




BLOCKCHAIN TECHNOLOGY

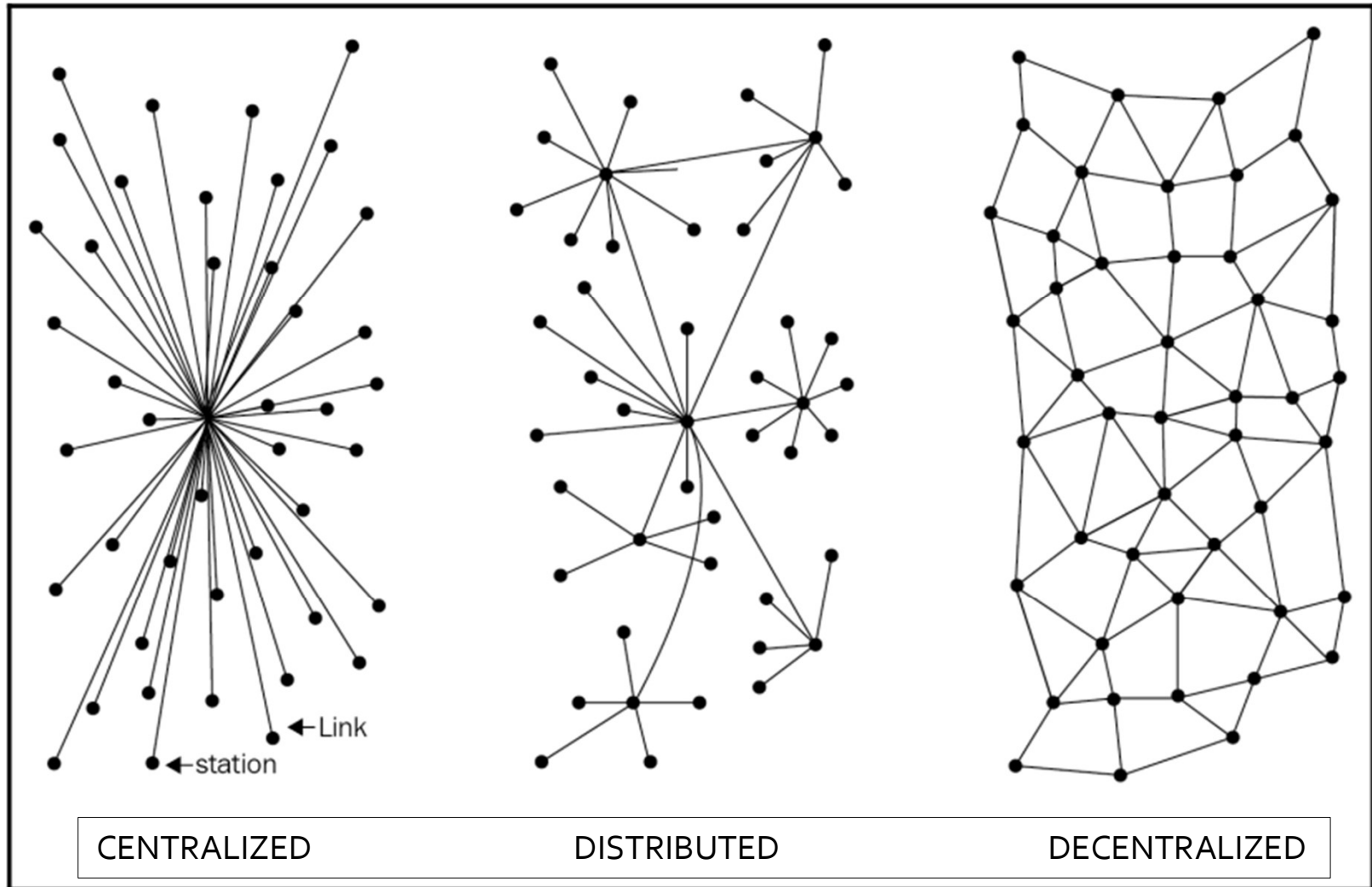
Decentralization



Introduction

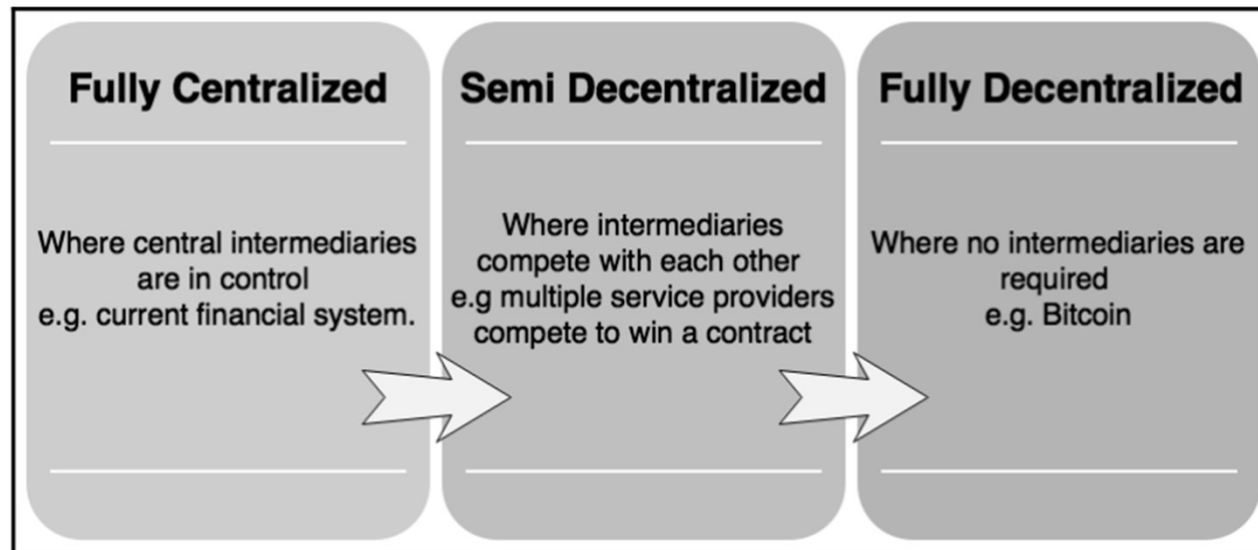
- Decentralization is not a new concept
 - has been used in strategy, management, for a long time
 - The basic idea is to
 - distribute control and authority to the peripheries of an organization instead of one central body being in full control of the organization.
 - produces several benefits for organizations
 - increased efficiency
 - accelerated decision making
 - better motivation
 - reduced load on top management
- 

Decentralization using blockchain




Methods of decentralization

- Disintermediation
 - Omitting intermediaries (e.g., banks)
- Contest-driven decentralization
 - different service providers compete in order to be selected
 - will not result in full decentralization
 - ensures that a service provider is not monopolizing the service (to a certain degree)






Benefits and challenges

- Benefits
 - Transparency
 - Efficiency
 - Cost saving
 - Development of trusted ecosystems
 - Privacy and anonymity (in some cases)
 - Challenges
 - security requirements
 - software bugs
 - human errors
- 



Benefits and challenges

- Essential perception
 - not everything can or needs to be decentralized
 - In what circumstances is blockchain preferred over traditional databases?
 1. Is high data throughput required? If the answer to this question is yes, then use a traditional database.
 2. Are updates centrally controlled? If yes, then use a conventional database.
 3. Do users trust each other? If yes, then use a traditional database.
 4. Are users anonymous? If yes, then use a public blockchain; if not, then use a private blockchain.
 5. If consensus is required to be maintained within a consortium then use a private blockchain, otherwise use a public blockchain.
 - Other aspect should also be considered
 - immutably
- 




How to decentralize

- Four questions whose answers provide a clear understanding
 - What is being decentralized?
 - What level of decentralization is required?
 - disintermediation or partial disintermediation
 - What blockchain is used?
 - Bitcoin, Ethereum, or any other blockchain
 - What security mechanism is used?
 - atomicity-based
 - either the transaction executes in full or does not execute at all
 - ensures the integrity of the system
 - based on reputation
 - allows for varying degrees of trust in a system




Blockchain and full ecosystem decentralization

- To achieve complete decentralization
 - it is necessary that the environment around the blockchain also be decentralized
- The blockchain is a distributed ledger that runs on top of conventional systems
 - Storage
 - Communication
 - Computation



Blockchain and full ecosystem decentralization

- Storage
 - Data can be stored directly in a blockchain
 - not suitable for storing large amounts of data by design
 - can store simple transactions and some arbitrary data
 - certainly not suitable for storing images or large blobs of data
- 




Blockchain and full ecosystem decentralization

- Storage
 - A better alternative: use Distributed Hash Tables (DHTs)
 - initially used in peer-to-peer software (BitTorrent)
 - the issue:
 - there is no incentive for users to keep the files indefinitely
 - Data may not be accessible if someone leaves the network




Blockchain and full ecosystem decentralization

- Storage
 - Two primary requirements
 - high availability
 - data should be available when required
 - link stability
 - network links also should always be accessible
- 



Blockchain and full ecosystem decentralization

- Storage
 - Other alternatives for data storage
 - InterPlanetary File System (IPFS)
 - Filecoin
 - Ethereum Swarm
- 



Blockchain and full ecosystem decentralization

- Communication
 - The internet is considered to be decentralized, but
 - Access to the internet is based on ISPs who act as a central hub for users
 - Services such as email and online storage are based on unconditional trust of a central authority
 - An alternative is to use mesh networks
 - they are limited in functionality when compared to the internet
 - they still provide a decentralized alternative
 - nodes can talk directly to each other without a central hub such as an ISP
 - An example of is FireChat
 - allows iPhone users to communicate with each other directly



Blockchain and full ecosystem decentralization

- Computation
 - Decentralization can be achieved by a blockchain technology such as Ethereum
 - smart contracts
 - decentralized programs with
 - embedded business logic
 - limited amount of data
 - do not necessarily need a blockchain to run
 - can run on the blockchain network
 - blockchain has become a standard execution platform
 - due to the security benefits



Blockchain and full ecosystem decentralization

- Decentralized Organizations (DOs)
 - software programs that run on a blockchain
 - based on the idea of actual organizations with people and protocols.
 - Can be added to the blockchain in the form of a smart contract or a set of smart contracts
 - parties interact with each other based on the code defined within the DO software.



Blockchain and full ecosystem decentralization

- Decentralized Autonomous Organizations (DAOs)
 - code is considered the governing entity rather than people or paper contracts
 - a human curator
 - maintains the code
 - acts as a proposal evaluator for the community
 - can hire external contractors
 - if enough input is received from the participants



Blockchain and full ecosystem decentralization

- Decentralized Autonomous Organizations (DAOs)
 - most famous DAO project is The DAO
 - was designed to be a venture capital fund
 - aimed at providing a decentralized business model with no single entity as owner.
 - Unfortunately
 - this project was hacked due to a bug in the DAO code
 - millions of dollars' worth in Ether was siphoned out of the project and into a child DAO created by hackers.
 - A hard fork was required on the Ethereum blockchain to reverse the impact of the hack
 - This incident opened the debate on the security, quality, and need for thorough testing of the code in smart contracts





Blockchain and full ecosystem decentralization

- Decentralized Autonomous Societies (DASs)
 - a concept whereby an entire society can function on a blockchain with the help of multiple, complex smart contracts and a combination of DAOs and Decentralized Applications running autonomously.
 - does not necessarily translate to a free-for-all approach
 - nor is it based on an entirely libertarian ideology
 - many governmental services can be delivered via blockchains
 - government identity card systems
 - Passports
 - records of deeds, marriages, and births.
 - Another theory
 - if a government is corrupt and do not provide the satisfactory levels of trust
 - society can start its own virtual one on a blockchain
 - driven by decentralized consensus and transparency.
 - might look like a libertarian's dream
 - but it is entirely possible on a blockchain.



Blockchain and full ecosystem decentralization

- Decentralized Applications (DApps)
 - DAOs, DASs, and DOs are Dapps
 - run on top of a blockchain in a peer-to-peer network
 - represent the latest advancement in decentralization technology
 - are software programs that
 - can run on their respective blockchains (Type I)
 - use an existing established blockchain (Type II)
 - use only the protocols of an existing blockchain (Type III)



Blockchain and full ecosystem decentralization

- Decentralized Applications (DApps)
 - Requirements to be considered DApp
 1. should be fully open source and autonomous
 - no single entity should be in control of most of its tokens.
 - All changes to the application must be consensus-driven based on the feedback given by the community
 2. Data and records of operations must be
 - cryptographically secured
 - stored on a public, decentralized blockchain
 - to avoid any central points of failure



Blockchain and full ecosystem decentralization

- Decentralized Applications (DApps)
 - Requirements to be considered as a DApp
 3. A cryptographic token must be used
 - to provide access and rewards to those who contribute value to the applications
 4. The tokens must be generated by the DApp
 - according to a standard cryptographic algorithm



Blockchain and full ecosystem decentralization

- Decentralized Applications (DApps)
 - Examples
 - KYC-Chain
 - provides the facility to manage Know Your Customer (KYC) data
 - securely and conveniently
 - based on smart contracts
 - OpenBazaar
 - enables commercial activities directly between sellers and buyers (with no central party, such as eBay and Amazon)
 - is not built on top of a blockchain
 - DHTs are used in a peer-to-peer network
 - makes use of Bitcoin and various other cryptocurrencies as a payment method





Blockchain and full ecosystem decentralization

- Platforms for decentralization
 - Ethereum
 - Cardano
 - Polkadot
 - Solana
- 