

CHAPTER 2

DECENTRALIZATION

From : Mastering Blockchain

By – Imran Bashir

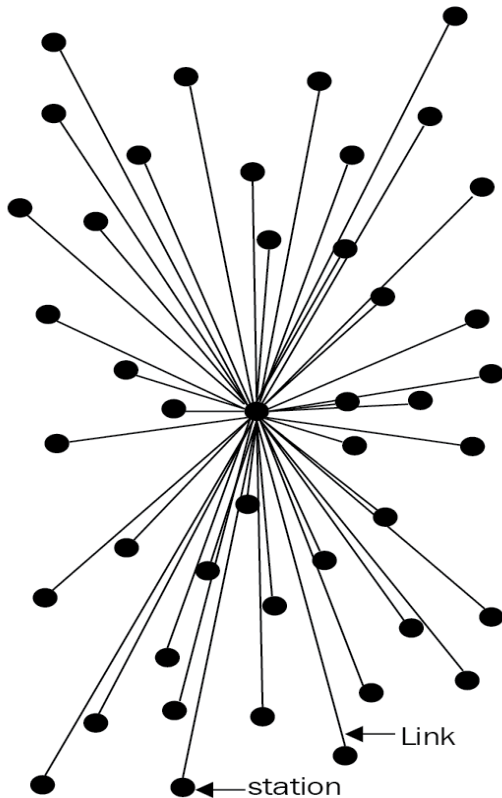
www.packet.com

Decentralization

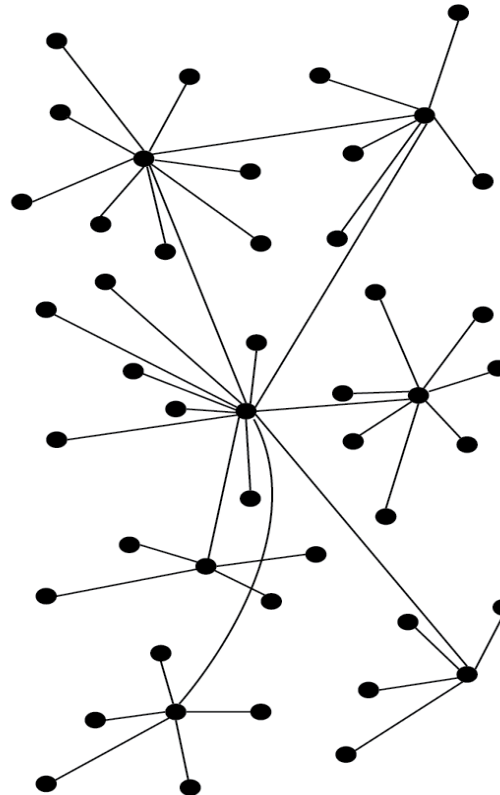
- ▣ Distributed control
- ▣ Distributed authority
- ▣ Benefits :
 - increased efficiency,
 - quicker decision making,
 - better motivation,
 - reduced burden on top management

Different types of network/system

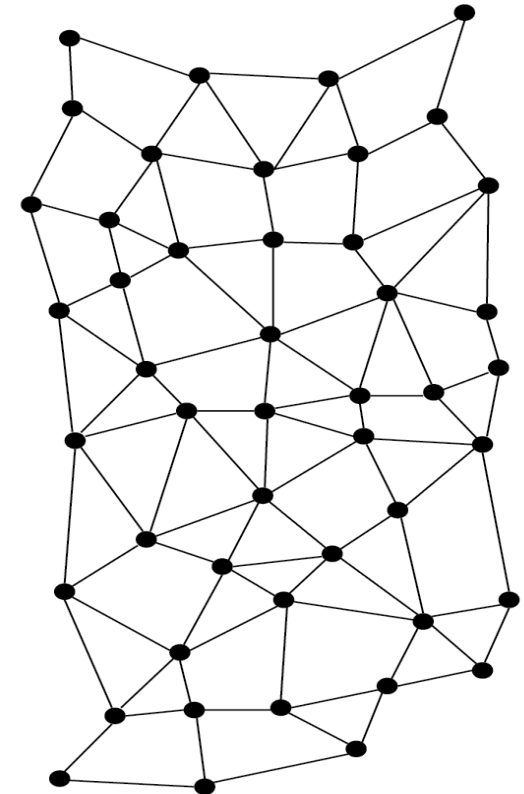
As appeared in paper by Paul Baran on distributed communication networks



CENTRALIZED



DECENTRALIZED



DISTRIBUTED

Methods of decentralization

Two methods –

1. Disintermediation :

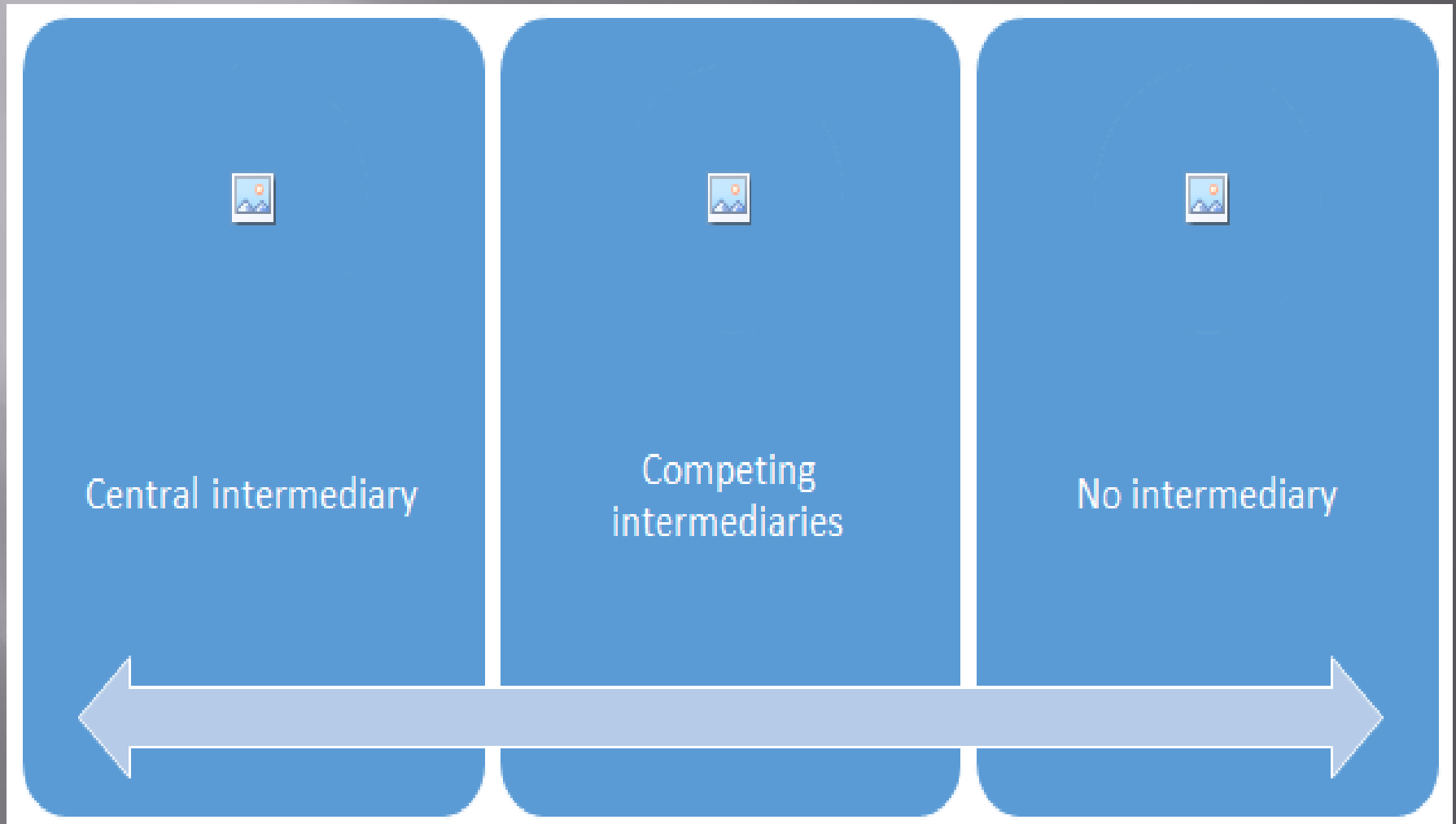
- ▣ Imagine you want to send money to your friend in another country. You go to a bank that will transfer your money to the bank in the country of your choice for a fee.
- ▣ In this case, the bank keeps a central database that is updated, confirming that you have sent the money.
- ▣ With blockchain technology, it is possible to send this money directly to your friend without the need for a bank.
- ▣ All you need is the address of your friend on the blockchain.
- ▣ This way, the intermediary is no longer required and decentralization is achieved by disintermediation.
- ▣ However, it is debatable how practical decentralization is in the financial sector by disintermediation due to heavy regulatory and compliance requirements.

Methods of decentralization

2. Through competition :

- a group of service providers compete with each other in order to be selected for the provision of services by the system.
- Does not achieve complete decentralization, but to a certain degree ensures that an intermediary or service provider is not monopolizing the service.
- In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service.
- This will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria mentioned earlier.
- This way, an environment of competition is cultivated among service providers, whereby they compete with each other to become the data provider of choice.

Scale of Decentralization



How to decentralize

- ▣ Decentralization Framework proposes four questions –
 1. What is being decentralized? E.g. ID system
 2. What level of decentralization is required? e.g. full or partial disintermediation
 3. What blockchain is used? E.g. Bitcoin/Ethereum
 4. What security mechanism is used? E.g. Atomicity/reputation

Blockchain and Full Ecosystem Decentralization

Identity, Wealth

Blockchain

Ethereum, Hyperledger

Storage

File System (IPFS), Database (BigChainDB)

Communication

The internet, Meshnets

Smart contract

- ▣ A smart contract can be thought of as a small decentralized program. Smart contracts do not necessarily need a blockchain to run;
- ▣ However, due to the security benefits that the blockchain technology provides, it is now becoming almost a standard to use blockchain as a decentralized execution platform for smart contracts.
- ▣ A smart contract usually contains some business logic and a limited amount of data.
- ▣ These small programs reside on the blockchain and execute business logic if some specific criteria are met.

Decentralized organizations

- ▣ **Decentralized organization (DOs)** are software programs that run on a blockchain and are based on the idea of real human organizations with people and protocols.
- ▣ Once a DO, in the form of a smart contract or a set of smart contracts, is added to the blockchain, it becomes decentralized and parties interact with each other based on the code defined within the DO software.

Decentralized autonomous organizations

- ▣ Just like DOs, a **Decentralized autonomous organization (DAO)** is also a computer program that runs on top of a blockchain and embedded within it are governance and business logic rules.
- ▣ DAO and DO are basically the same thing, but the main difference is that DAOs are autonomous, which means that they are fully automated and contain artificially intelligent logic, whereas DOs lack this feature and rely on human input in order to execute business logic.
- ▣ **Ethereum** blockchain led the way with the introduction of DAOs for the first time.

Decentralized autonomous corporations

- ▣ DAOs, Decentralized autonomous corporations (DACs) are a similar concept but are considered a **smaller subset of DAOs**.
- ▣ The definitions of DACs and DAOs can sometimes overlap, but a general difference is that DAOs are usually considered to be non-profit, whereas **DACs can make money via shares** offered to the participants and by paying dividends.
- ▣ These corporations can run a business **automatically** without human intervention based on the **logic programmed** within them.

Decentralized autonomous societies

- ▣ Decentralized autonomous societies (DASs) are a concept whereby entire societies can function on a blockchain with the help of **multiple complex smart contracts and a combination of DAOs** and Decentralized applications (DAPPs) running autonomously.
- ▣ This model does not mean an outlaw approach, nor is it based on a totally libertarian ideology; instead, many services that a government offers can be delivered via blockchain, **such as Government Identity Card systems, passport issuance, and records of deeds, marriages, and births.**

Decentralized applications

- ▣ All ideas mentioned earlier come under the larger umbrella of decentralized applications.
- ▣ All DAOs, DACs, and DOs are **basically decentralized applications** that run on top of a blockchain in a peer-to-peer network.
- ▣ This is the latest advancement in technology with regard to decentralization.
- ▣ Decentralized applications or **DAPPs are software programs that can run on their own blockchain**, use another already existing established blockchain, or use only protocols of an existing blockchain solution.
- ▣ These are called Type I, Type II, and Type III DAPPs

Requirements of a DAPP

1. The DAPP should be **fully open source and autonomous** and no single entity should be in control of a majority 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 of the application must be **cryptographically secured and stored on a public,** decentralized blockchain in order to avoid any central points of failure.
3. A **cryptographic token** must be used by the application in order to **provide access and rewards** to those who contribute value to the applications, for example, miners in bitcoin.
4. The **tokens must be generated** by the decentralized application according to a standard cryptographic algorithm. This generation of tokens acts as a proof of the value to contributors (for example, miners).

Platforms for Decentralization

Ethereum -

- ▣ Ethereum tops the list as being the first blockchain that introduced a Turing-complete language and the concept of a virtual machine.
- ▣ With the availability of this Turing complete language called Solidity, endless possibilities have opened for the development of decentralized applications.

Platforms for Decentralization

Maidsafe-

- ▣ Maidsafe provides a SAFE (Secure Access for Everyone) network that is made up of unused computing resources, such as storage, processing power, and the data connections of its users.
- ▣ The files on the network are divided into small chunks of data that are encrypted and distributed throughout the network randomly. This data can only be retrieved by its respective owner.
- ▣ One key innovation is that duplicate files are automatically rejected on the network, which helps reduce the need for additional computing resources to manage the load.
- ▣ It uses **Safecoin** as a token to incentivize its contributors.

Platforms for Decentralization

Lisk -

- ▣ Lisk is a blockchain application development and cryptocurrency platform. It allows developers to use JavaScript to build decentralized applications and host them in their own respective sidechains.
- ▣ Lisk uses the **Delegated Proof of Stake (DPOS)** mechanism for consensus whereby 101 nodes can be elected to secure the network and propose blocks.

