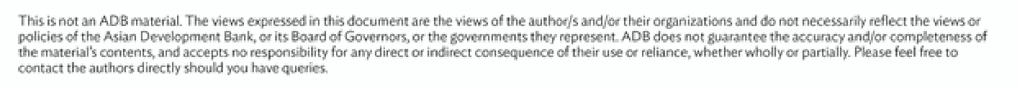
Blockchain Foundations

Nicholas Giurietto

Asian Development Bank Seminar
Manila, May 23 2018



This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

PROMOTING BLOCKCHAIN
INNOVATION IN AUSTRALIA

ADCA

About ADCA

ADCA is the industry body that represents Australian businesses participating in the digital economy through blockchain technology.

ADCA aims to encourage the responsible adoption of blockchain technology by industry and governments across Australia as a means to drive innovation in service delivery across all sectors of the economy.

ADCA

Everybody is Talking About Blockchain

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
S. Adams E-mail: SCOTTADAMS@AOL.COM
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
11/17 © 1995 United Feature Syndicate, Inc.(NYC)
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.

ADCA

Agenda

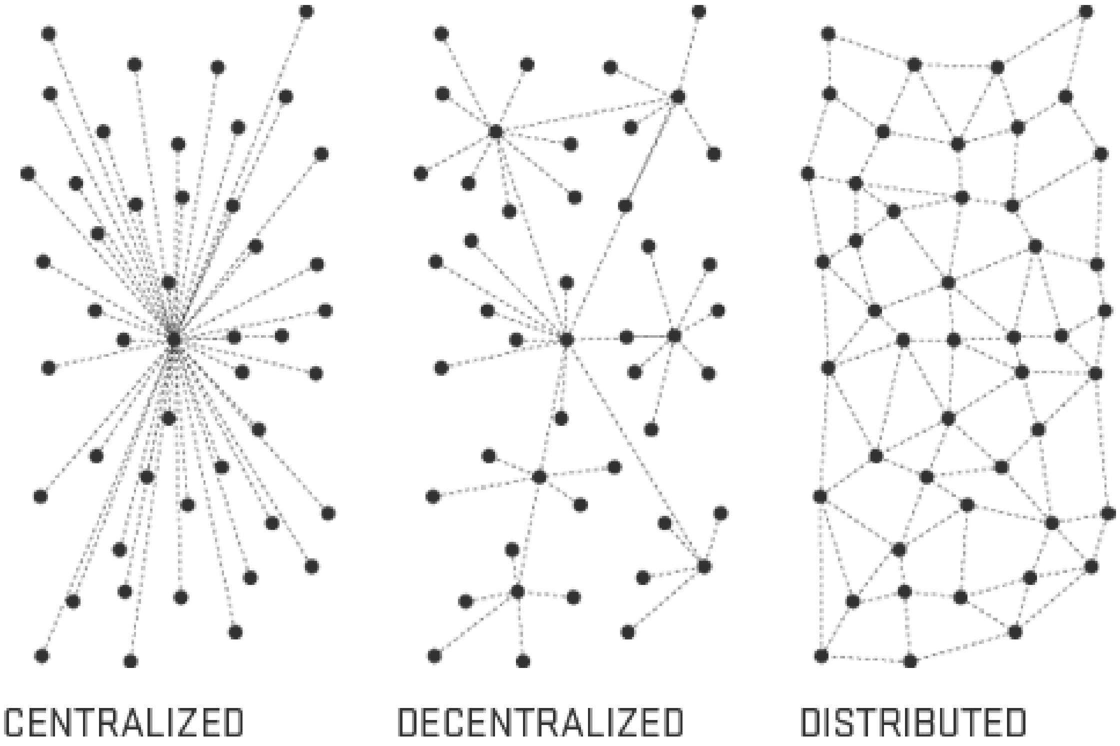
- Technical Foundations
- Smart Contracts
- Identity
- Australian Blockchain Innovators

Bitcoin & Blockchain

- *“Peer-to-peer electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution”*
- Proposed by Satoshi Nakamoto in May 2008
- Bitcoin “Genesis Block” in January 2009
- Current market value approx. USD 40 Billion

- Underlying technology for Bitcoin
- A distributed database that contains blocks of timestamped transactions linked together in a continuous chain
- Supports consensus methodology and data immutability
- Allows creation and trading of an electronic asset

Distributed Ledger Provides TRANSPARENCY



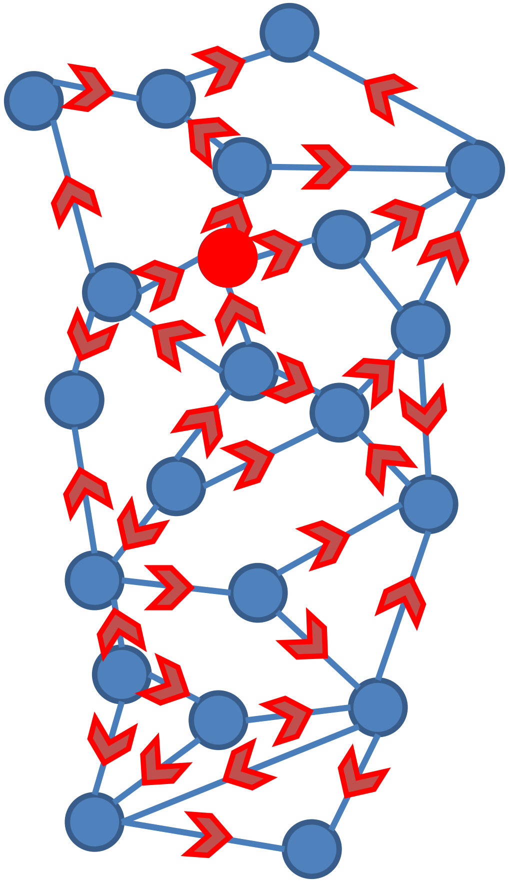
ADCA

Single Source of Truth

I see what you see

ADCA

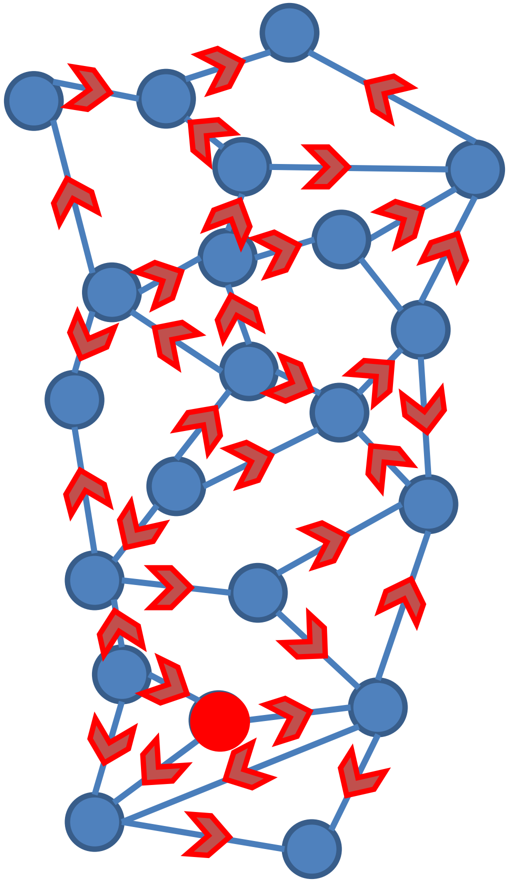
Consensus Protocol establishes ACCURACY

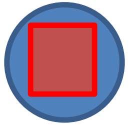


1. A new **transaction** is created on one node

2. The transaction is broadcast to all nodes

Consensus Protocol establishes ACCURACY





1. A new **transaction** is created on one node

2. The transaction is broadcast to all nodes

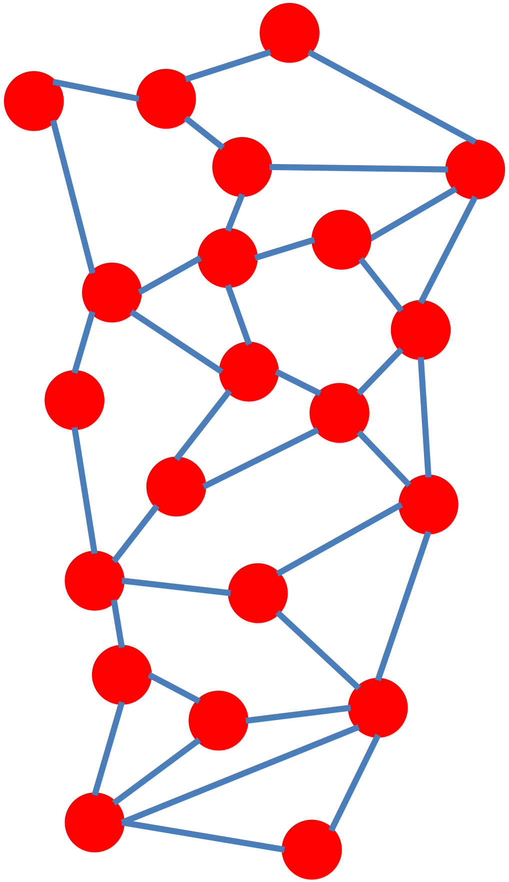
3. Each node competes to collect new transactions into a “block”

4. A **random** node ‘wins’

   - and broadcasts the new block to other nodes.

ADCA

Consensus Protocol establishes ACCURACY



1. A new **transaction** is created on one node

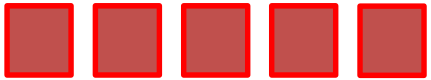
2. The transaction is broadcast to all nodes

3. Each node competes to collect new transactions into a new "block"

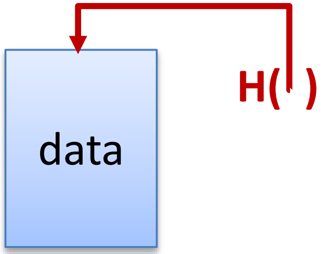
4. A **random** node 'wins'

   - and broadcasts the new block to other nodes.

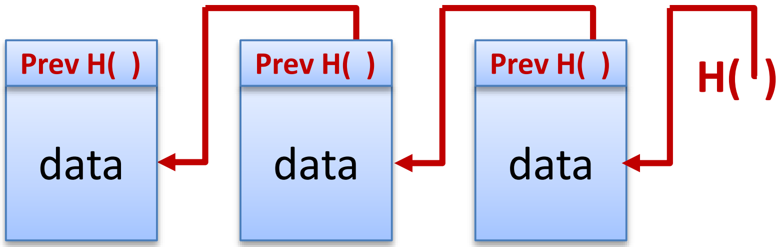
5. All other nodes add the new block to their blockchain.



Blockchain provides IMMUTABILITY



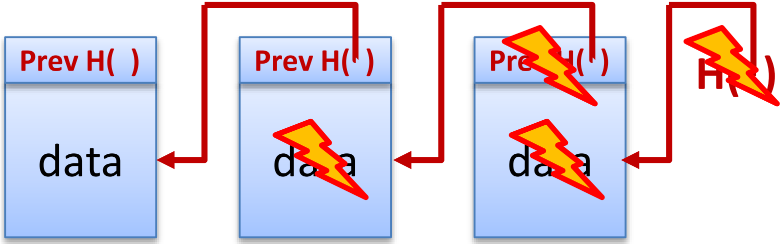
- A hash-pointer is a cryptographic reference to a piece of data
- SHA-256 is a standard compression algorithm
- The hash is **uniquely associated** with the underlying data



- In a Blockchain each new block contains the hash function of the previous block.
- To verify the whole chain – **and every transaction in it** – you only need to be able to confirm the most recent hash

ADCA

Blockchain provides IMMUTABILITY



- If the data is corrupted (accidentally or deliberately) then the next hash and all subsequent blocks fail
- This creates a **tamper-evident ledger**

The Elements of TRUST

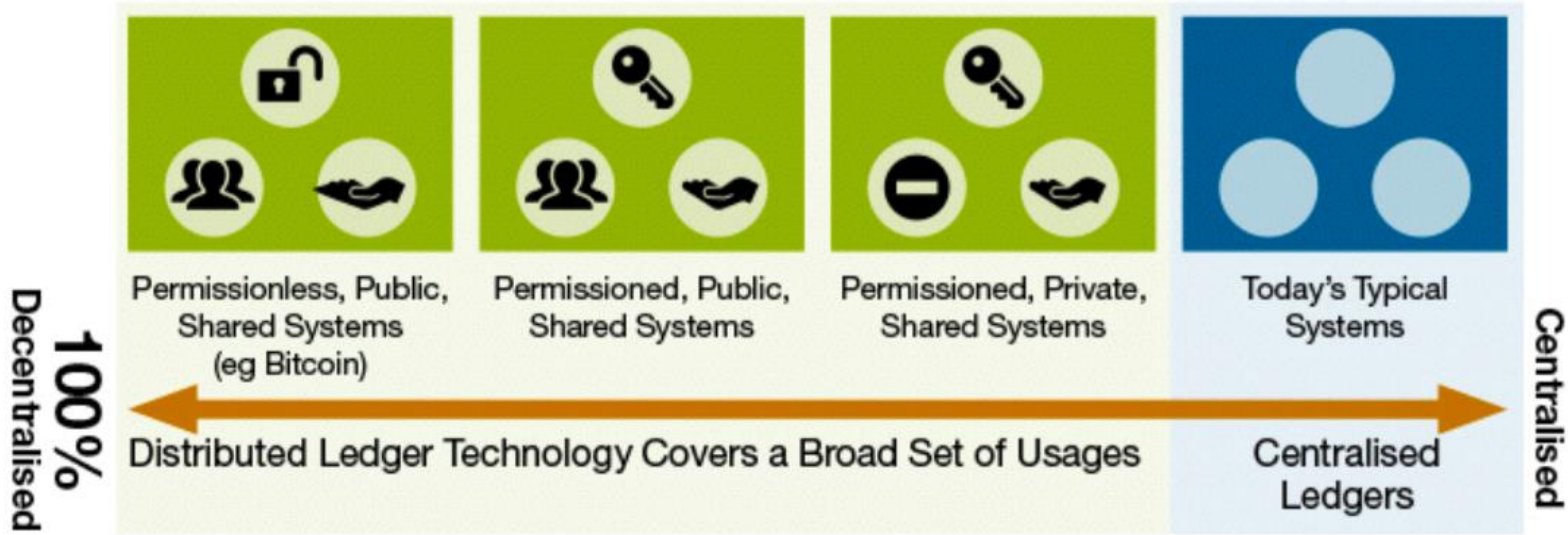
SECURITY

ACCURACY

TRANSPARENCY

IMMUTABILITY

Public, Permissioned and Private Blockchains



Permissionless, Public, Shared Systems (eg Bitcoin)
Permissioned, Public, Shared Systems
Permissioned, Private, Shared Systems
Today's Typical Systems
100% Decentralised
Centralised
Distributed Ledger Technology Covers a Broad Set of Usages
Centralised Ledgers

ADCA

Public, Permissioned and Private Blockchains

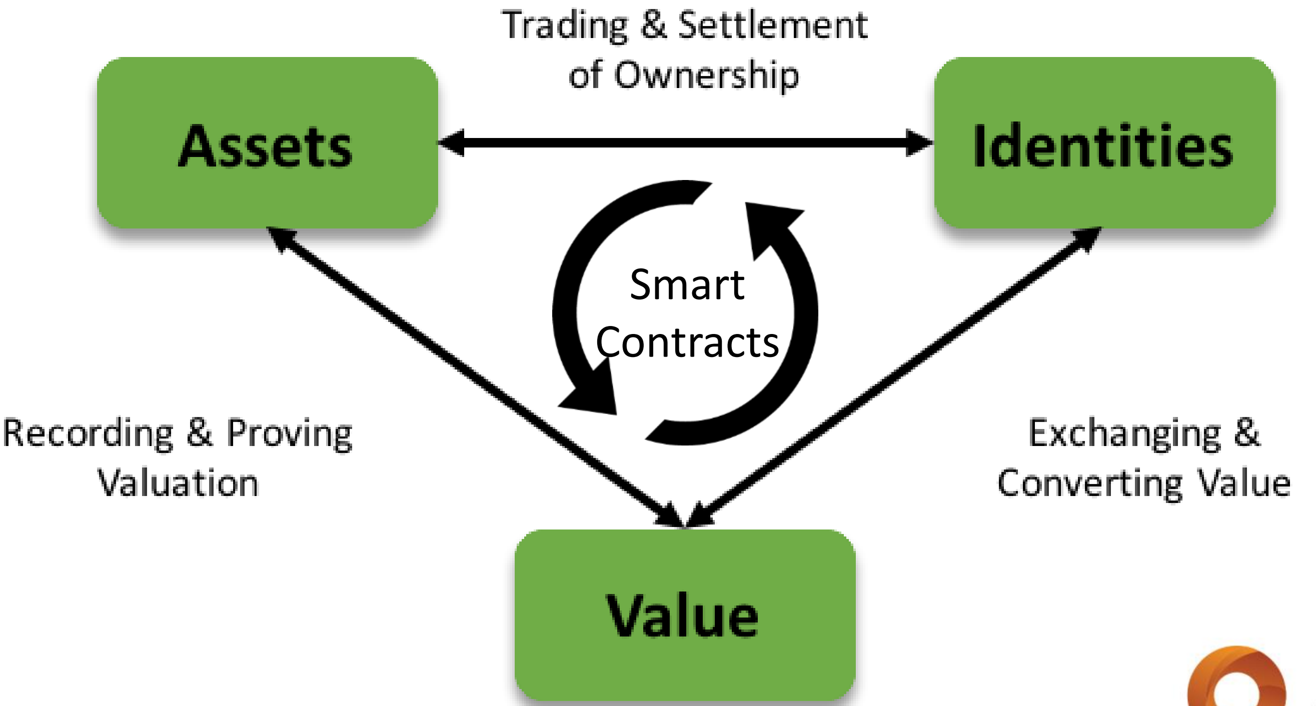
Different use cases require different solutions.

Trade offs include:

- Security
- Consensus mechanism
- Speed

Smart Contracts

Future Blockchain Ecosystem


Trading & Settlement of Ownership
Assets
Identities
Smart Contracts
Recording & Proving Valuation
Exchanging & Converting Value
Value

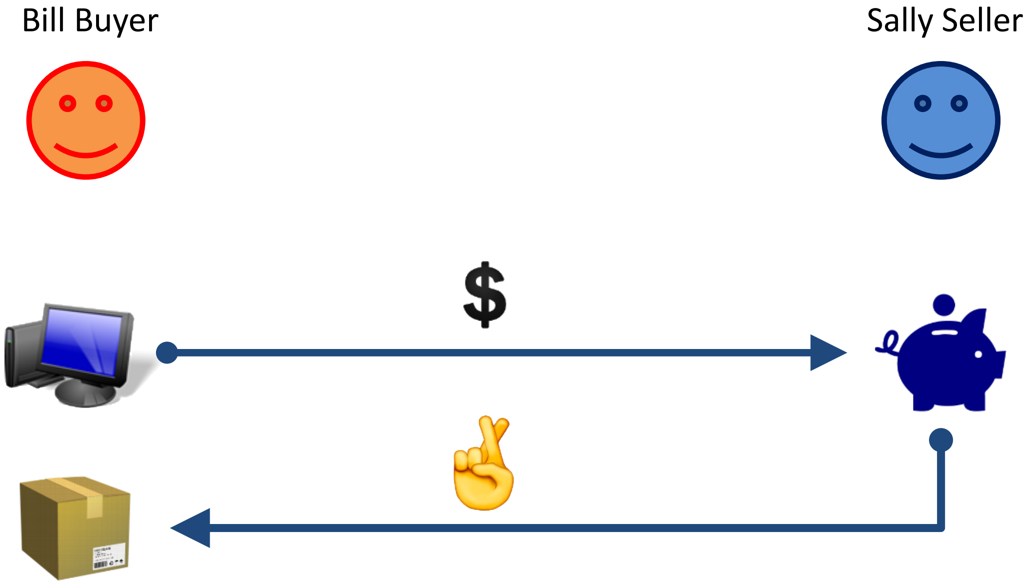
ADCA

Smart Contracts

Features of a Smart Contract:

- computer programs that emulate (key) contractual clauses
- stored on a blockchain to give all parties confidence that they will operate as intended

Online Escrow Use Case for a Smart Contract

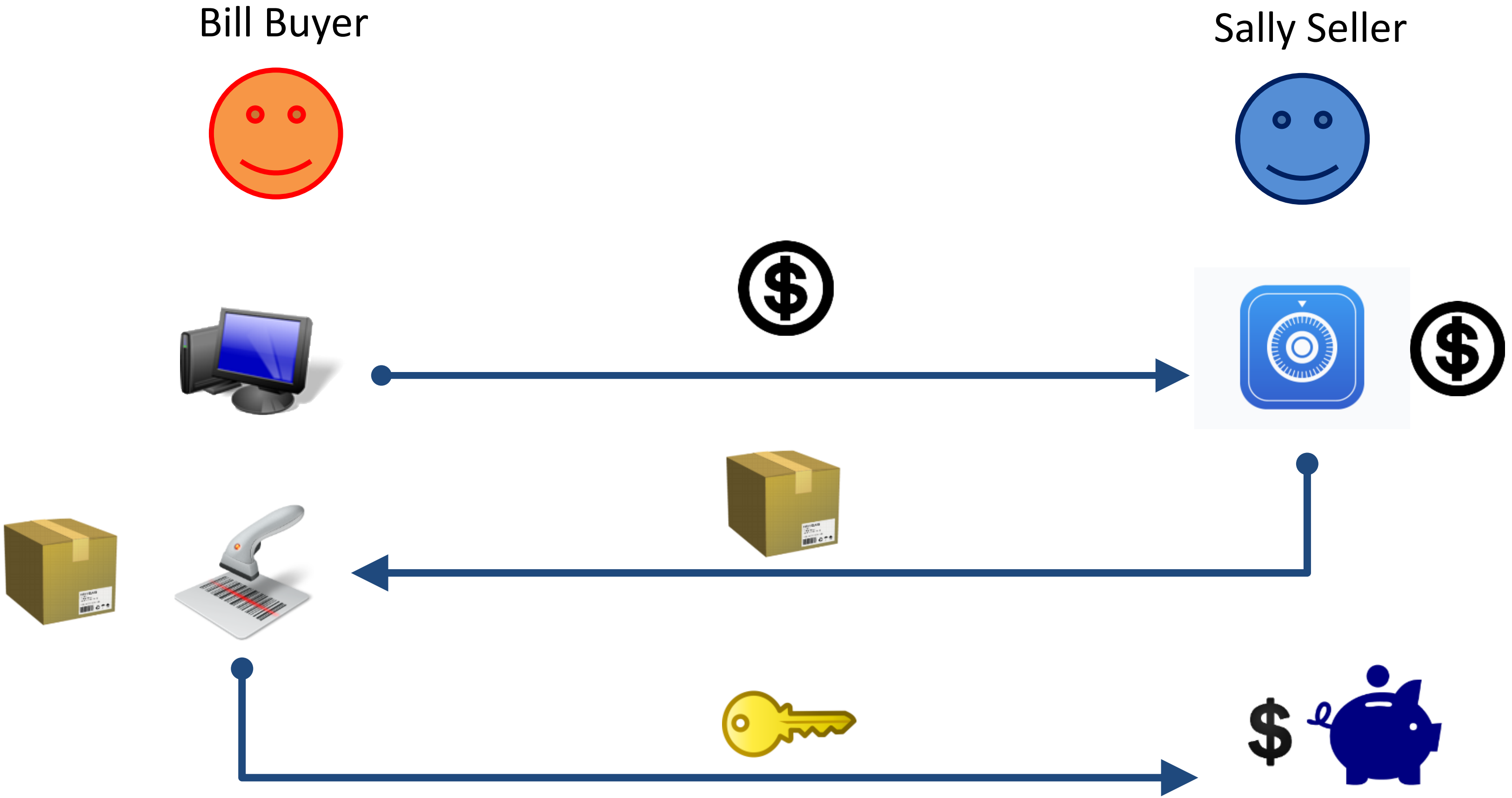


Bill Buyer

Sally Seller

ADCA

Online Escrow Use Case for a Smart Contract



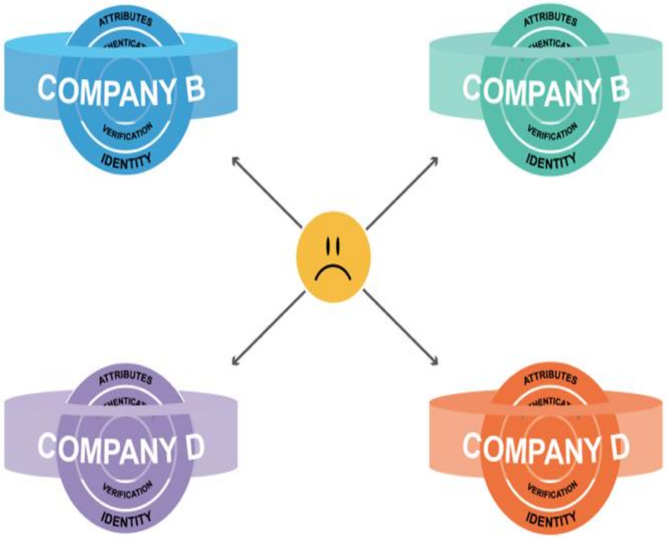
Solving Identity

ADCA

Identity is a Broken System

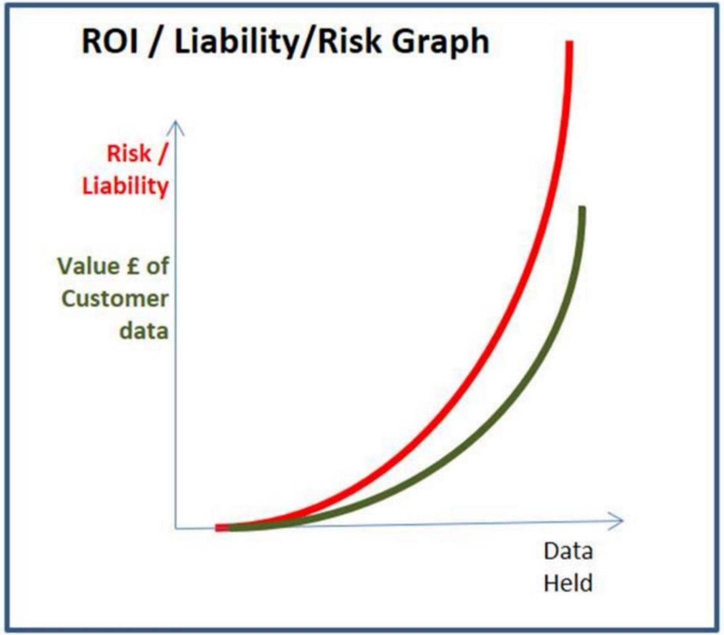
Identity information is currently held by companies about an individual:

- Duplication
- Sensitive data sent to multiple parties
- Company liable for storage
- Many ‘honeypots’ for hackers to attack

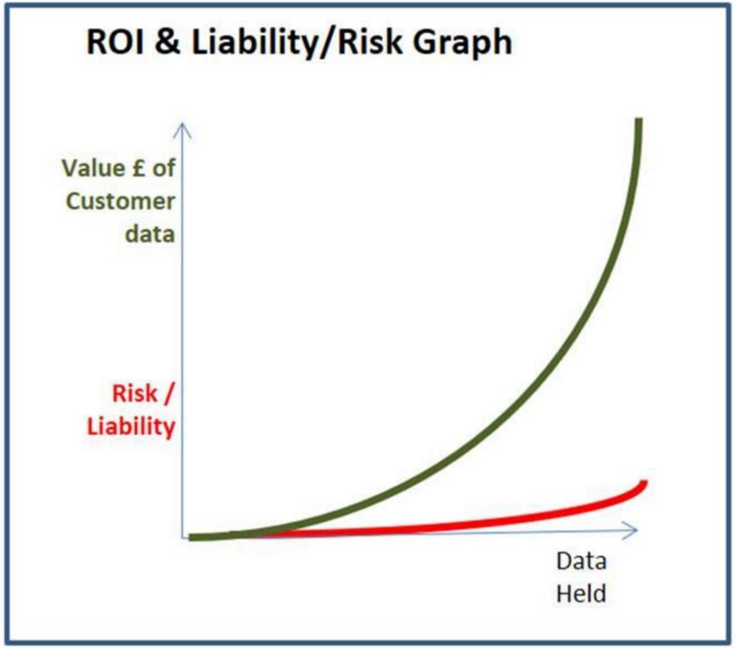


ADCA

Identity is a “Toxic Asset”

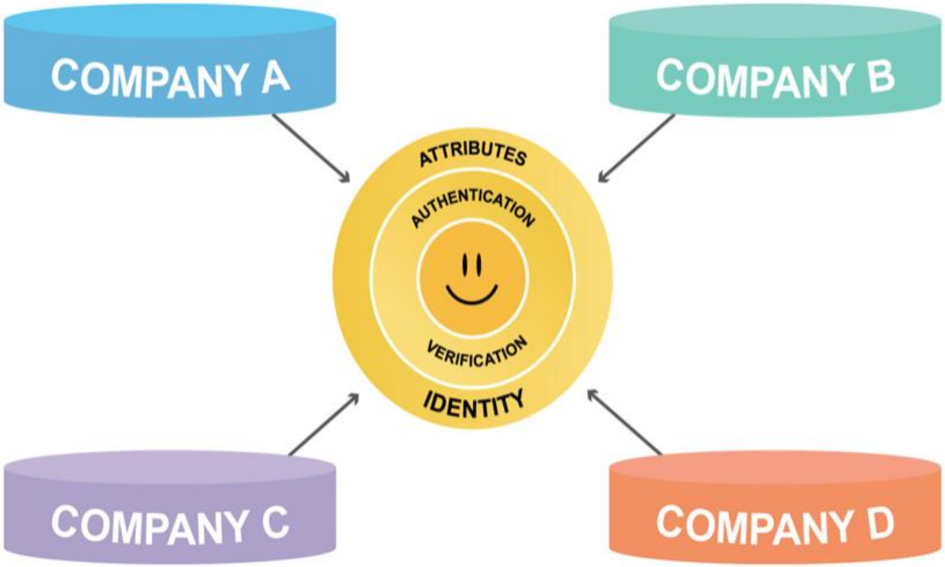


ROI / Liability/Risk Graph



ROI & Liability/Risk Graph

Blockchain could enable “Self-Sovereign Identity”



Australian Blockchain Innovators

ADCA

Introducing Australian Blockchain Innovators

ASX

STANDARDS Australia

DATA 61

CSIRO

ADCA

Introducing Australian Blockchain Innovators

CommonwealthBank

Introducing Australian Blockchain Innovators

OTHERA
No Risk, Business Credit Score

CIVIC LEDGER

agridigital

ScalaMed

tbs x3

BIT TRADE LABS

ADCA

ADCA

AUSTRALIAN DIGITAL
COMMERCE ASSOCIATION

PROMOTING BLOCKCHAIN
INNOVATION IN AUSTRALIA