding the value of Bitcoin as a consequence of their own self-interested participation. Those constituencies are (1) consumers who pay with Bitcoin, (2) merchants who accept Bitcoin, (3) "miners" who run the computers that process and validate all the transactions and enable the distributed trust network to exist, and (4) developers and entrepreneurs who are building new products and services with and on top of Bitcoin.**
>
> Marc Andreessen, American Entrepreneur

MINING AND VERIFICATION IN A BLOCKCHAIN

- **Currencies rely on verification**, and **verification relies on challenge**. If anyone can verify a transaction anytime, the transaction is not secure! A degree of challenge is required to create trusted verification.
- So how do you tell if a deal using a pretty rock was made in gold…or just a rock…in cyberspace? **You issue a challenge to solve a math problem.** And you issue a reward for the solution – a shiny new coin.
- "Miners" are essential to blockchain. They solve difficult math problems using intensive computing to verify transactions.

MINERS are independent agents who are compensated for their work. But as we will see, mining becomes more difficult over time.

Sources: 1. https://www.ibm.com/blogs/cloud-computing/2017/04/11/characteristics-blockchain/ 2. https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/'

MINING BASICS

A FEW USEFUL TECHNICAL DEFINITIONS

NONCE ("number only used once")

The number that blockchain miners are solving for. It is obtained by solving a complex mathematical puzzle that can only practically be solved on a computer.

HASH

A function created by an algorithm – that converts an alphanumeric string into an encrypted output of fixed length. A hash is deterministic – it will produce the same encryption each time it is used on the same input. *A hash converts a bunch of letters and numbers into a code – and because it is of fixed length, its size does not provide a clue as to the original input.*

TARGET HASH

A target hash is a number that a hashed block header must be less than or equal to in order for a new block to be awarded. The target hash is used in determining the difficulty of the input, and can be adjusted in order to ensure that blocks are processed efficiently.

MINER / MINING

A **miner** is actually a computer, or "node," that performs calculations. Decoding and encoding the blockchain is referred to as mining. Mining involves the use of computers to run hashing algorithms to process the most recent block, with the information needed in mining found in the block's header. The cryptocurrency network sets **a target value** for this **hash** – the target hash - and miners try to determine what this value is by testing out all possible values.

PROOF OF WORK

Cycling through solutions in order to guess the nonce is referred to as proof of work. The miner who is able to find the value is awarded the block and paid in cryptocurrency. Use of Proof of Stake (PoS) is a different method of validation.

MERKLE TREE

A Merkle tree is a data structure that is used in computer science applications. In bitcoin and other cryptocurrencies, Merkle trees serve to encode blockchain data more efficiently and securely.

HOW IS MINING PERFORMED? "In the PoW model—which Bitcoin, Ethereum, Bitcoin Cash, and Litecoin use, to name a few—individuals, groups, or businesses compete with one another with high-powered computers to be the first to solve complex mathematical equations that are essentially part of the encryption mechanism. These equations correspond to a group of transactions, which is known as a block. The first individual, group, or business that solves these transactions, and in the process validates the accuracy of these transactions within a block, receives a "block reward." A block reward is paid out as digital tokens of the currency that's being validated."

WHAT'S IN IT FOR THE MINERS? "the current block reward for bitcoin is 12.5 tokens. That means whoever is the first to correctly solve equations for a block is paid 12.5 tokens. With bitcoin near $9,500 per coin, that works out to a nearly $119,000 haul."

WHEN DO MINES BECOME EMPTY? There are only 21M Bitcoins under current protocols. Various estimates have been made for completion of mining, and speculation on what will happen to the network is rampant. It is possible that transaction fees will replace coin payments, or that the network itself will become unstable.

Sources: 1. https://www.investopedia.com/terms/n/nonce.asp 2. https://www.investopedia.com/terms/h/hash.asp 3. https://www.investopedia.com/terms/t/target-hash.asp4. 4. https://www.investopedia.com/terms/m/mining.asp 5. https://www.investopedia.com/terms/p/proof-work.asp 6. https://www.investopedia.com/terms/m/merkle-tree.asp 7. https://www.fool.com/investing/2018/03/14/the-basics-of-cryptocurrency-mining-explained-in-p.aspx 8. https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/

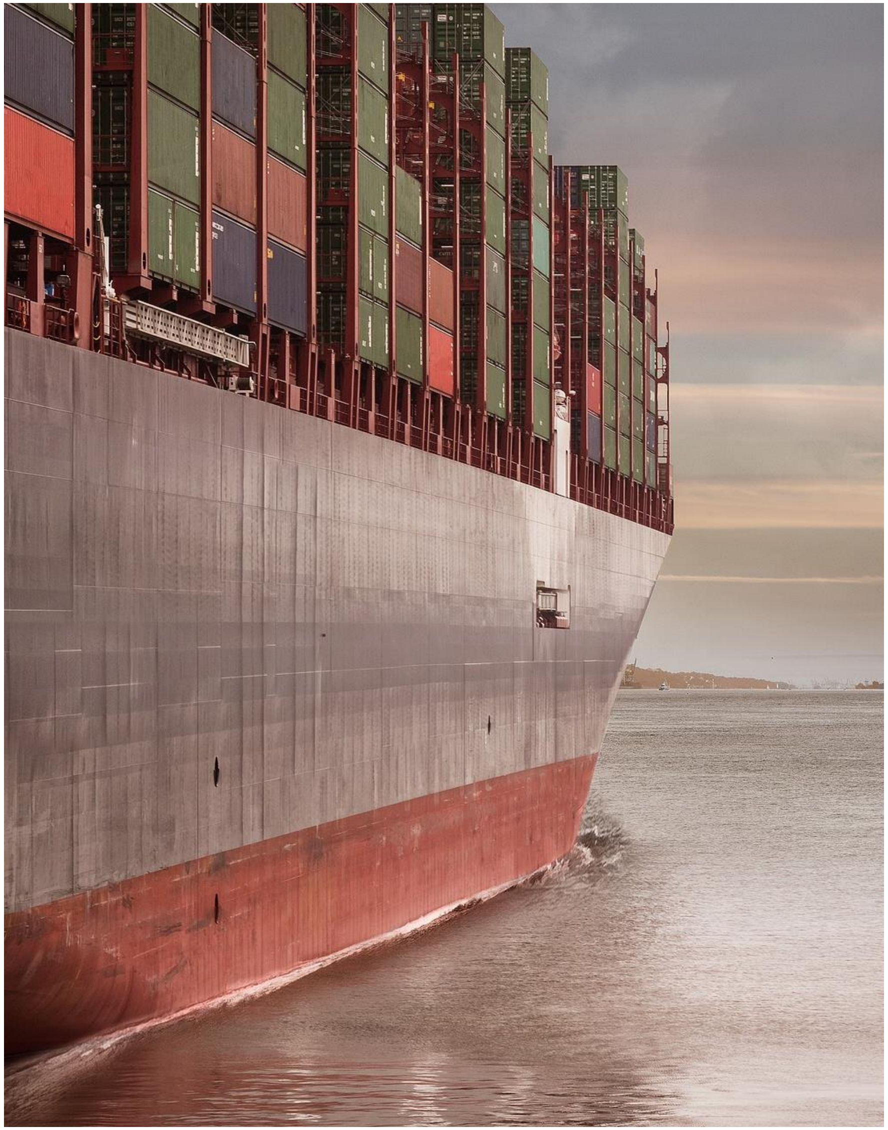
CRYPTOCURRENCIES AND STORAGE

CRYPTOCURRENCIES

> **What is a Store of Value?**
> **A store of value is an asset that maintains its value without depreciating. Gold and other metals are good stores of value as their shelf lives are essentially perpetual, whereas a perishable good (e.g., milk) is a poor store of value due to its propensity to decay. Interest-bearing assets, such as U.S. Treasury bonds (T-bonds), are very good stores of value because they generate interest income and their principal balances are backed by legal contracts.**
>
> Investopedia

- One question that is presently the subject of debate: **are cryptocurrencies really stores of value? It's helpful to look at their market significance, first...**

Source: https://www.investopedia.com/terms/s/storeofvalue.asp



MARKET SIGNIFICANCE OF CRYPTOCURRENCIES

Bitcoin
…has experienced an exponential increase in value since 2009, trading around **$6,583 per Bitcoin** as of September 30, 2018.

Market capitalization
The total market capitalization of crypto is estimated at **$211B**.

Retail participation
The number of users on crypto exchange platforms is estimated to be greater than **30M**.

Institutional participation
Major financial services institutions, such as **Fidelity**, are launching crypto products and services.

Cryptoassets
There are now more than 2,000 cryptoassets, which include newer types of assets, such as stablecoins.

Fundraising
Initial coin offerings (ICOs) have raised **$5.4B** in 2017. In 2018, ICOs have already raised a staggering **$14.2B** as of August 29, 2018.

Financing
Venture capitalists have already invested **$3.9B** in blockchain and crypto companies in 2018.

Security tokens
tZero obtains letter of intent for sale of **$160M** worth of tZero security tokens.

- Clearly – cryptocurrencies are a **significant financial force**. They trade readily. And they are following a similar path to gold and money, in terms of adoption…

Sources: 1. https://assets.kpmg/content/dam/kpmg/us/pdf/2018/11/institutionalization-cryptoassets.pdf 2. Coindesk, Bitcoin (USD) Price (September 30, 2018) 3. CoinMarketCap, All Cryptocurrencies (October 17, 2018) 4. Wall Street Journal, Fidelity Says It Will Trade Bitcoin for Hedge Funds (October 15, 2018) 5. Coinbase adds 100,000 users after CME announces bitcoin futures (November 3, 2017) 6. https://thenextweb.com/hardfork/2018/10/02/vcs-blockchain-investment/ 7. https://www.crowdfundinsider.com/2018/06/135698-tzero-signs-letter-of-intent-with-gsr-capital-for-160-million-security-token-investment/ 8. KPMG, Cryptoasset Services, Market Research (October 2, 2018)

STABILITY AND POTENTIAL

TRADITIONAL VERSUS CRYPTOCURRENCY: STABILITY

- The “gold standard” in the U.S. has evolved, from use of gold as currency in the early part of its history, to abandonment of the gold standard entirely in 1971. The stability of the U.S. Dollar, as “fiat money,” has been much greater than that of cryptocurrencies. However, even given swings in value and the dramatic increase in overall value, Bitcoin has stabilized rapidly.

> **FIAT MONEY** an intrinsically worthless object, such as paper money, that is deemed to be money by law.

> **Bitcoin, which is becoming an investible asset class like unallocated gold, has the potential to become a store of value that is natively digital, generationally relevant, and an alternative to traditional asset classes.**
>
> KPMG: Nagaraj, Hunter, Caplain

CRYPTOCURRENCIES: POTENTIAL

- Metcalfe’s Law states that a network’s value is proportional to the square of the number of its users. By this measure, Bitcoin and Ethereum have increasing potential over time. But,
  - Calculations using network theory suggest that cryptocurrencies are presently overvalued
  - Crashes may be predictable based on overvaluations relative to the number of users.

> **If it were to replace gold entirely, one bitcoin could be worth $357,000. That’s calculated by taking the total value of all the gold ever mined in the world, which is about $7.5 trillion, and dividing that number by 21 million—the total bitcoins that can ever exist.**
>
> CNBC

Sources: 1. https://www.businessinsider.com/history-of-us-gold-standard-2015-12 2. https://cointelegraph.com/news/bitcoin-vs-us-dollar-heres-how-the-dollar-compares-to-bitcoin-in-terms-of-volatility 3. http://lexicon.ft.com/Term?term=fiat-money 4. https://assets.kpmg/content/dam/kpmg/be/pdf/2018/11/institutionalization-cryptoassets.pdf 5. https://www.technologyreview.com/s/610614/how-network-theory-predicts-the-value-of-bitcoin/ 6. https://www.cnbc.com/2018/01/16/skeptics-say-bitcoin-has-no-value-heres-why-theyre-wrong.html

TRUTH-FREE DATA MANAGEMENT

TRANSPARENCY OR BLURRED LINES?

- With the Blockchain, every agreement, process, task, and payment would have a digital record and signature that is readily verifiable and shareable.
- However, the question is raised as to who controls the data that is being input to the blockchain. Even if fraudulent data is transparent, it may not be known to a viewer that the information is incorrect.

Sources: 1. https://hbr.org/2017/01/the-truth-about-blockchain 2. https://medium.com/blocfest/the-truth-is-out-there-48384bff9749

THE CASE FOR TRANSPARENCY

- Transparency on the blockchain for transactions allows for a multitude of applications. Retailers could offer gift cards and store amounts on the block chain. These values would be easily verifiable and could be guaranteed that only the owner of the gift card is using it. No external payment processes would be necessary for tracking and funds could be easily transferred between accounts as it would be recorded on the ledger.
- Blockchains fundamental distributed database removes the need for one authority controlling data. Trust is no longer placed into a singularity but rather now placed into some clever and complex math and code that makes illicit activity extremely difficult.

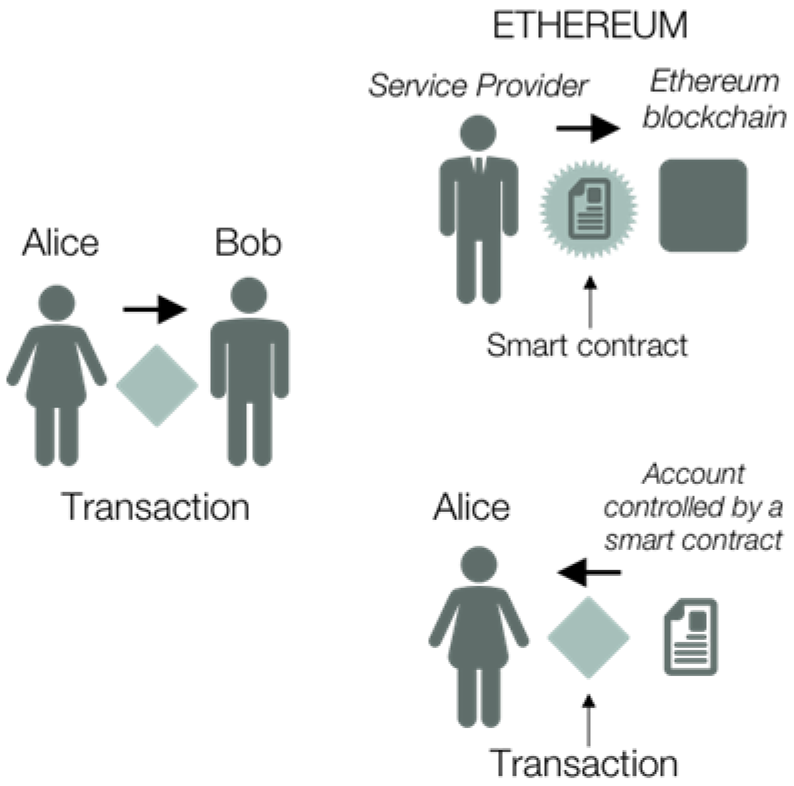
> “ **blockchain is really exciting technology because it's actually providing both transparency, but also agility in a contractual relationship that any organization should have**
>
> Jean-Philippe Courtois, Executive Vice President Microsoft

Sources: 1. https://hbr.org/2017/01/the-truth-about-blockchain 2. https://medium.com/blocfest/the-truth-is-out-there-48384bff9749 3. https://www.businessinsider.com/microsoft-vp-technologies-changing-humanity-finding-success-blockchain-2018-1

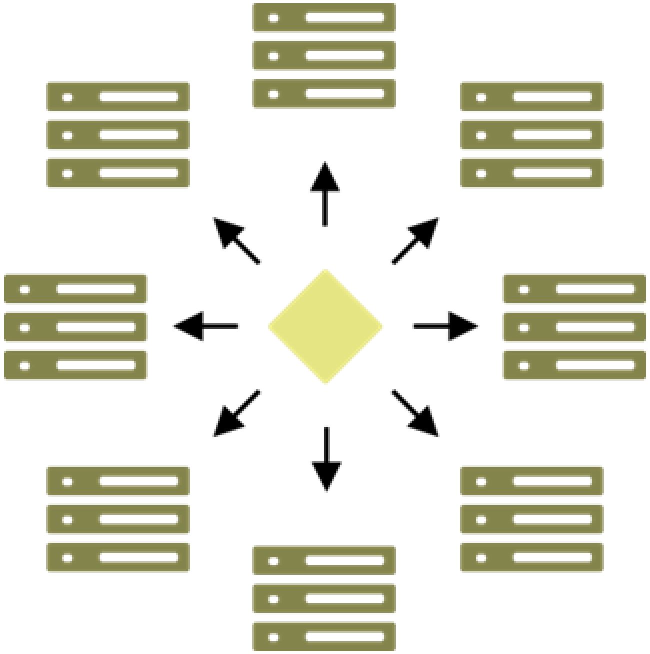
APPENDIX—A BLOCKCHAIN TRANSACTION

A TRANSACTION IS BORN

- Depending on the system, a **transaction** can mean different things.
- In Bitcoin, a transaction is the transfer of cryptocurrency from one person (Alice) to another (Bob).
- In other systems, such as Ethereum, someone can place a line of code, called a **smart contract** on the blockchain, that triggers a transaction when certain conditions are met.



PEER-TO-PEER NETWORK



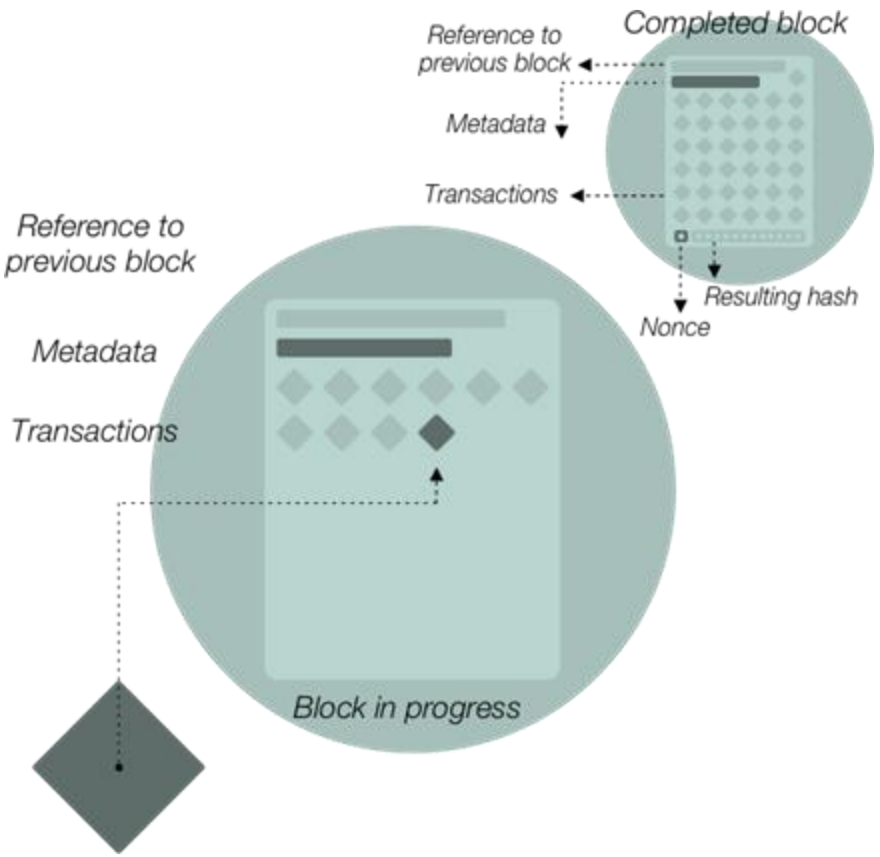
THE TRANSACTION IS BROADCAST TO A PEER-TO-PEER NETWORK

- Alice wants to send money to Bob.
- To do so, Alice must create a transaction on her computer.
- Her computer then sends out "**nodes**" that search the blockchain for proof that Alice has sufficient funds, the private key to her funds and Bob's receiving address (conditions of the smart contract).

NEW BLOCKS

THE RACE TO CRETE NEW BLOCKS

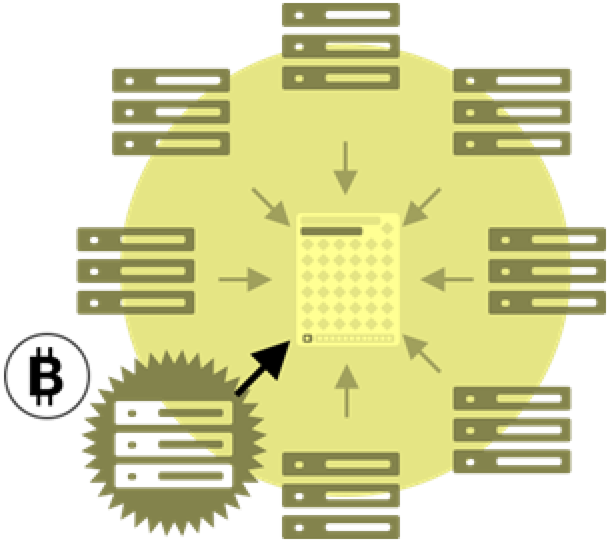
- A subset of nodes, called “**miners**”, organize valid transactions into lists called blocks.
- Blocks in progress contain a list of recent valid transactions.
- To complete a block, the miner must guess the block’s “**nonce**” or unique tag by performing a mathematical puzzle.
  - Then, the nonce is combined with other data in the block to create an encrypted digital fingerprint, called a **hash**.



COMPLETING AND ADDING THE NEW BLOCK

COMPLETING A NEW BLOCK

The hash must meet certain conditions; if it doesn't, the miner tries another random nonce and tries it again. Because it takes enormous effort to find a valid hash, hackers are less likely to modify the blockchain. Once a valid hash is created it is called **proof of work**.



ADDING A NEW BLOCK TO THE CHAIN

- When a miner becomes the first to solve a new block's mathematical puzzle, it sends the block to the rest of the network for approval, earning digital tokens in reward.
- Mining difficulty is noted in the blockchain's protocol. Blocks contain a reference to a previous block, meaning they are mathematically chained together.
- Tampering with an earlier block would require repeating the proof of work for all the subsequent blocks in the chain.

SUMMARY OF A TRANSACTION

1

The blockchain consists of a series of transactions, stored in the form of data.

A few things need to happen in order to perform a transaction.

2

First, if Alice wants to send cryptocurrency to Bob, she has to have cryptocurrency to send and Bob's information so he can receive it.

Computers or "nodes" go out and search for these conditions to make sure that the transaction is valid.

3

A subset of nodes, called "miners" organize the valid transactions into blocks.

To complete a block, the miner must do a complicated math puzzle to figure out the block's "nonce" or unique tag.

The nonce, is then combined with other data in the block to create a digital fingerprint or a "hash".

4

The hash must meet certain conditions, or the miner has to try a different nonce.

Since the process takes a lot of effort, hackers are less likely to try and modify the blockchain.

Once a valid hash is created it is called proof of work.

The first miner to create a valid hash for the block gets digital tokens as reward.