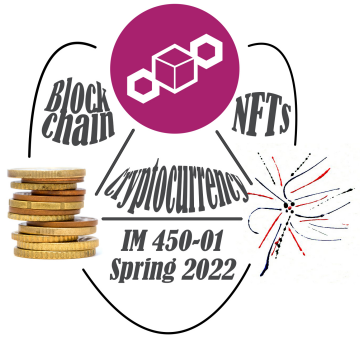
IM 450-01 Issues in IM: *Blockchain, Cryptocurrency, NFTs*

Spring 2022

Class 2—January 25

Blockchain:
What is it and how does it work?



Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the blockchain distributed consensus model as the most important invention since the Internet itself.

What is Blockchain?
From “Blockchain: Background and Policy Issues”

<https://crsreports.congress.gov/product/pdf/R/R45116/3 >

“A blockchain is a digital ledger that allows parties to transact without the use of a central authority to validate those transactions. These transactions are not limited to financial ones, but may include item tracking, identity logging, verifying the completion of an action, or others.

The use of a central, validating authority (i.e., a third party) can be avoided because in a blockchain, as transactions are added, the identities of the parties conducting those transactions are verified, and the transactions are verified as they are added to the ledger as a block of transactions.

The ledger is auditable because each block of transactions is dependent upon the previous block in such a way that any change would alert other users of a change to the history of transactions. The strong relationships between identities, transactions, and the ledger enable parties to verify with a high degree of confidence the state of resources as logged in the ledger.

With an agreement on that history, parties may then conduct a new transaction with a shared understanding of who has which resource and of their ability to trade that resource.”

Goals for the Technological features central to blockchains

- **Decentralized networks (evade centralized authorities and bottle-necks).**
- **Immutablity (prevents double spends).**
- **Trust-by-consensus (trust is built into the network rather than “assumed” among human participants).**
  - **Raises accountability standards**
  - **Polices both the bookkeeping and the bookkeepers**
  - **Cryptographically secured transactions**
- **Faster & cheaper exchanges (than other methods of exchange & validation) by cutting out the middleman.**
- **User Anonymity. Lowers identity issues--protects identity and privacy**

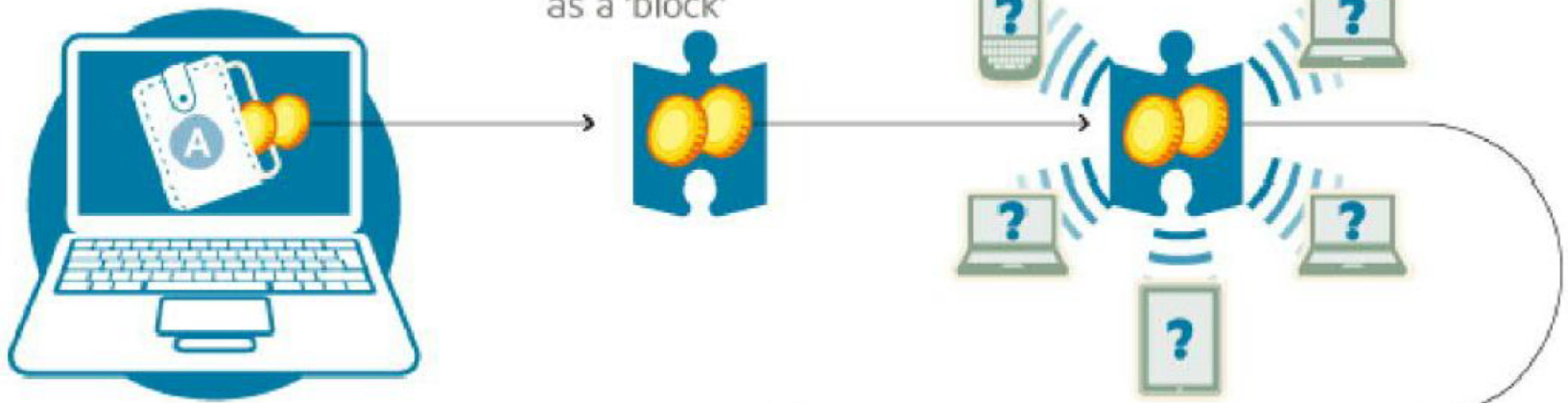
Blockchain: how does it work?

- **How Blockchain Works - in 2 Minutes**
  - https://www.youtube.com/watch?v=WiRFuHXHBhk&t=121s

A wants to send money to B

The transaction is represented online as a 'block'

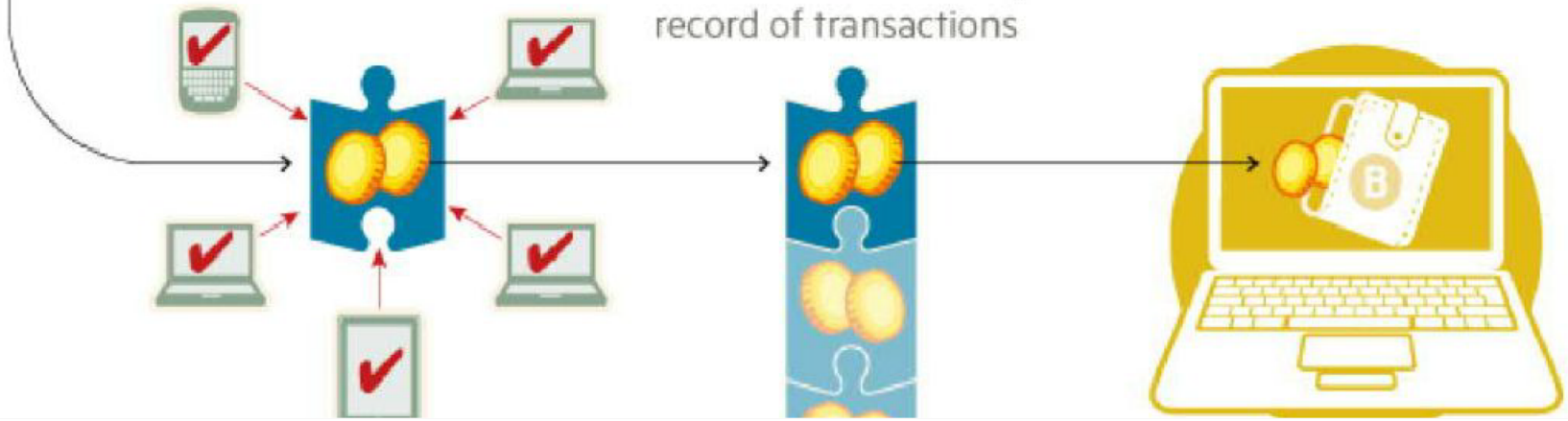
The block is broadcast to every party in the network



4 Those in the network approve the transaction is valid

5 The block then can be added to the chain, which provides an indelible and transparent record of transactions

6 The money moves from A to B



Blockchain 101 - A Visual Demo

- https://www.youtube.com/watch?v=_160oMzblY8&t=829s

Technological features central to blockchains

Asymmetric Key Encryption
Hash Values
Merkle Trees
Peer-to-Peer Networks
Ledgers
Transactions
Smart Contracts & Smart Property
Governance Procedures

Technological features central to blockchains:
Asymmetric Key Encryption

- **Asymmetric key encryption, also known as a public-private key cryptosystem, serves to create identities on a blockchain.**
- **A user creates two elements, a public key which helps identify their transactions on the blockchain, and a private key which is necessary to conduct a transaction with the public key.**
- **Asymmetric encryption allows for the authentication of users because only those with the private key can decrypt data encrypted with the public key or encrypt the data for public key decryption, thereby creating a signature.**

Technological features central to blockchains:

Hash Values

- A hash uses similar mathematical functions as an encryption method to produce a string of characters as an output given some data as input. This is a one-way function, meaning a hash value may be created from an input, but the input cannot be recreated from the hash.
- In blockchains, a number of transactions are tranched together to make a single block, which is then hashed.
- Hash values are used to validate the block's integrity. Any alterations to the transactions that make up a block will change the hash value of the block as a whole.
- If a block's hash value stays the same over time, users can have a high degree of confidence that the transactions in that block have not been tampered with. This allows users on the blockchain to determine whether or not they can trust the history of transactions on the blockchain.

Technological features central to blockchains:

Merkle Trees

- In a Merkle tree, data is segmented apart from a single whole data file.
- There is a root block of data with a hash value, then subsequent blocks of data (sometimes referred to as child, branch, or leaf blocks) that have their own hash value.
- Each subsequent block of data takes the hash value of their previous block (sometimes referred to as a parent block) as an input in the creation of the hash value of the new block.
- This creates a chain or tree of hash values, cryptographically tying new blocks of data to previous ones in a way that prohibits altering previous data.
- If data in a previous block were to be added, modified, or deleted, the hash value of the subsequent blocks of data would not compute to what they would need to be, alerting users that a change was made.
- This also allows hash values to be created for smaller, more discrete blocks of data. Hashing these smaller blocks is computationally.

Technological features central to blockchains:

Merkle Trees

- Blockchains borrow the concept of Merkle trees to make hash chains.
- In a blockchain, a first block is created and a hash value is computed for it. This is the root block.
- Subsequent blocks then use the hash value of the previous block in the chain as one of the inputs to create that next block.
- This chaining of hash values creates a strong relationship between blocks on the chain, and an auditable and immutable record of the transactions on the blockchain.

Technological features central to blockchains:
Peer-to-Peer Networks

- A peer-to-peer (P2P) network allows a disparate system of computers to connect directly with each other without the reference, instruction, or routing of a central authority. P2P networks allow for the sharing of files, computational resources, and network bandwidth among those in the network.
- In a blockchain, a P2P network allows the users of the blockchain to broadcast directly to and among each other the current state of the blockchain (so that users may agree on the history of transactions), and when a new block is added. This also allows for redundancy of the data in the blockchain, as any user may download a complete copy of the current ledger of transactions and add a new block, so that there will not be a single point of failure for the blockchain if a node on the network goes down.

Technological features central to blockchains:
Ledgers

- **Blockchain uses asymmetric encryption, hash values, Merkle trees, and P2P networks to build a ledger.**
- **The transactions captured in that ledger are not limited to financial ones (e.g., trading currency for goods and services).**
- **Those participating on a blockchain have a common understanding of how transactions are added and build upon one another, who can participate on the network, and how conflicts are resolved.**

Technological features central to blockchains:

Transactions

- Blockchains consist of a series of blocks of transactions.
- A transaction is an event in which a resource or asset changes possession from one party to another.
- These individual transactions are signed by the users engaging in those transactions through the use of public-private key encryption.
- Because the private key is necessary to release and accept a resource in a transaction on the blockchain, the users transacting on the blockchain are, in effect, signing the transaction to ensure its security.
- Transactions are grouped together and made into a block.
- In some blockchain implementations, these [blocks of transactions] are validated upon [its] creation through the act of *mining* for the creation of blocks.
- The integrity of the entire ledger is ensured by each block having a hash value which is dependent on the previous block's own hash value. Each of these three steps relies on strong cryptography which ensures the ledger's validity.

Technological features central to blockchains:
Smart Contracts & Smart Property

- **Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.**
- **Smart property can be physical such as car, house, smartphone etc. or it can be non-physical such as shares of a company.**

Technological features central to blockchains:
Governance Procedures

- **A blockchain can be *public* or *private*.**
- **In a *public* blockchain, anyone can create a public-private key pair and download a copy of the blockchain. This is usually accomplished through a software package which governs transactions on the blockchain.**
- **In a *private* blockchain, the membership of users on the blockchain is controlled. In private blockchains, the users authorized to participate may be bound by contractual relationships with each other, their blockchain addresses may be closely tied to their real-world identities, or participation on that blockchain may be agreed upon by other members in the blockchain.**

Technological features central to blockchains:
Governance Procedures

- **A blockchain can be *permissioned* or *permissionless*, which is independent of whether the blockchain is public or private.**
- **A *permissioned* blockchain is one in which the permission of a user is assigned to them. Some users may only be able to view a whole or portion of the blockchain; others may be able to add new blocks. In this system, the administrator(s) do not serve as a central authority, since they do not govern the creation of blocks on the blockchain, just the rights of users on the blockchain.**
- **In a *permissionless* blockchain, all users have equal rights, with any one able to download the full blockchain and have an opportunity to potentially add additional blocks.**

Technological features central to blockchains:

Additional Terminology

- ***Consensus***: Users on the blockchain must reach *consensus* on the rules for creating and publishing new blocks and resolving disagreements.
- ***Users***: The *users* on a blockchain could be the individuals, businesses, or other identities which have a public-private key pair and conduct transactions.
- ***Nodes***: A *node* is a computing system on that blockchain.
- ***Mining***: The creation and publication of a new block in the blockchain is called *mining.*
- ***Proof of Work scheme:*** In a *proof of work* scheme, those seeking to add a block to the blockchain are presented a difficult computational problem. By solving the problem, they win the opportunity to post the next block and possibly a reward for doing so. Their solution is broadcast to others users who can validate it immediately without going through the same resource intensive computation required to solve the problem.
- ***Proof of stake* scheme**: In a *proof of stake* scheme, the next block may be awarded to the user who has an appropriate stake in that block.
- ***Round Robin* scheme**: In the *round robin* scheme, users on the network take turns adding new blocks. Because some level of trust is necessary for round robin schemes to work, they are used in permissioned blockchains.

Q&A? Blockchain:
What is it and how does it work?