Blockchain 101

Swee-Won LO (Ph.D.)
Lecturer, School of Business

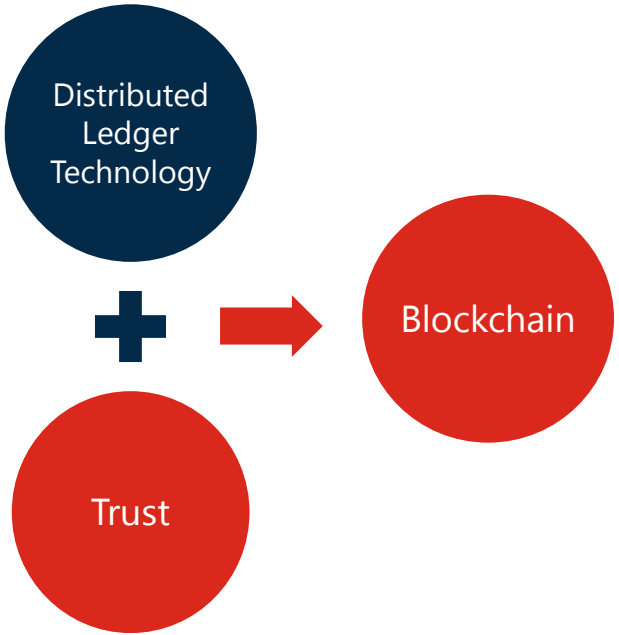
SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Agenda

- Blockchain & Distributed Ledger Technology (DLT)
- Cryptoeconomy
- Fun fact: “Tragedy of the Commons”
- Cryptoeconomy – a more technical introduction
- Blockchain Evolution
- Blockchain 3.0

Blockchain & Distributed Ledger Technology (DLT)

- Blockchain = Distributed Ledger Technology?
- DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers)[1].
- DLT is easy to implement if its users are trustworthy.



1. World Bank Group's FinTech note on Distributed Ledger Technology (DLT) and Blockchain (link)

Blockchain's Provision of "Trust"

- Crypto – "cryptography", a suite of algorithms that provides security guarantee based on computational difficulty – preventing/thwarting dishonest actors.

- Economy – "incentives", rewards given to honest actors who contribute and/or help to maintain the integrity of the blockchain.

1. Vitalik Buterin's Introduction to Cryptoeconomics (link)

The Tragedy of the Commons[1]

by Garrett Hardin in *Science Magazine* (1968)

Abstract

The population problem has no technical solution; it requires a fundamental extension in morality.

- Individuals driven by self-interest act independently, deplete or spoil common resource through their collective action.

- Solution:
  - Governmental: Policy, control, "central administration" has no self-interest.
  - Non-Governmental: Definable resources, dependence on the resources, community is small.

1. Garrett Hardin's paper on ScienceMag (link)

But are we all bad?

- Using land bank as an example:

  Suppose the land banks are giving out lands for free. Do we take only what is enough?

  Some will take more than necessary.

  Land as a "common pool resource" in this case – is depleted.

Analysis of economic governance

Elinor Ostrom (August 7, 1933 – June 12, 2012), First Female Nobel Prize Winner in Economic Sciences (2009)[1]

Prize-winning work: Analysis of economic governance, especially the commons

- 8 design principles that are very similar to what blockchain is.
- Self-organisation: Collective wisdom, transparent, mutual monitory, conflict resolution.

1. https://content.ubs.com/microsites/together/en/nobel-perspectives/laureates/elinor-ostrom.html

Analysis of economic governance

Elinor Ostrom (August 7, 1933 – June 12, 2012), First Female Nobel Prize Winner in Economic Sciences (2009)[1]

Prize-winning work: Analysis of economic governance, especially the commons

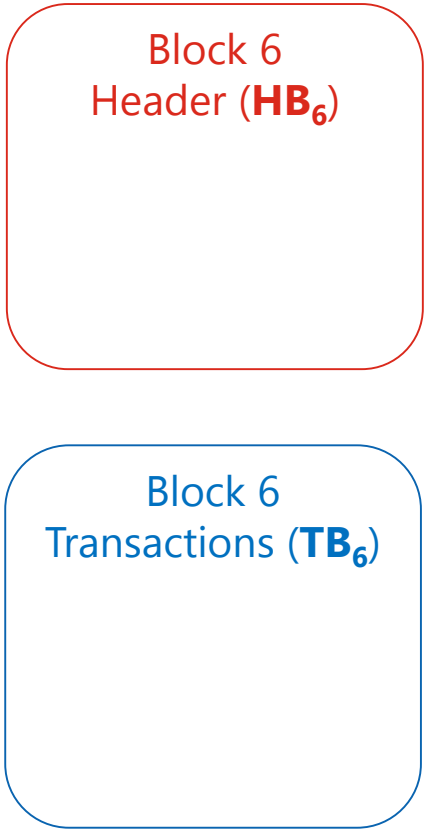
- Ostrom's work "challenged conventional wisdom, showing that common resources can be successfully managed without government regulation or privatisation".

1. https://content.ubs.com/microsites/together/en/nobel-perspectives/laureates/elinor-ostrom.html

Blockchain & Cryptoeconomy

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Blockchain's Provision of "Trust" – the [Crypto] part



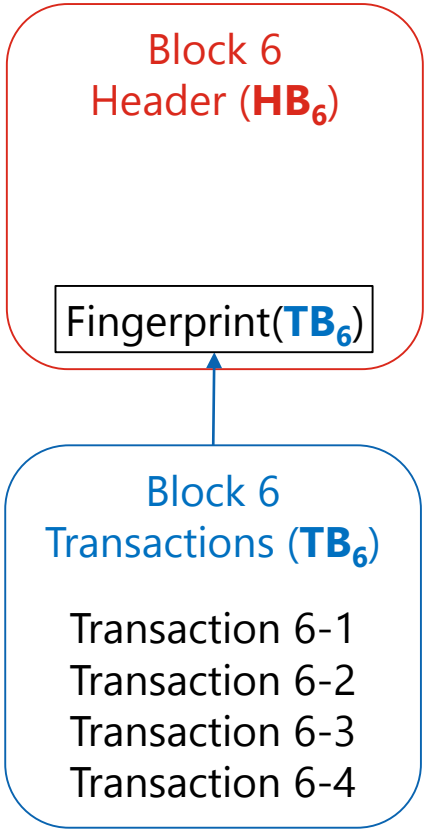
Blockchain's Provision of "Trust" – the [Crypto] part

Block 6
Header ($\mathbf{HB_6}$)

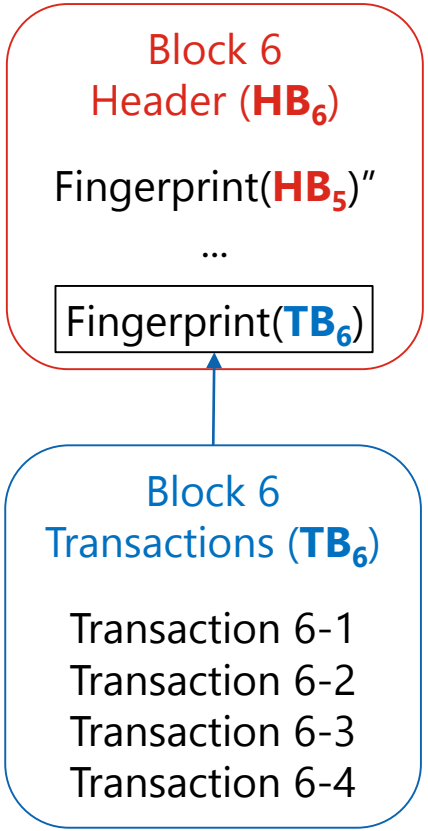
Block 6
Transactions ($\mathbf{TB_6}$)

Transaction 6-1
Transaction 6-2
Transaction 6-3
Transaction 6-4

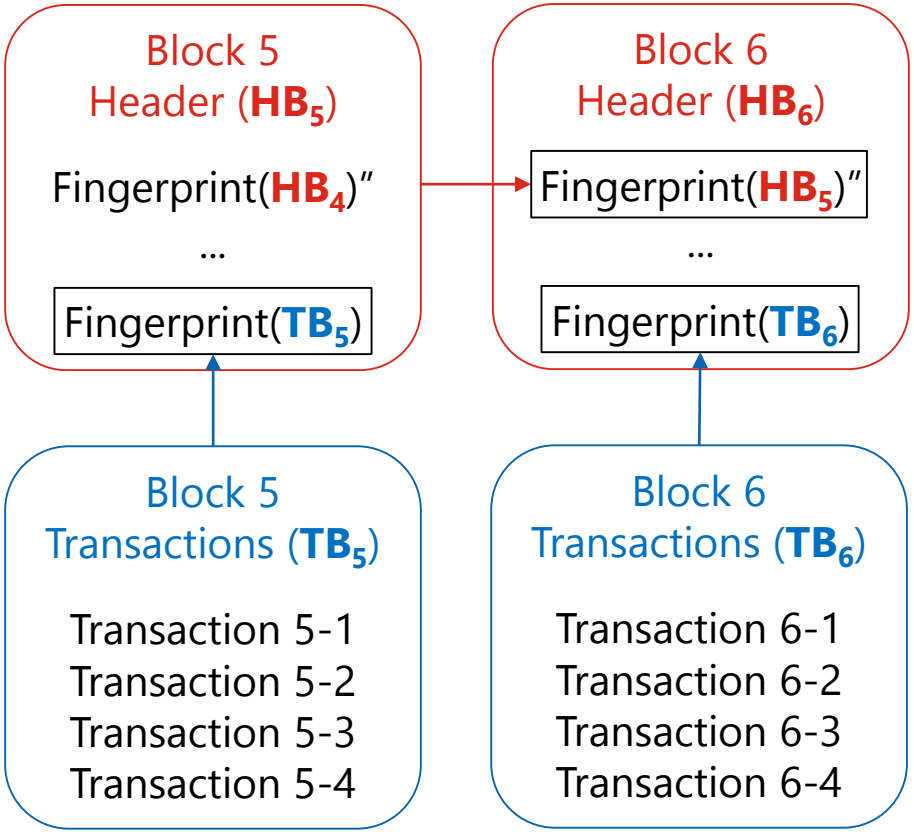
Blockchain's Provision of "Trust" – the [Crypto] part



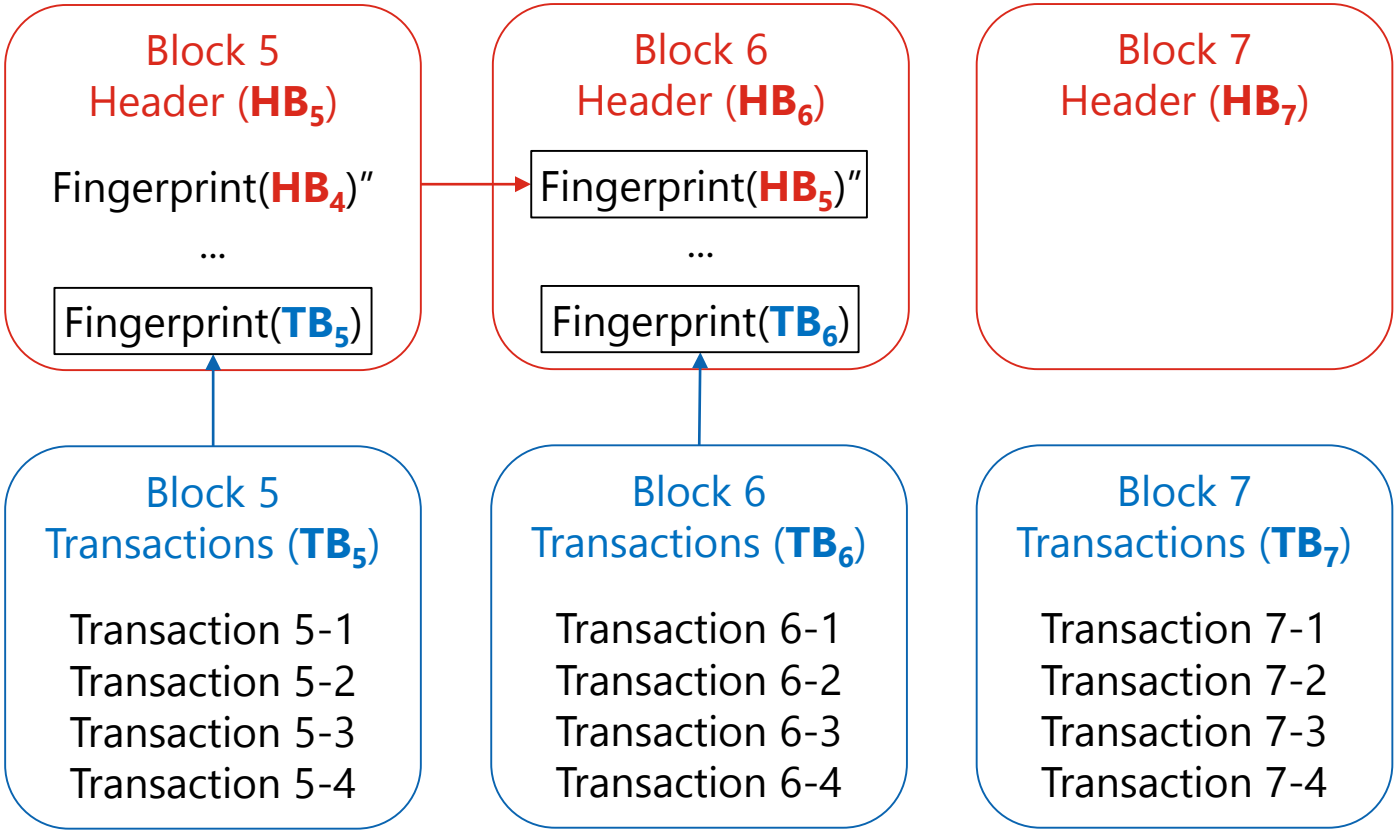
Blockchain's Provision of "Trust" – the [Crypto] part



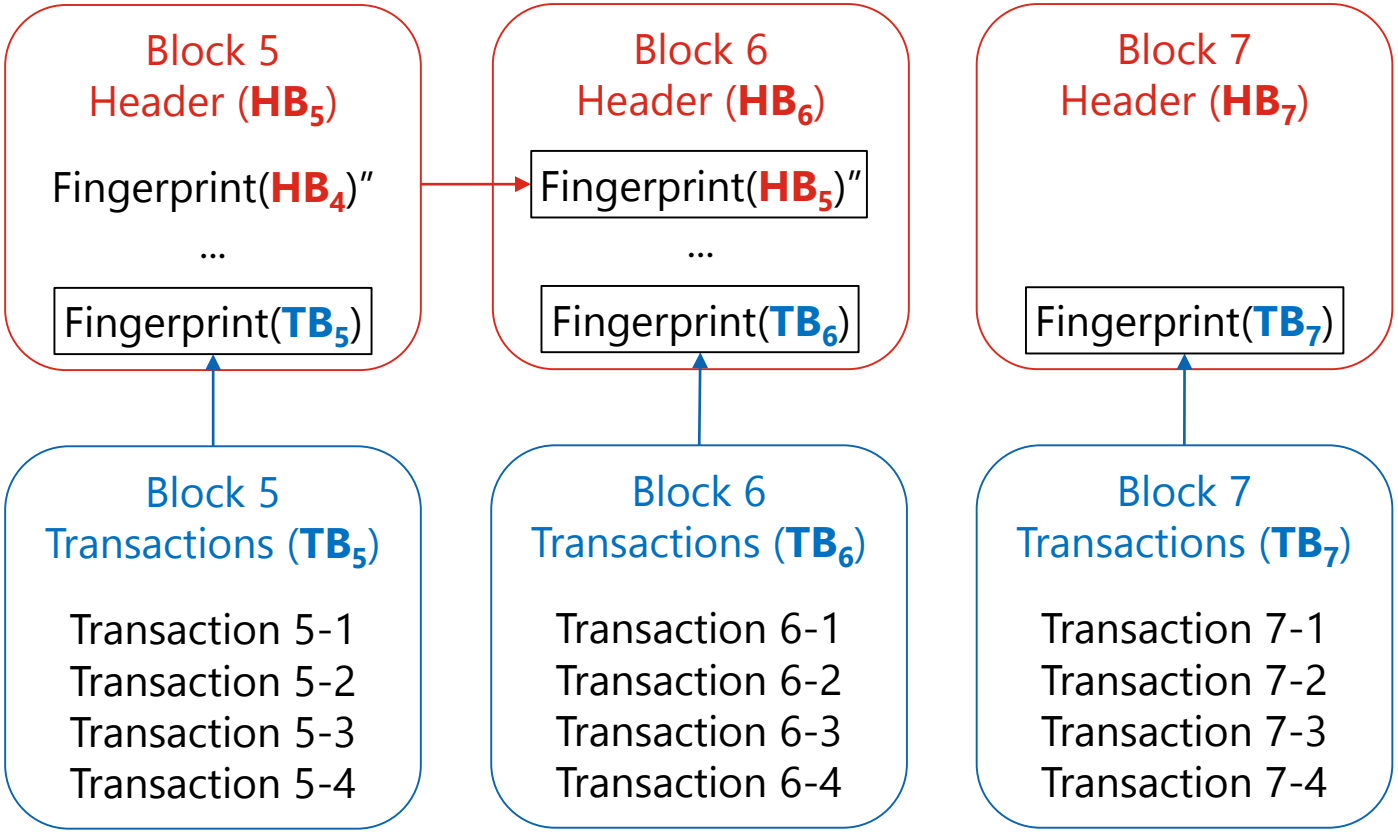
Blockchain's Provision of "Trust" – the [Crypto] part



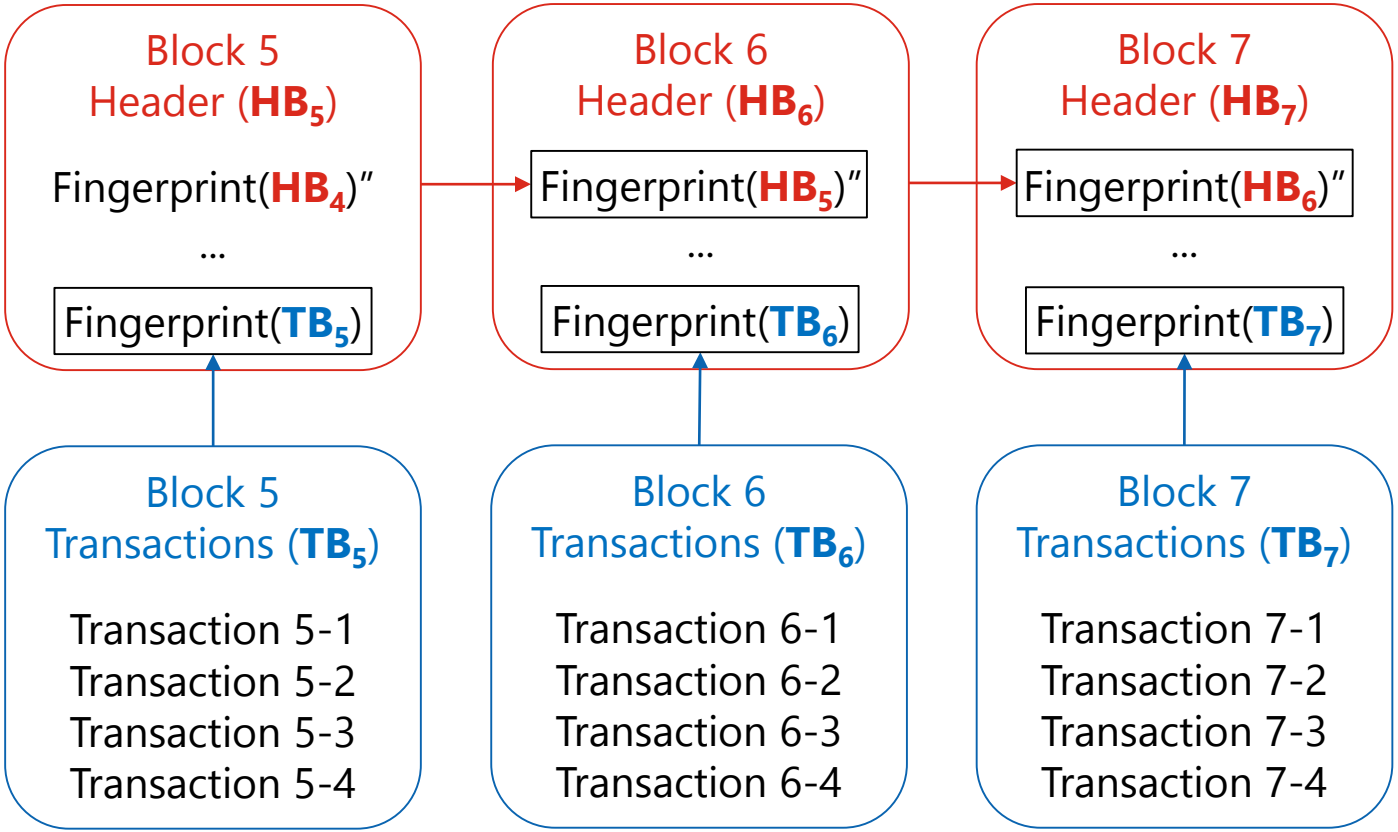
Blockchain's Provision of "Trust" – the [Crypto] part



Blockchain's Provision of "Trust" – the [Crypto] part



Blockchain's Provision of "Trust" – the [Crypto] part



Fingerprint() is a cryptographic hash function

Blockchain's Provision of "Trust" – the [Crypto] part

Fingerprint is a cryptographic hash value

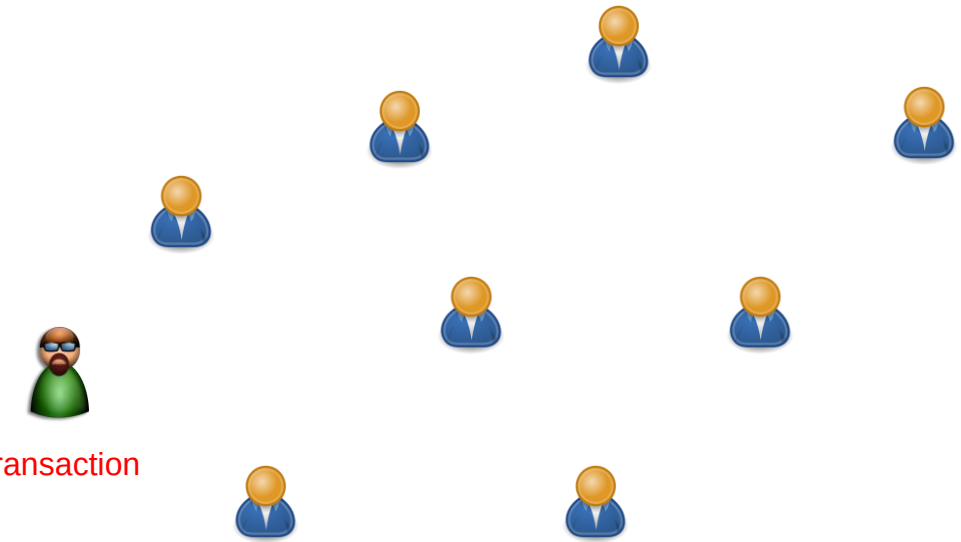
Analogy to a human fingerprint:

- Different person, different fingerprint
- Collision-resistant

To modify Transaction 6.2

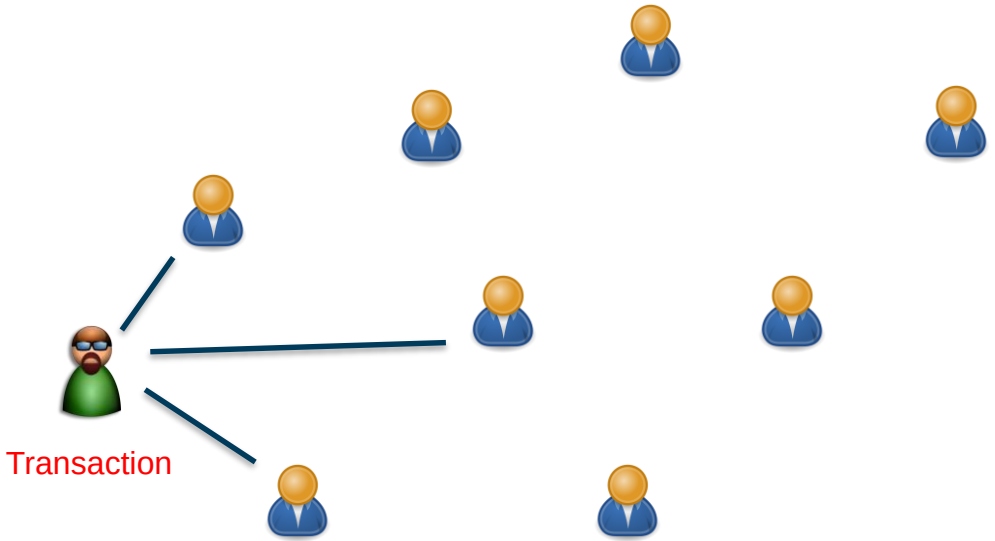
- Find a "collision" for Fingerprint(TB_6), or
- Find a partial "collision" for Fingerprint(HB_6)"

Blockchain's Provision of "Trust" – the [Economy] part



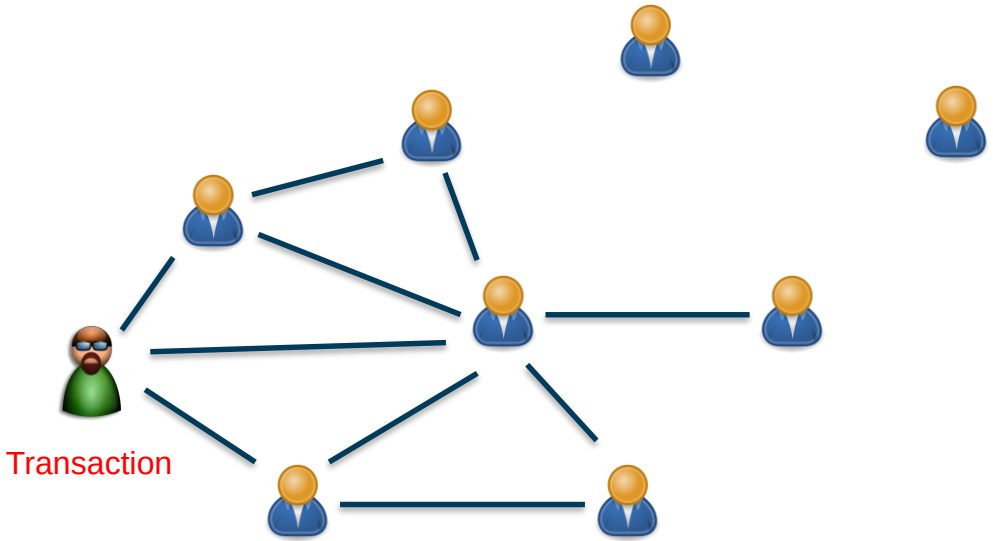
- Bob has a Bitcoin transaction that he wishes to perform on the Bitcoin blockchain.
- Bob broadcasts his transaction to the network.

Blockchain's Provision of "Trust" – the [Economy] part



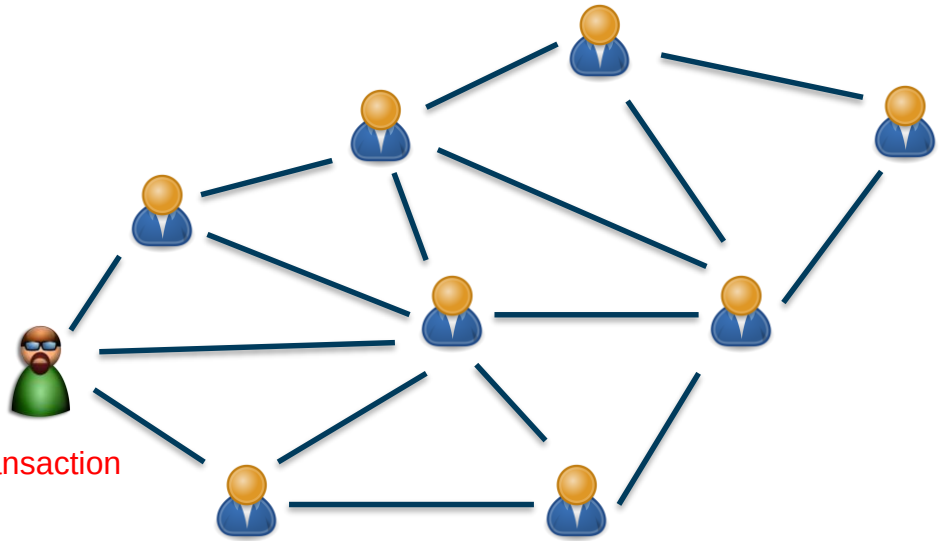
- Peer-to-Peer network

Blockchain's Provision of "Trust" – the [Economy] part



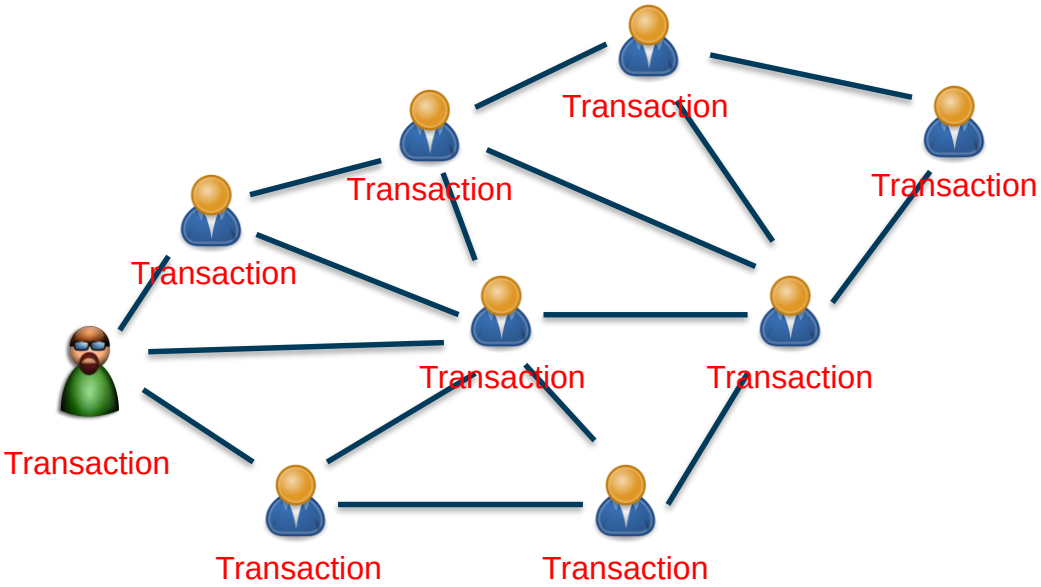
- Peer-to-Peer network

Blockchain's Provision of "Trust" – the [Economy] part



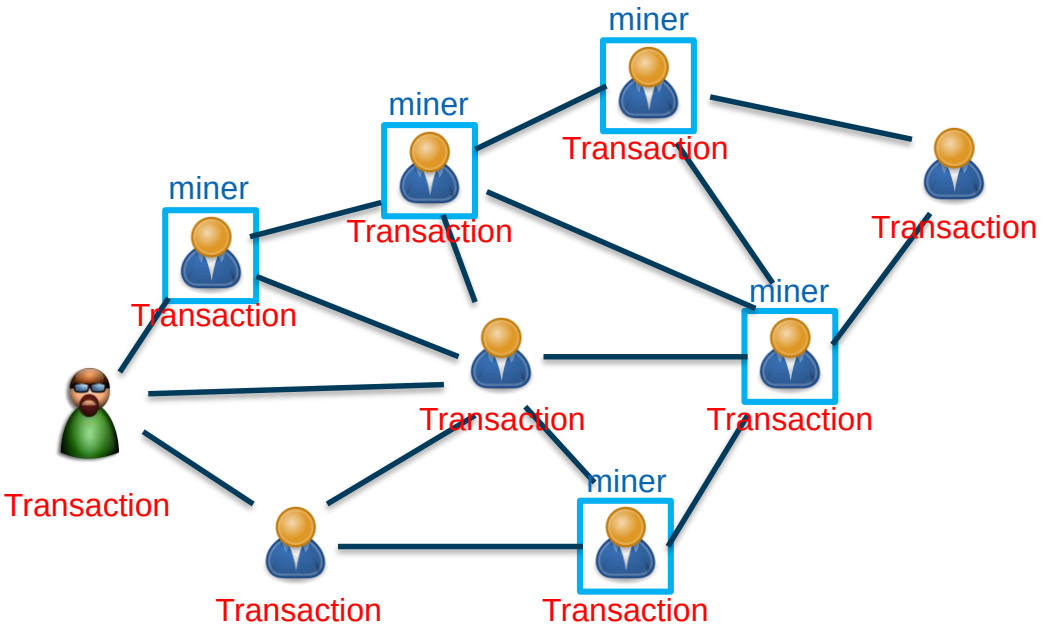
- Peer-to-Peer network

Blockchain's Provision of "Trust" – the [Economy] part



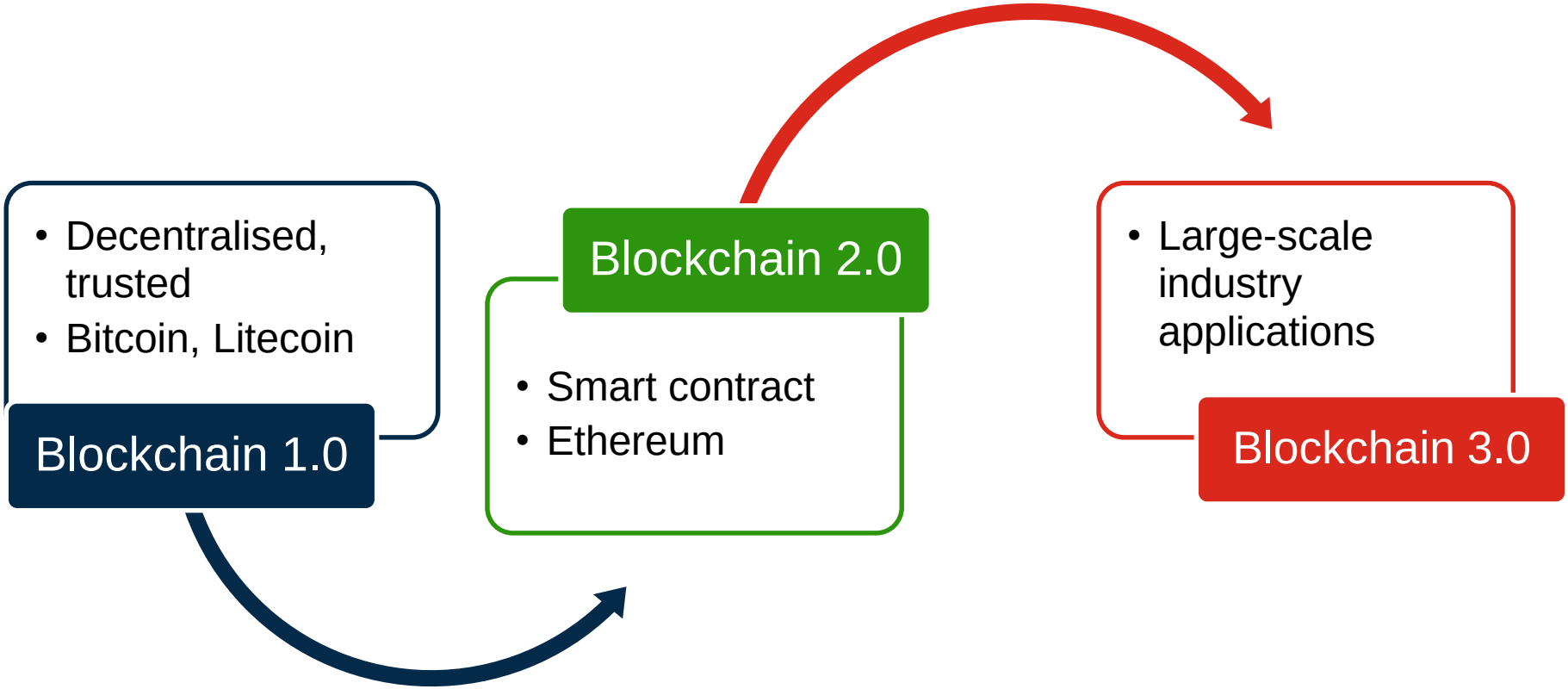
- Peer-to-Peer network

Blockchain's Provision of "Trust" – the [Economy] part



- Peer-to-Peer network
- Miners will <u>validate</u> the transaction and add the transaction to a new block in the blockchain.
- A transaction is confirmed only when a miner found a valid "partial fingerprint" for the new block header.
- The effort of the miner will be rewarded with incentive.
  - Why would a miner validate a bad transaction?

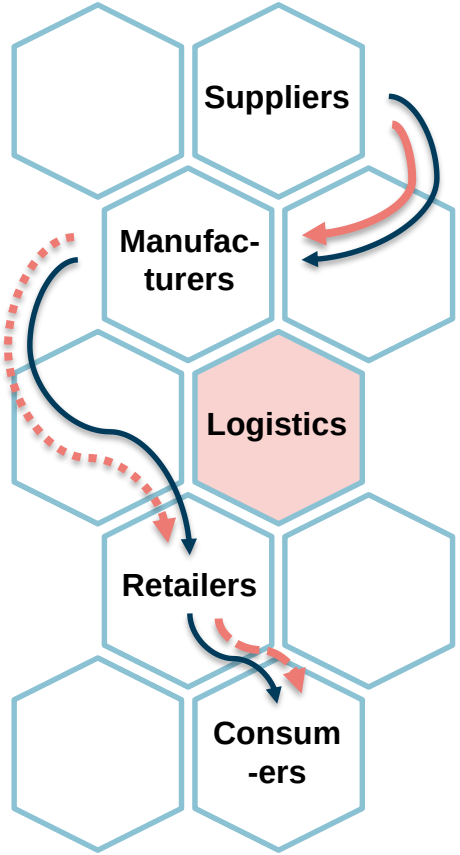
Blockchain Evolution



Blockchain 3.0

Supply chain as an example

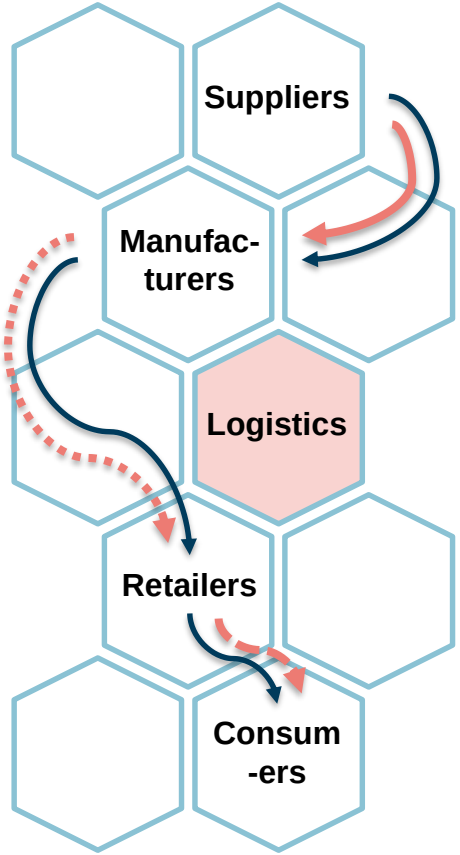
- Traditionally: Each party has its own record of the goods
- Dispute resolution is complicated and time-consuming
- Counterfeiting of goods is difficult to detect



Blockchain 3.0

Bringing blockchain to supply chain

- Single version of (trusted) truth [Crypto]
- No party has incentive to cheat [Economy]
- Revolutionalises the retail industry
  - Authenticity of goods can be verified
  - Consumer – Retailer interaction changes
  - Consumer's purchase behaviour changes
- Potential problem: Scalability, storage, privacy, etc.



Inclusiveness

The practice or policy of including people who might otherwise be excluded or marginalised, such as those who have physical or mental disabilities and members of minority groups.

https://en.oxforddictionaries.com/definition/inclusiveness

SUSS
SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Blockchain 3.0

Inclusiveness – some examples

- Sentinel chain[1] – to provide affordable and secure financial services to the unbanked, accepting livestock as collateral.
  - Cited as a practical use case in World Economic Forum's latest report on "Global Financial & Monetary System in 2030"[3].
- AID:Tech[2] – bringing social and financial inclusion to the world's underserved populations.

1. https://sentinel-chain.org/
2. https://aid.technology/
3. http://www3.weforum.org/docs/WEF_Global_Future_Council_Financial_Monetary_Systems_report_2018.pdf

Takeaways (1/2)

- Blockchain is a distributed ledger technology with built-in trust, thereby enabling it to be decentralised.
- Trust is provided by means of the “cryptoeconomy” concept – a combination of using cryptography to thwart dishonest actors and incentives to reward honest actors.
- Bitcoin, Litecoin, etc. are prominent blockchains focusing on financial transactions; works are ongoing to enable micropayment.
- Bitcoin, Litecoin and the likes are what we call Blockchain 1.0

Takeaways (2/2)

- Blockchain 2.0 is a blockchain system with smart contract functionality that can perform functions using information outside of the blockchain, e.g., Ethereum.
- Blockchain 3.0 is the vision of using blockchain to build a decentralised, secure, and “efficient” ecosystem in different industry – but many challenges remain.
- Scalability, storage, data privacy, consensus, etc.
- Blockchain as a trust machine should be leveraged to provide inclusivity to better serve the society.

Thank you!

swlo@suss.edu.sg

www.sussblockchain.com

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES