Blockchain Technology

Beni Iyaka H00181266
bi34@hw.ac.uk
MSc Software Engineering
2016 - 2017

Outline

- What is Blockchain Technology?
- Overview
- History
- Characteristics
- Description
- Principles
- Benefits
- Challenges
- Blockchain Technology as a Network
- Blockchain technology Evolution
- Further Readings

What is Blockchain Technology?

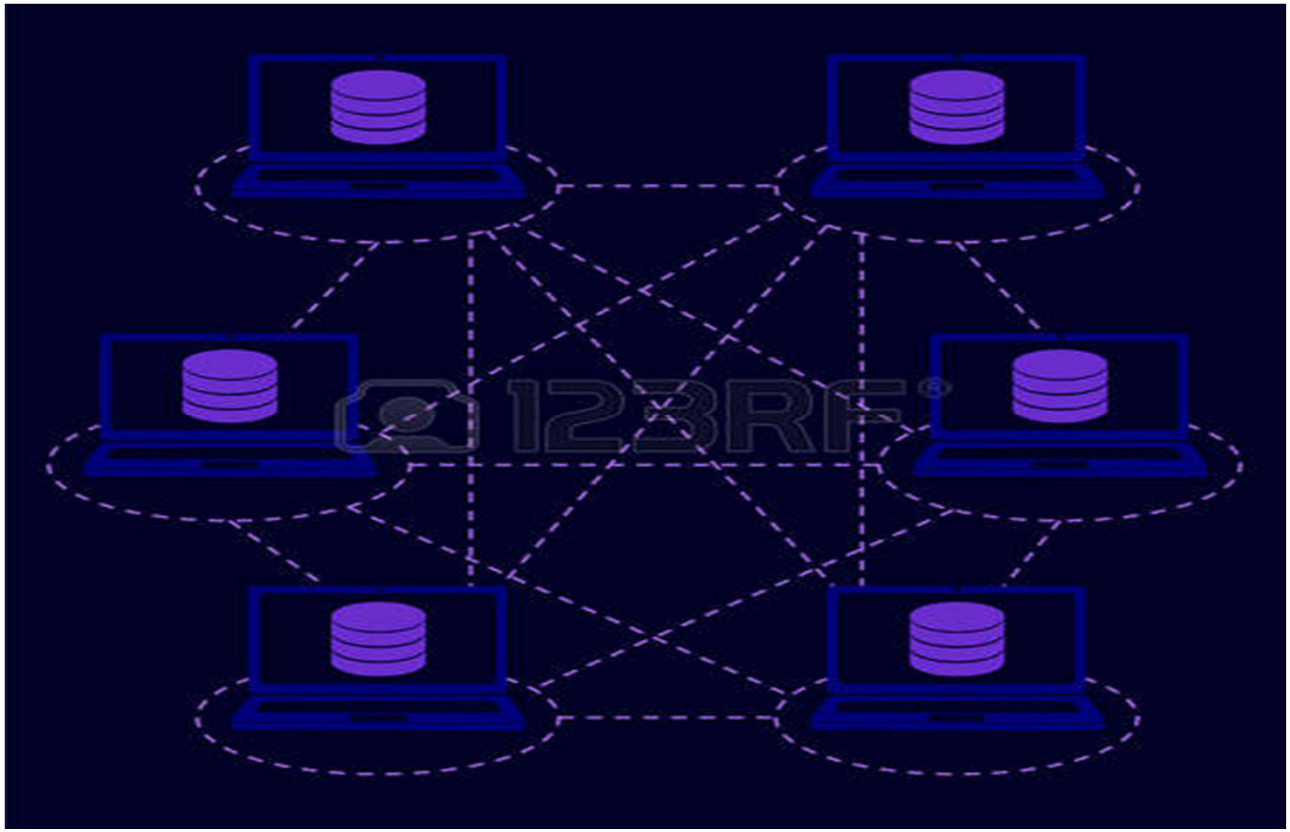
- A way to structure data and the foundation of cryptocurrencies like Bitcoin.
- A transactional application that establishes trust, accountability and transparency while observing the business process.
- A process used to vastly reduce cost and complexity of cross enterprise processes.

Source: Wright, Aaron, and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia." *Available at SSRN 2580664*(2015).

- A transactional method used to monitor transactions without the use of a 3rd party.
- Blockchain technology is a protocol for building an immutable historical record of transaction.

Source: Wright, Aaron, and Primavera De Filippi. "Decentralized blockchain technology and the rise of lex cryptographia." *Available at SSRN 2580664*(2015).

What is Blockchain?



Source: http://www.centrodeinnovacionbbva.com/sites/default/files/blockchain-cibbva.jpg

Overview of Blockchain Technology

Blockchain is a combination of old system ways in a new way. Of which some of these ways are:

- Cryptographic signatures.
- Peer to Peer Network.
- Hashing functions.
- Public/Private key cryptography.
- Elliptic curve cryptography.
- Distributed System.

Pilkington, M., 2016. Blockchain technology: principles and applications. *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*.

History

- The first block was invented in 2009.
- Blockchain technology was invented by Satoshi Nakamoto which is the fiction name used.
- Blockchain Technology was then adopted by Crypto-geeks.
- In december 2010, Satoshi posted something which turned out to be his/her last post.

Pilkington, M., 2016. Blockchain technology: principles and applications. *Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar*.

- Maybe his name is Satoshi Nakamoto.
- But I don’t think so.
- He mostly doesn’t know how to code unless code of fighting
- I’m sure he knows nothings about Cryptography.

Characteristics of Blockchain Technology

- Durability

- Blockchain Technology is safe for long term storage since it can be moved around.

- Portability

- Blockchain Technology can be moved around resulting to it being durable.

- Divisibility

- Blockchain Technology can be used in small amount

- Limited Supply

  - Blockchain Technology will help maintain value of our resources because it allows us to have small equal amount.

- Acceptability

  - Blockchain Technology allows us to spend it around.

- Uniformity

- Blockchain Technology can be used in small amounts, those small amounts are equal.

Description of Blockchain Technology

- No third party required

- Blockchain Technology builds a direct link between consumers and suppliers by removing the need of a third party. Because:
  * When a third party is required, the risk of fraud by the 3rd party is high.
  * When the flow is too complex, the more third parties are required. E.g.: Banks, Transaction.
  * The easier it is to do a transaction, the more people transact.

- Blockchain Technology can reduce liquidity by giving us a way to reduce friction through the mathematical validation of transaction.

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRWJAfw05yA102xB1YRKPpYWt0C7ldmIZr4X9S1Hvvm-VRlqtnP

- Most people think of it as the technology behind Bitcoin; but blockchains technology potential extend far beyond digital currencies.

https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcQeqpxvozynBitJFkcH0_as_7KoaLnaFY016JjjKWXHnz63gWsL

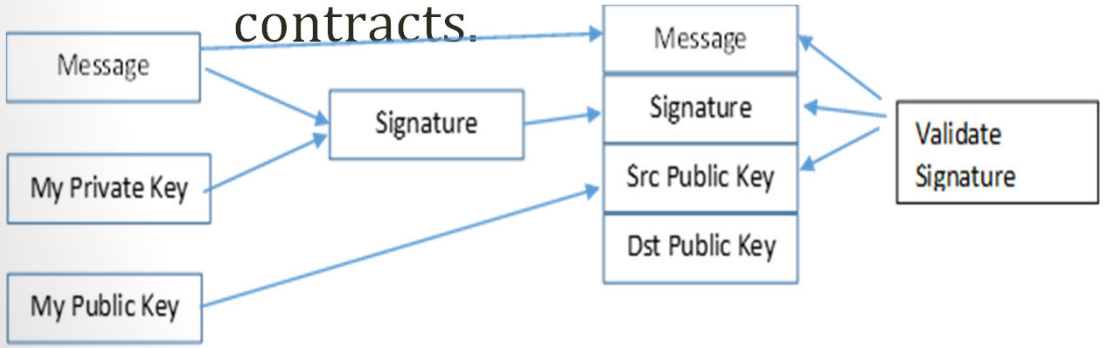
Blockchain Technology helps us use Digital signature:

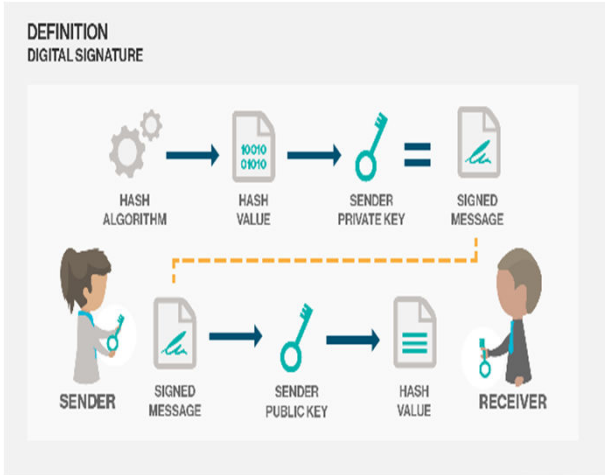
* To verify possession of private key.

* To verify that messages came from the right person.

* Verify that messages haven't been changed or tampered with.

* Allow fine grained version control contracts.





Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

Blockchain Technology provides us with signed blocks of transactions so as:

* To preserve the sequence of transactions.

* To allow fine-grained access control at the level of a transaction.

* To create continually updated audit trials.

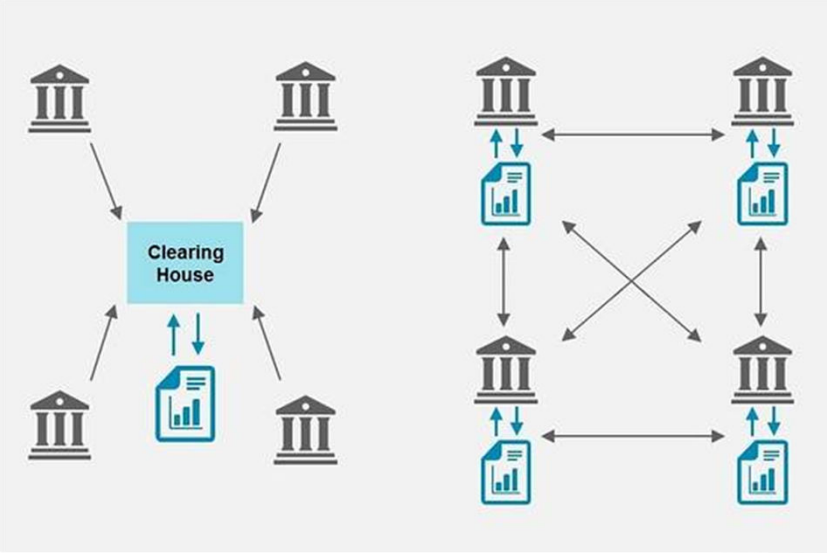
Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

Blockchain Technology helps with distributed ledgers to:

* Establish a single version.

* Reduce or eliminate the need for centralized third parties.

* Open the door to the autonomous agents, processes and organisations implied by smart contract technology.



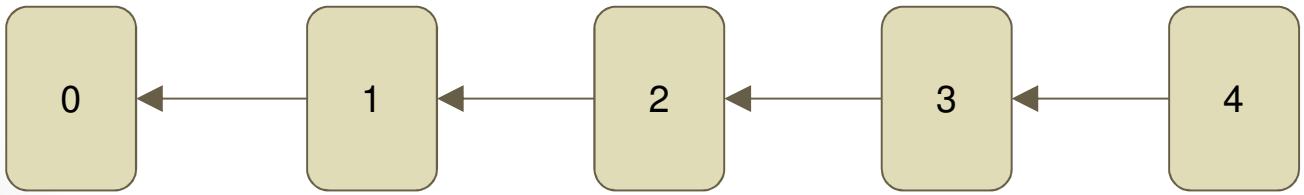
Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- Blockchain Technology makes us go back to the peer to peer system.
- Blockchain Technology is fast compare to other technology.
- No special equipment is needed while doing the transaction.
- Trust a trustless system by making use of encryption system public key and private key; of which, Public key is the identity of a user in a blockchain while the private key is known by it owner only.

- Make the transaction at minimal cost possible
- Since it is a peer to peer system, no chargebacks is required.
- No monthly fees.
- It provides transparency to the transaction.
- Remove the need of special.
- Remove fraud.

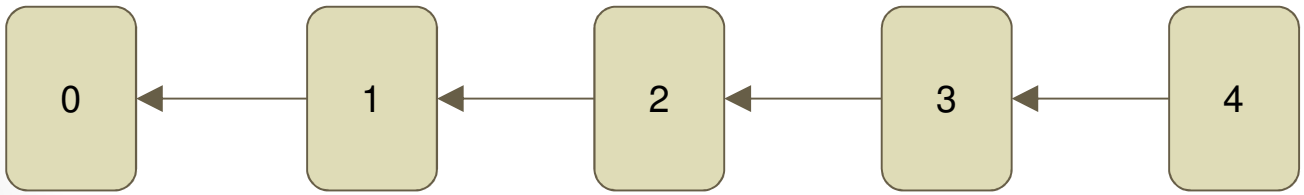
Principles of Blockchain Technology

- Blockchain makes sure that all the transactions are grouped together into a block to form a chain.
- The chain represent a set of blocks linked together.
- The blocks are numbered in an ascending order.
- Once a block is stored, it becomes read-only.



Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- Blockchain makes sure that all the transactions are grouped together into a block to form a chain.
- The chain represent a set of blocks linked together.
- The blocks are numbered in an ascending order.
- Once a block is stored, it becomes read-only.



Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- To create a new block, blockchain technology uses a process called mining which automatically creates a block on a certain time average.

- For bitcoin, the average time is 10minutes.

Benefits of Blockchain Technology

- Empowered users
- Blockchain Technology technology gives the user full control of their information and transactions.
- Disintermediation and trustless exchange
- Blockchain Technology allows two concerned parties to make exchange without an intermediate of a 3rd party; resulting to a strong reduction or elimination of any counterparty risk.

Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- Durability, Reliability and Lastingness

- Blockchain Technology is categorized as a Decentralized network; therefore, there is no central point of failure and it is better editable to resist malicious attacks.

Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- Faster Transaction

- Transaction within Banks can take days for clearing and mostly after working hours. Blockchain Technology was designed to reduce transaction times and also to be processed 24/7.

- Transparency and Immutability

- Blockchain Technology provides transparency by providing a publicly viewable changes to public blockchain.

Source: Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

Some challenges that comes with Blockchain Technology

- Lack of privacy
- Since Blockchain Technology provides transparency, all the user's transactions are out there for people to see.
- Lack of Scalability
- Since Blockchain Technology provides a peer to peer transaction, it is quite difficult to perform a peer to peer transaction with someone in another country/continent without the need of a 3rd party like a Bank.

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

- Blockchain Technology provides digital tokens which are like money, it can be locked up with different multi signature security but once someone else get access to them, they are gone.

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

Blockchain Technology as a Network

There a 3 types of network namely:

- Centralized network
- Decentralised Network
- Distributed Network

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

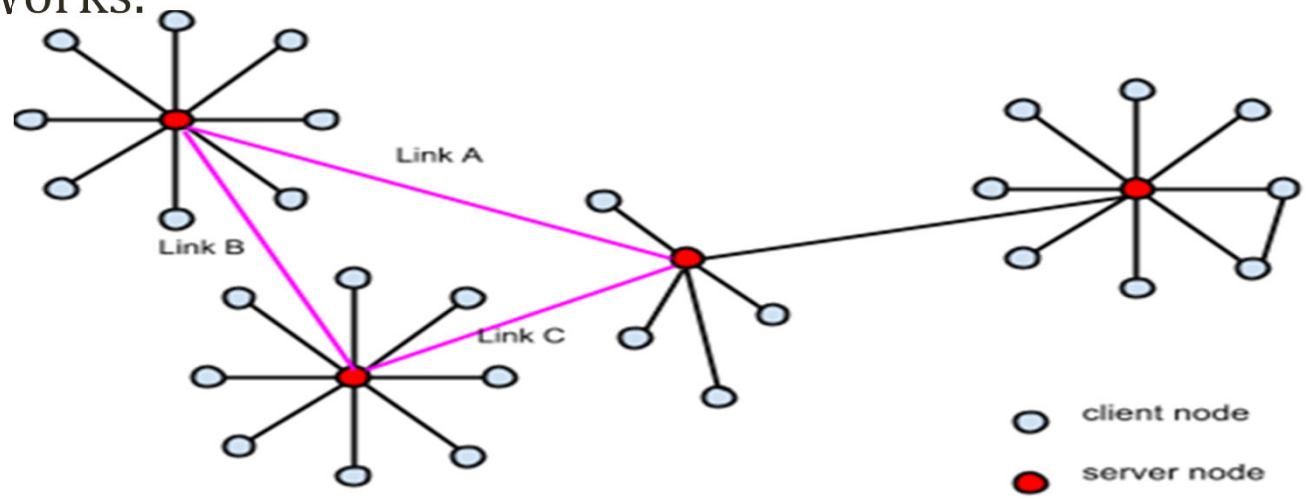
Centralised Network

- This is a Type of network whereby all users are connected to a central server, which is acting as the heart of the network.

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

Decentralised Network

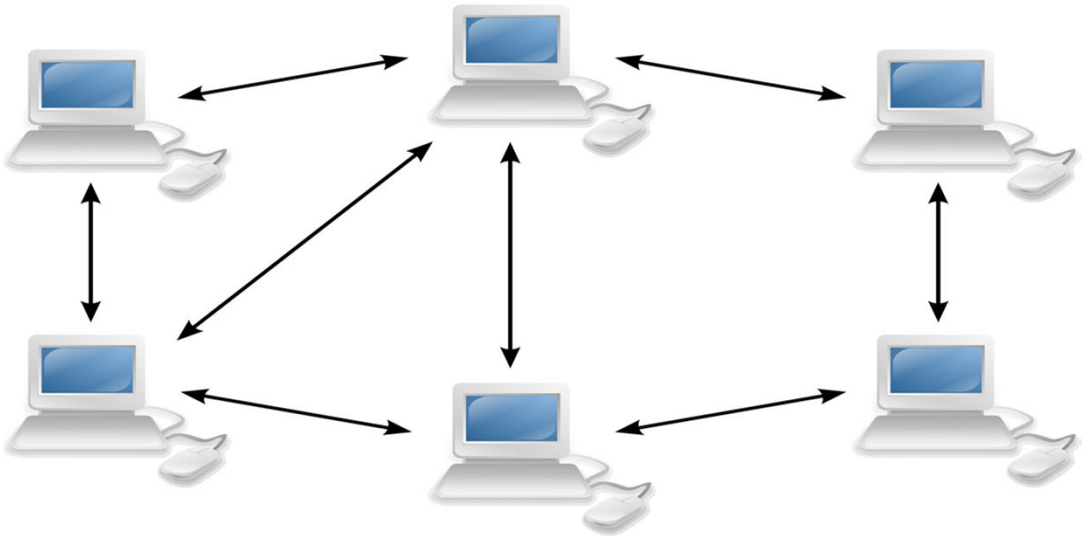
- This is a combination of centralised and distributed network because each node in the network is connected to their network server and also to the server in other networks.



Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

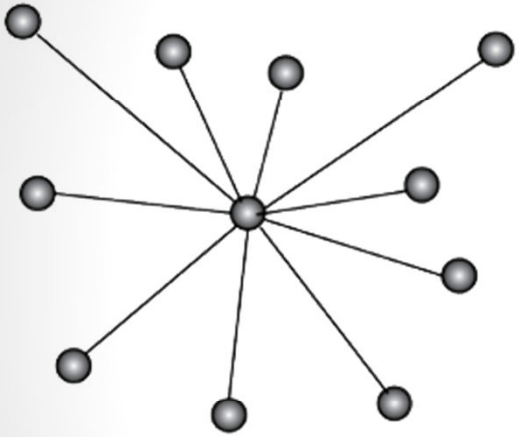
Distributed Network

- This is a type of network whereby all the nodes within the network are connected with one another.

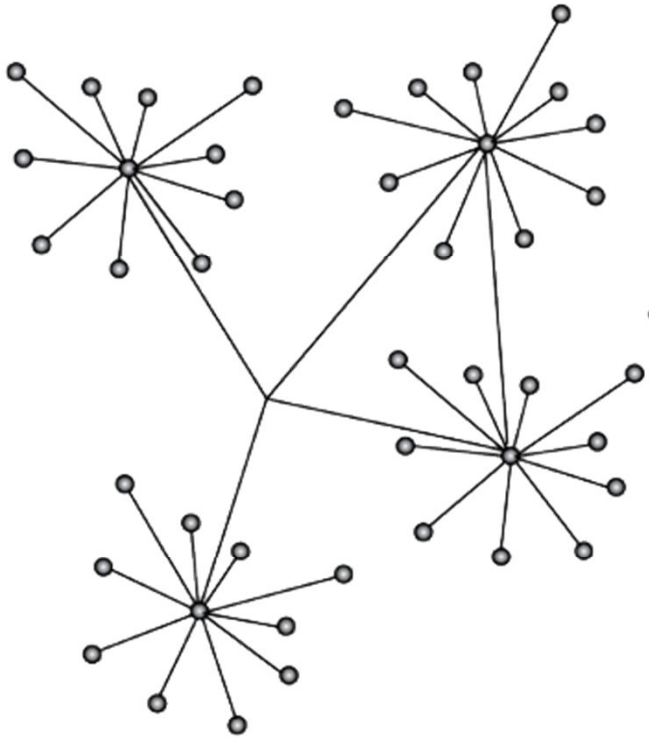


Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

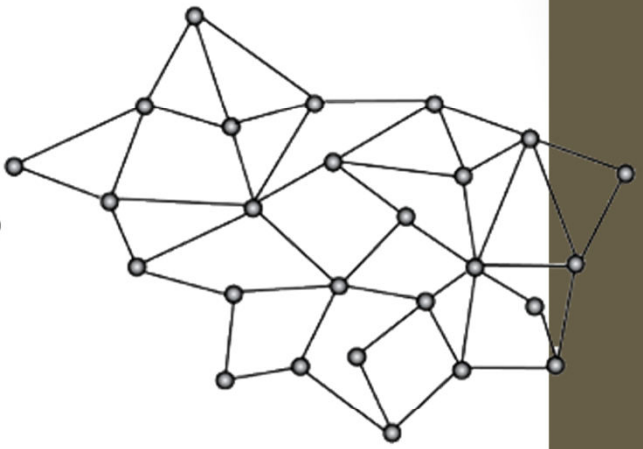
Network Evolution



i) centralized Network

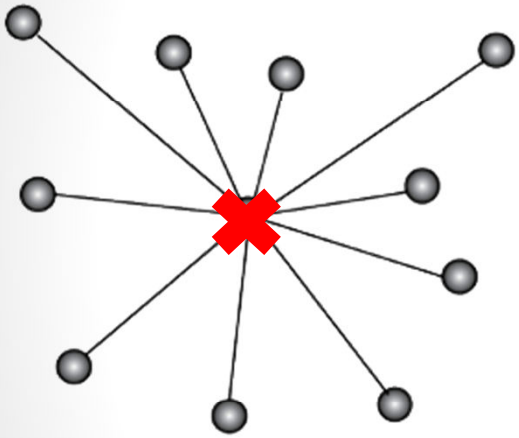


ii) decentralized network

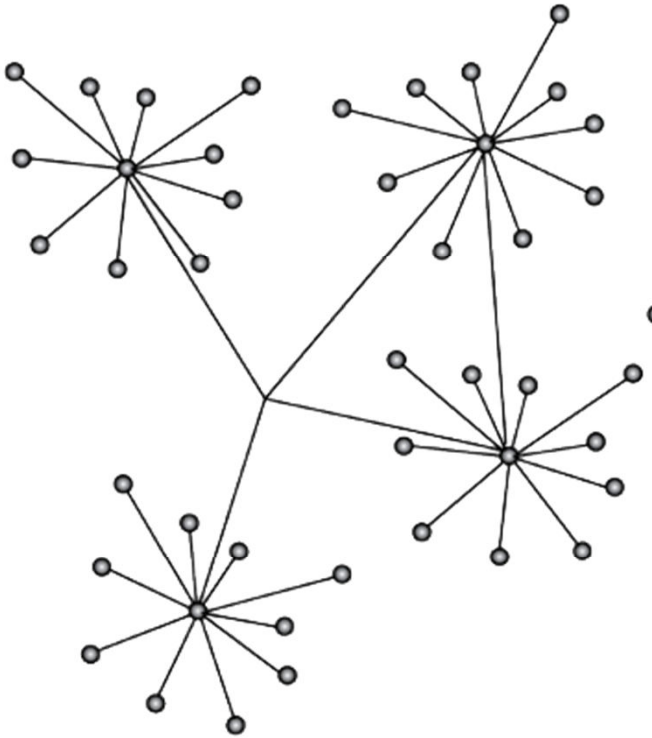


iii) distributed network

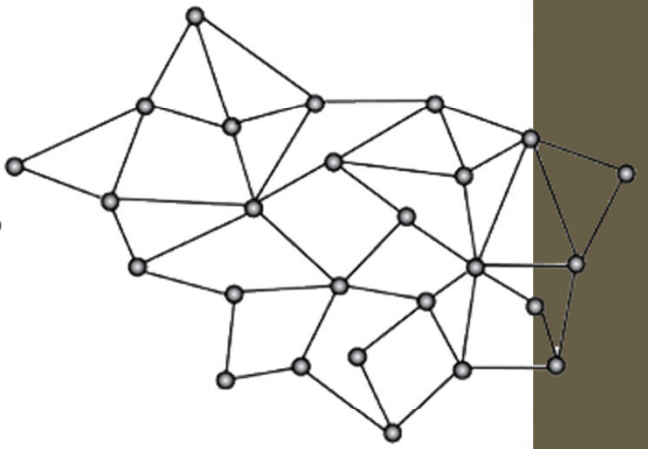
Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.



i) centralized

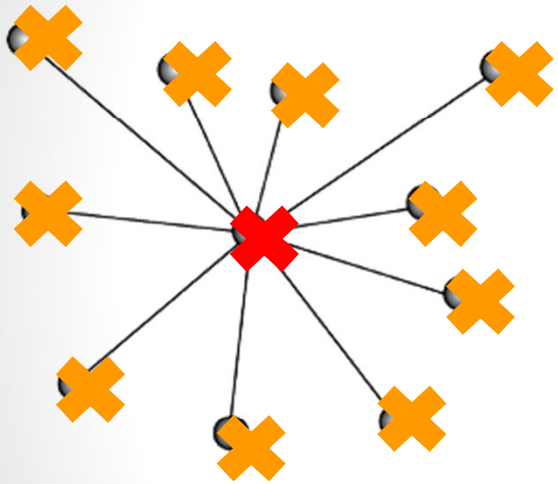


ii) decentralized

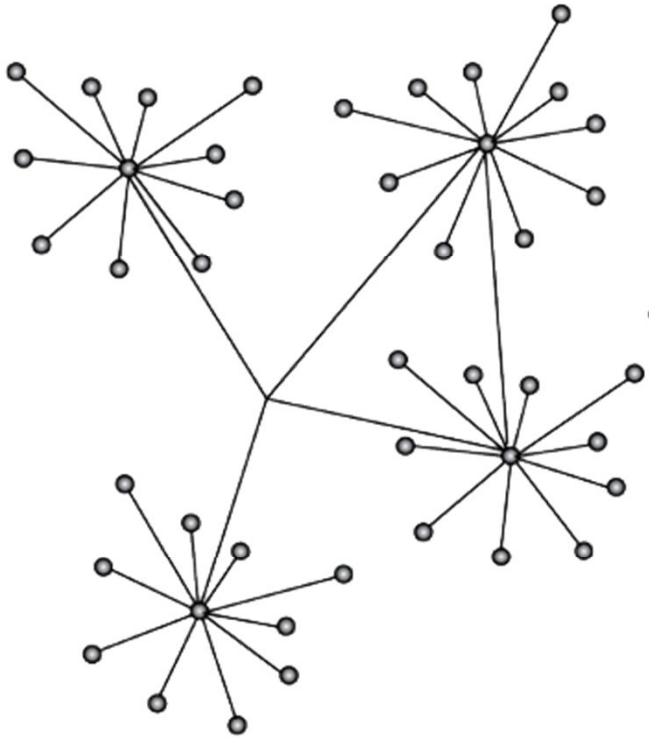


iii) distributed

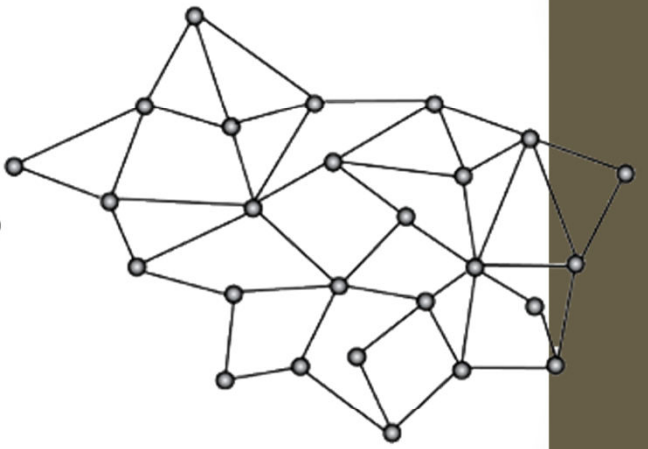
Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.



i) centralized

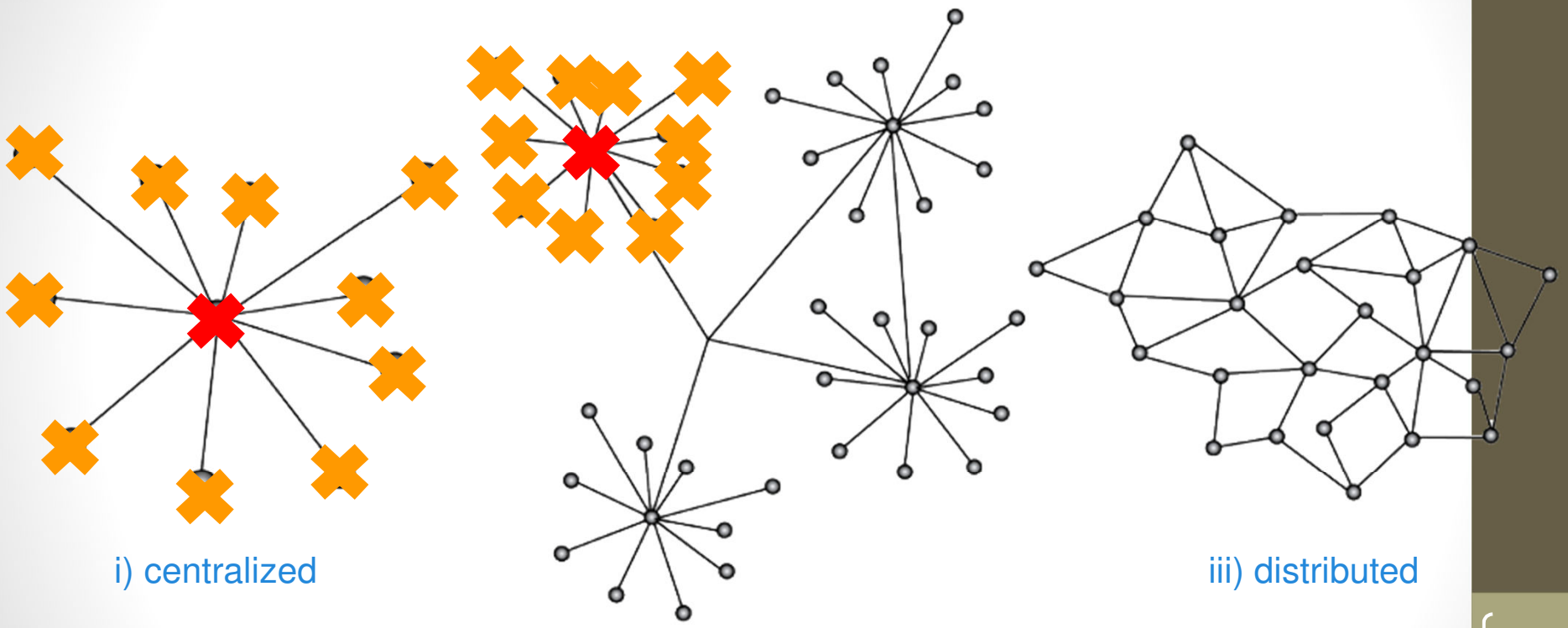


ii) decentralized



iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

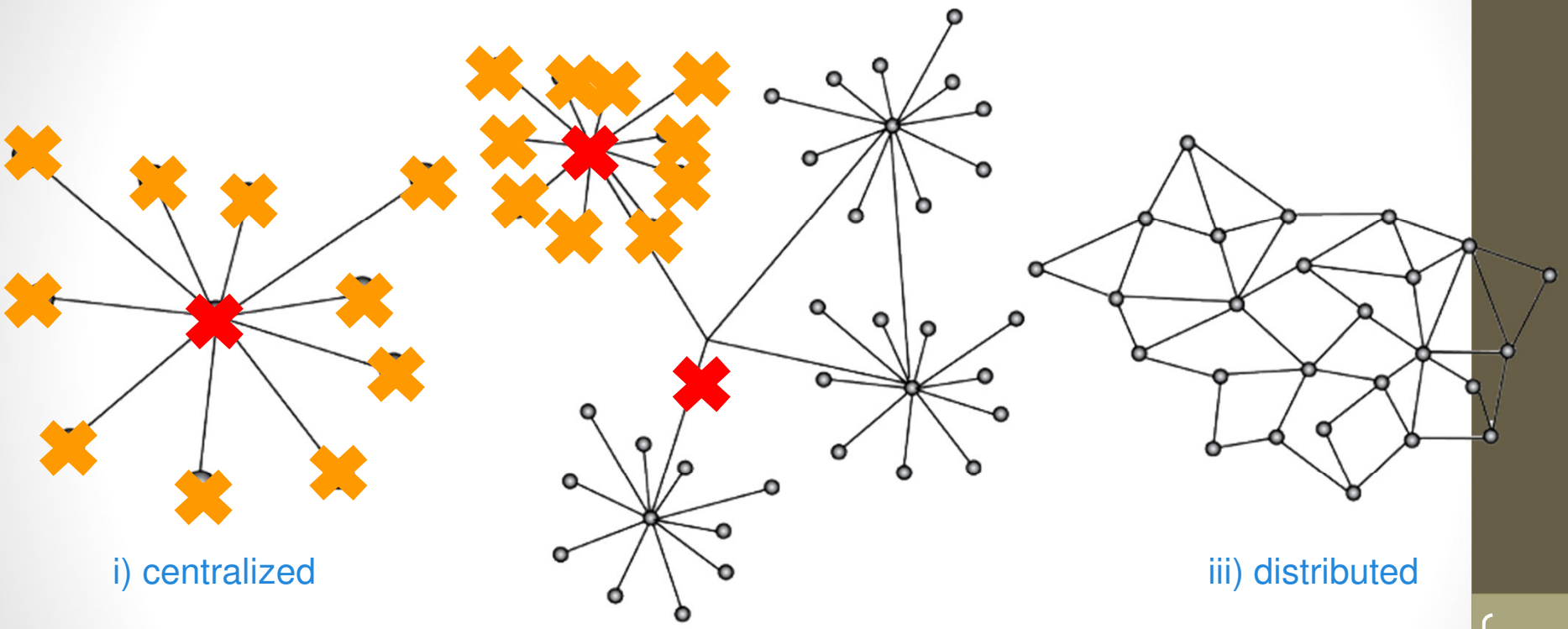


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

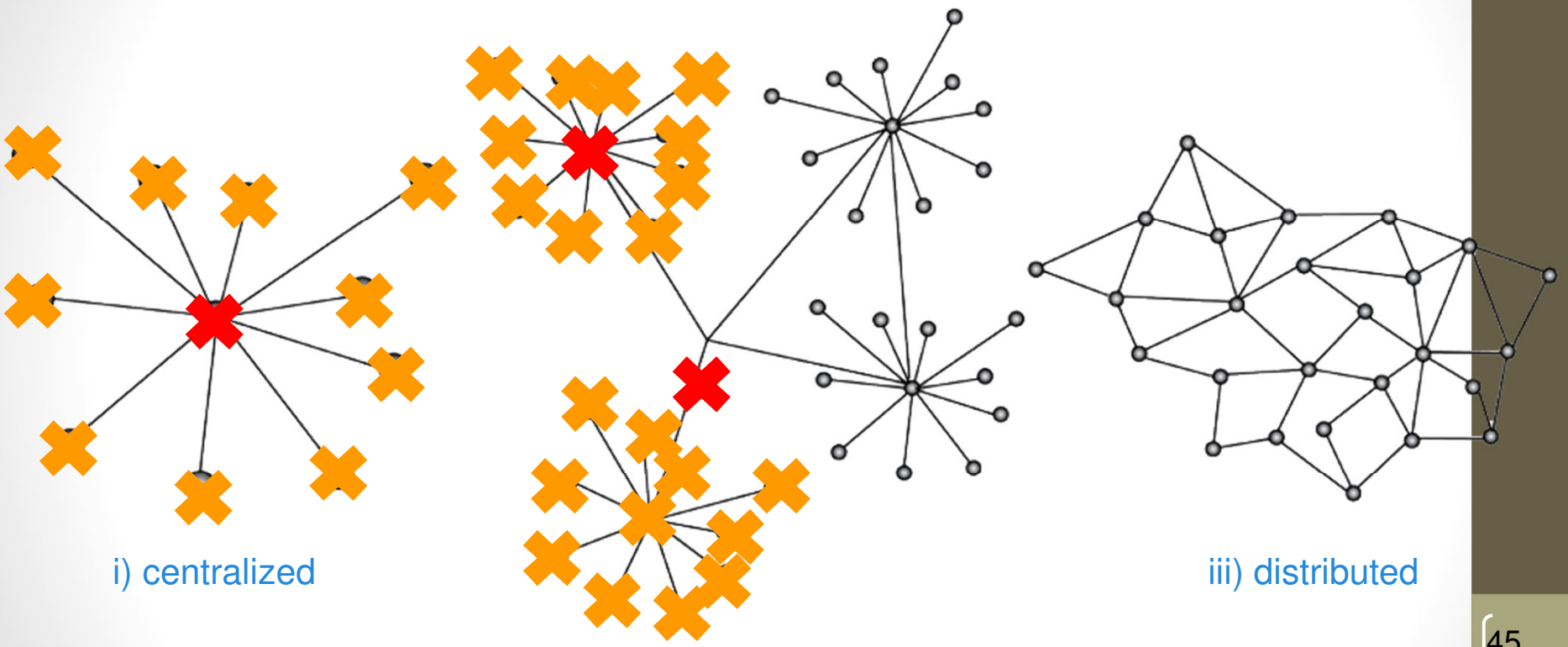


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

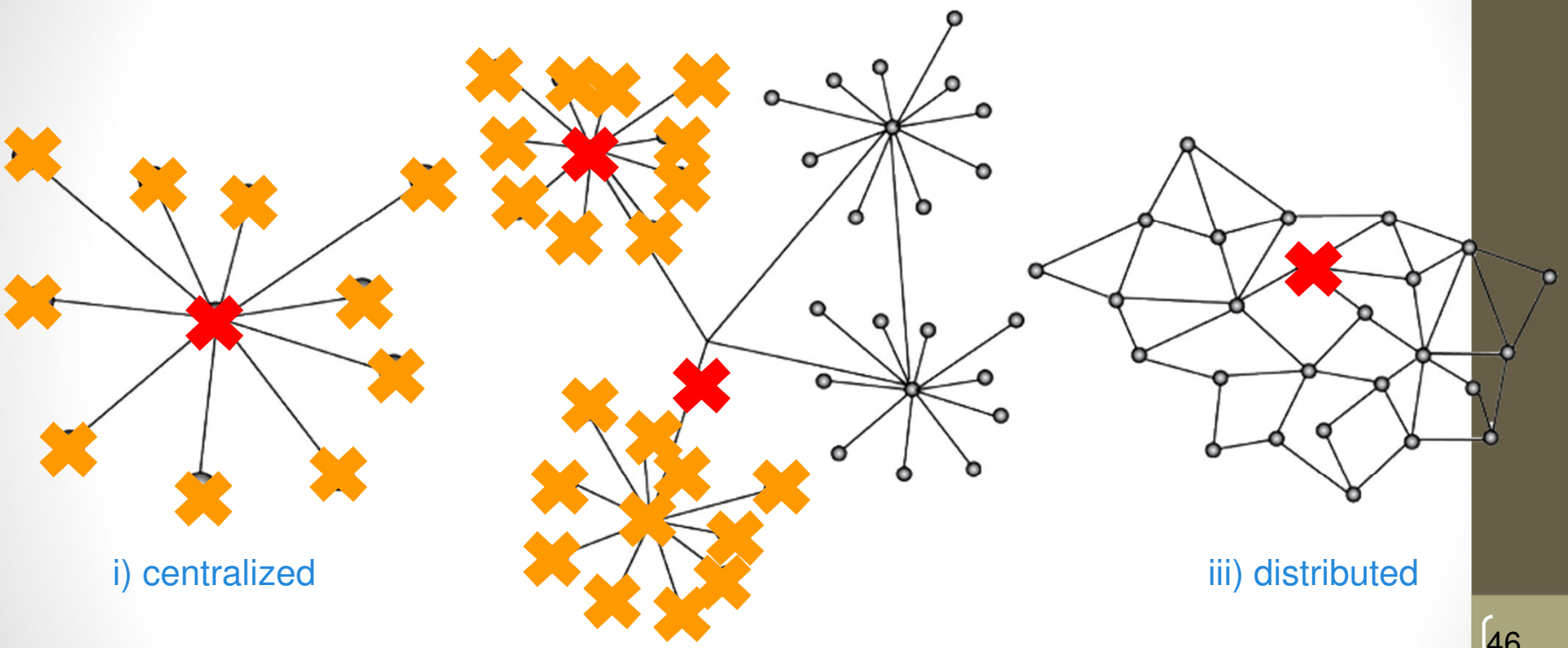


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

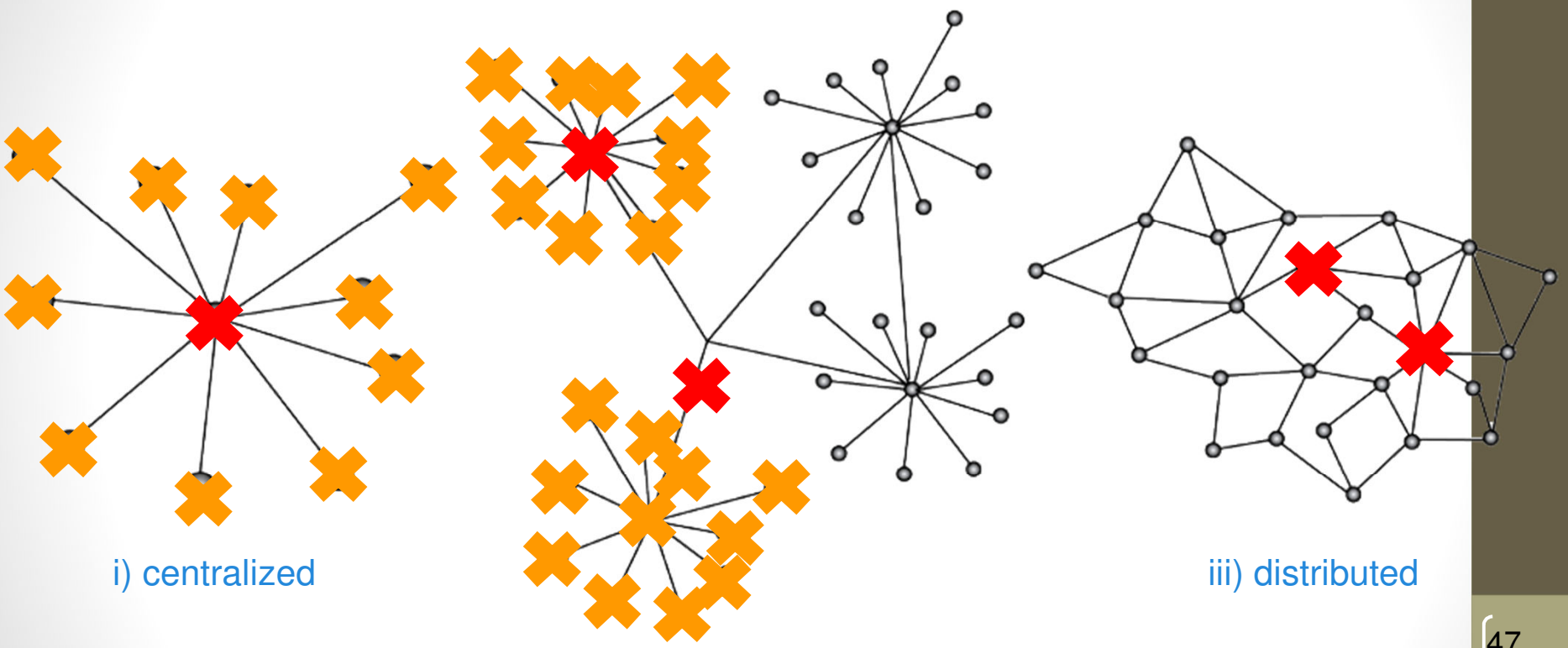


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

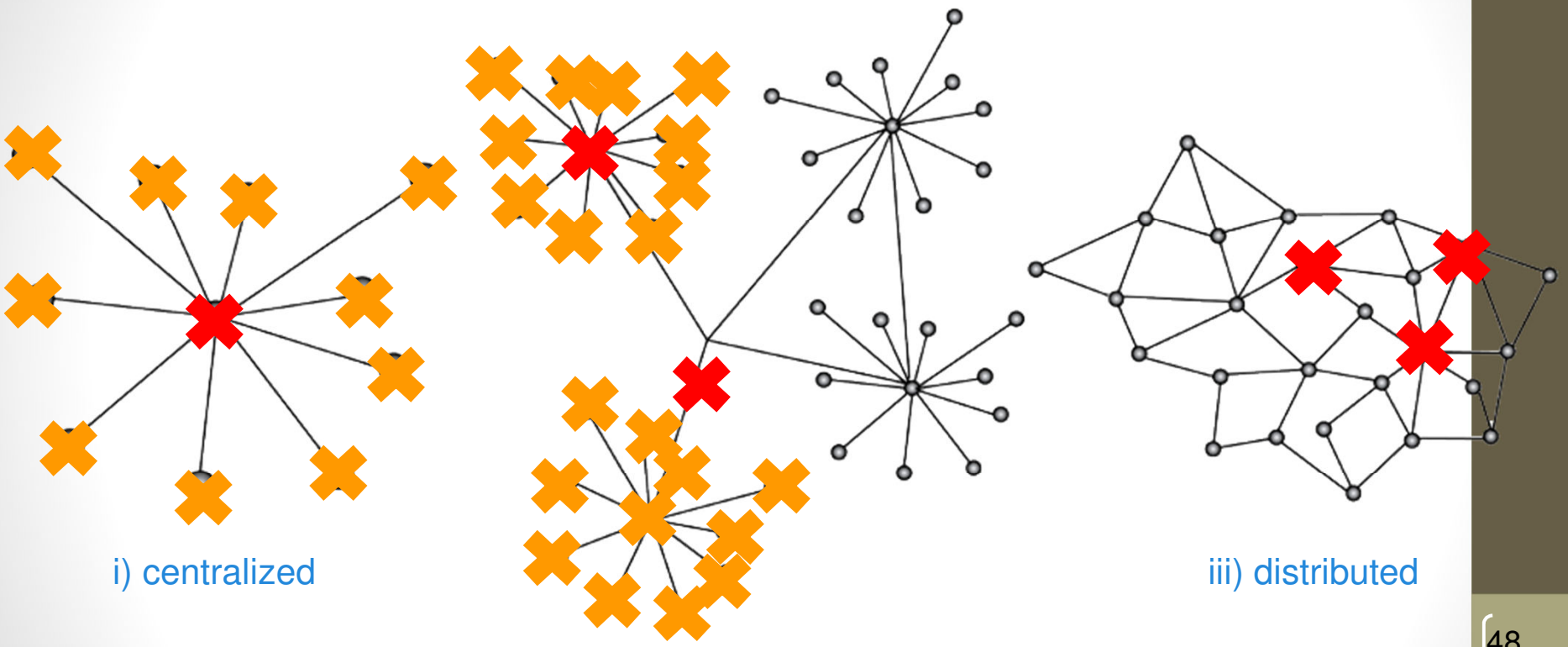


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.

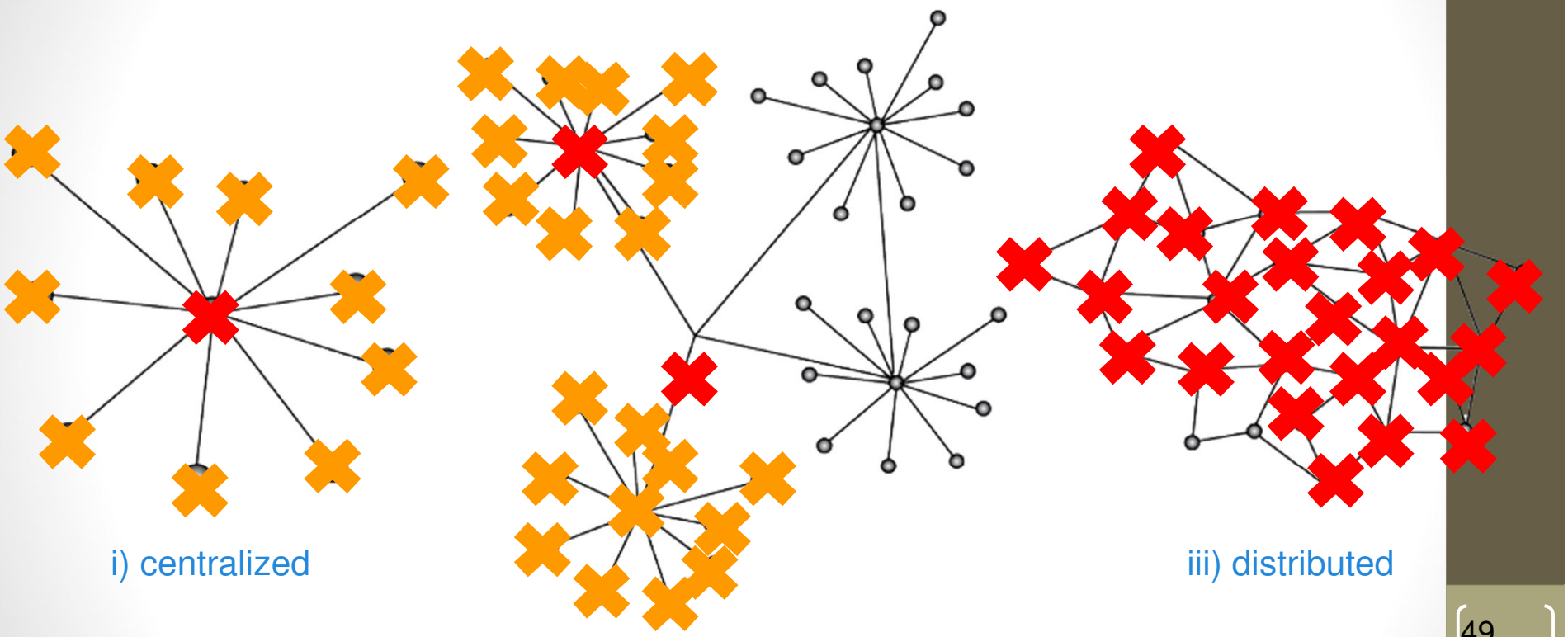


i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.



i) centralized

ii) decentralized

iii) distributed

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.


Blockchain Technology
the second coming
of
the Internet

- Blockchain Technology can be seen as a database or a giant network known as a distributed leger which captures ownership, value and also permits anyone who can access the network to view and take part.

- In a distributed network, the network is updated and verified through the agreement of everybody involved. When somethings is added, it can not be changed and if it looks valid to everyone then, the update is approved.

- Compared to the internet in the 90's, Blockchain Technology has a similar investment and a similar version of potential users.

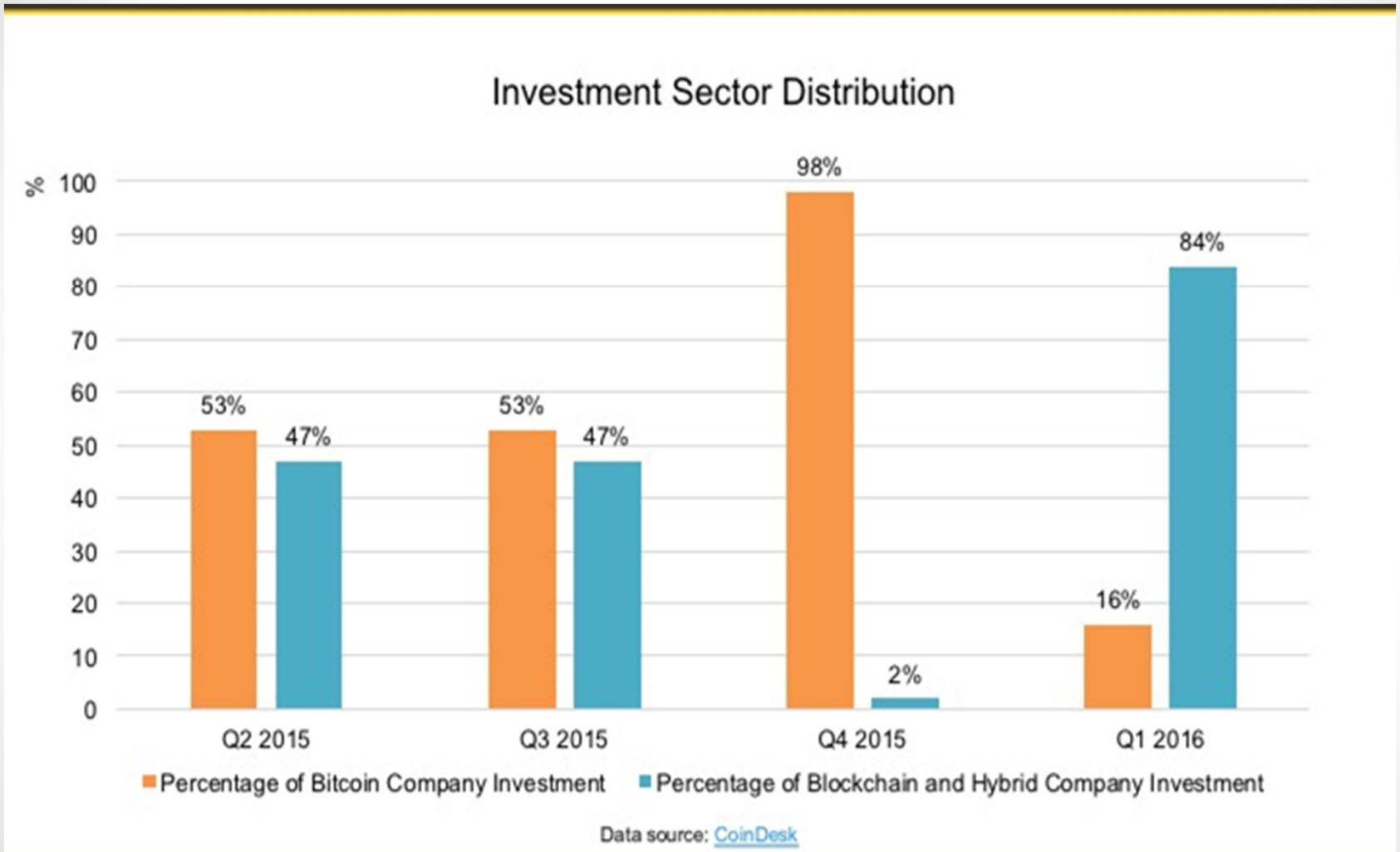
- Blockchain Technology was built for finance first but now it has been used in different aspects.

- Will be discussed further at a later stage….

Evolution
of
Blockchain Technology network

- Bitcoin, Litecoin, dogecoin are known to be the 1st generation of Blockchain Technology.
- 1st generation network just transfer value.
- Most of the Blockchain Technology improved technologies are built upon existing blockchains by

Mainelli, M. and von Gunten, C., 2014. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. Long Finance.


Investment Sector Distribution
%
100
90
80
70
60
50
40
30
20
10
0
53%
47%
53%
47%
98%
2%
16%
84%
Q2 2015
Q3 2015
Q4 2015
Q1 2016
Percentage of Bitcoin Company Investment
Percentage of Blockchain and Hybrid Company Investment
Data source: CoinDesk

Further readings

https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/

https://bitsonblocks.net/2016/05/09/confused-by-blockchains-revolution-vs-evolution/

https://bitsonblocks.net/2015/12/01/the-pros-and-cons-of-internal-blockchains/

Further readings

https://bitsonblocks.net/2015/09/28/a-gentle-introduction-to-digital-tokens/

https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/

https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/