BLOCKCHAIN

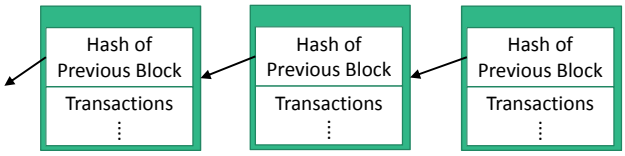
www.data61.csiro.au

Blockchain is an emerging technology that allows participants in an industry ecosystem to transact with each other without relying on a central trusted authority to record transactions. Blockchain ensures the integrity of a distributed ledger which is replicated across the ecosystem. Bitcoin uses a blockchain for financial transactions, but next-generation systems also allow programs ("smart contracts") to run as transactions.

Blockchains

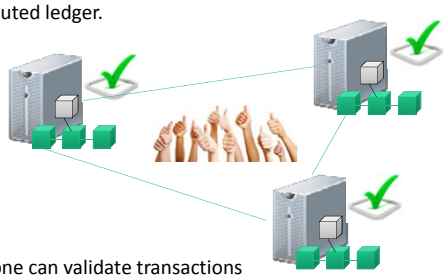
A Cryptographic Chain of Groups of Transactions

The blockchain data structure is a time-stamped list of blocks, chained together cryptographically.



An Immutable Distributed Ledger

Blockchains record all transactions that have occurred, and provide tamper-proof immutable data storage called a "distributed ledger". The whole network of participating organisations reach consensus on transactions included into the distributed ledger.

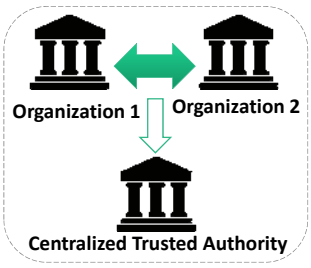


Blockchains can be:

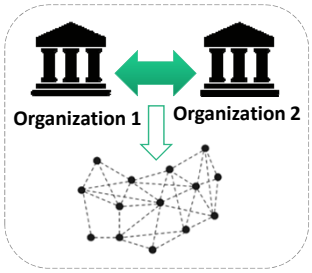
- **Permissionless**: Anyone can validate transactions
- **Permissioned**: Only pre-approved participants can validate transactions

Either way, consensus and trust in the integrity of the ledger is distributed over participants.

Distributed Trust



Traditional trust environment



Distributed trust environment

Projects with Australian Treasury

- **Distributed Ledger Technology: Scenarios for the Australian Economy Over the Coming Decades**
- **Risks and Opportunities for Systems Using Blockchain and Smart Contracts**

Findings

- Supply chains are a highly promising domain for the application of blockchain technology
- Supply chain on Blockchain may enable significant opportunities for trade finance and insurance
- Public blockchains may be appropriate for some purposes
- Blockchains and smart contracts make it possible to create 'programmable money'
- Blockchain may help reduce cost and time of remittances, but challenges remain for solutions to KYC (Know-Your-Customer)
- There are open questions about blockchain governance
- A blockchain is usually only one component of a broader IT system
- Sometimes too much integrity causes problems
- Blockchains have a different cost model
- Private blockchains are often not private enough

Uses in Industry and Society

Financial services

- Digital currency
- (International) payments
- Reconciliation for correspondent banking
- Securities registration, clearing and settlement
- Markets
- Trade finance

Government services

- Registries and identity
- Grants and social security
- Quota management
- Taxation

Enterprise and industry

- Supply chain
- Internet of Things (IoT) storage, compute and management
- Metered access to resources and services
- Digital rights and IP management
- Data management
- Attestation and proof of existence
- Inter-divisional accounting
- Corporate affairs (board and shareholder voting)

FOR FURTHER INFORMATION

Mark Staples
e mark.staples@data61.csiro.au

Xiwei (Sherry) Xu
e xiwei.xu@data61.csiro.au

REFERENCES

[1] Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly, 2015
[2] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital CryptoCurrencies*, O'Reilly, 2014