Blockchain

William Fisher

November 2022

Descriptions

- “[B]lockchain refers to a chain of digital records that are timestamped and organized into blocks, where each block is added in a sequential manner and linked through a cryptographic “hash” of information contained in the prior block in the chain. Each block is stored in a distributed ledger, which is shared, replicated, and synchronized among the participating nodes of a decentralized peer-to-peer network where each such node adheres to a set of rules for validating the addition of blocks to the chain. This characteristic is said to result in an immutable ledger of transactions that cannot be edited or deleted, thereby making a blockchain secure by design.”
    - Covington, “Intellectual Property Issues in Blockchain and FinTech” (2018)

Descriptions

- A decentralized ledger of transactions: "It is a digital record that is shared instantaneously across a network of participants. It is distributed because the record is held by each of the users (or nodes) on the network and each copy is updated with new information simultaneously. DLT uses a consensus technique to ensure that every node agrees on the record, with different distributed ledger technologies using different consensus methods. A key advantage of DLT is that there are not multiple competing sets of records that need to be reconciled but just one, albeit maintained on multiple nodes. This one record represents a golden source of data."
  - Whitepaper, "Smart Contracts and Distributed Ledger – A Legal Perspective" (2017)

Descriptions

- “A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you create a so-called transaction which is required to be accepted by all others. The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied. Furthermore, while your transaction is applied to the database, no other transaction can alter it.

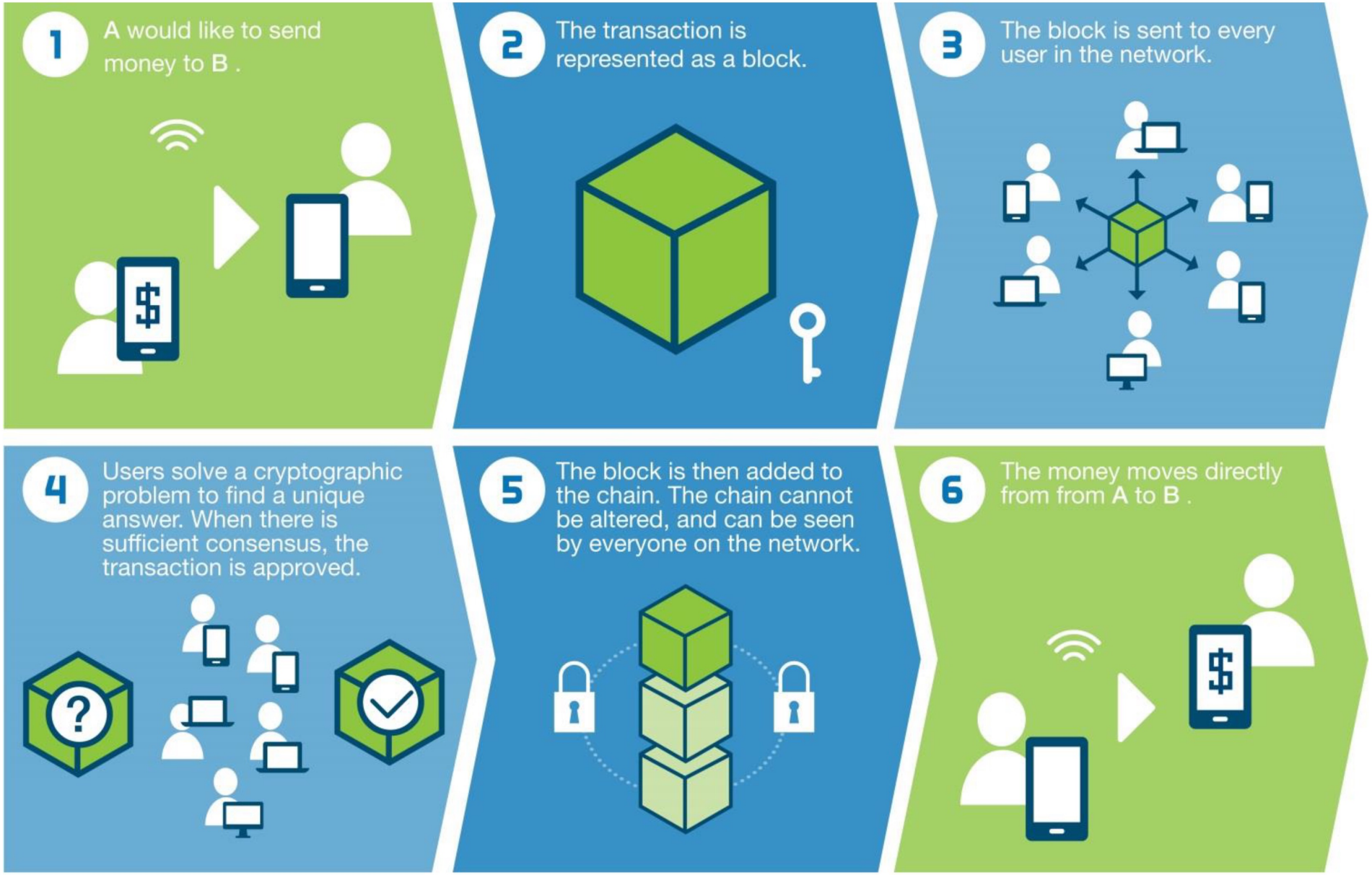
Descriptions

- “A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you create a so-called transaction which is required to be accepted by all others. The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied. Furthermore, while your transaction is applied to the database, no other transaction can alter it.
- “As an example, imagine a table that lists the balances of all accounts in an electronic currency. If a transfer from one account to another is requested, the transactional nature of the database ensures that if the amount is subtracted from one account, it is always added to the other account. If due to whatever reason, adding the amount to the target account is not possible, the source account is also not modified.

Descriptions

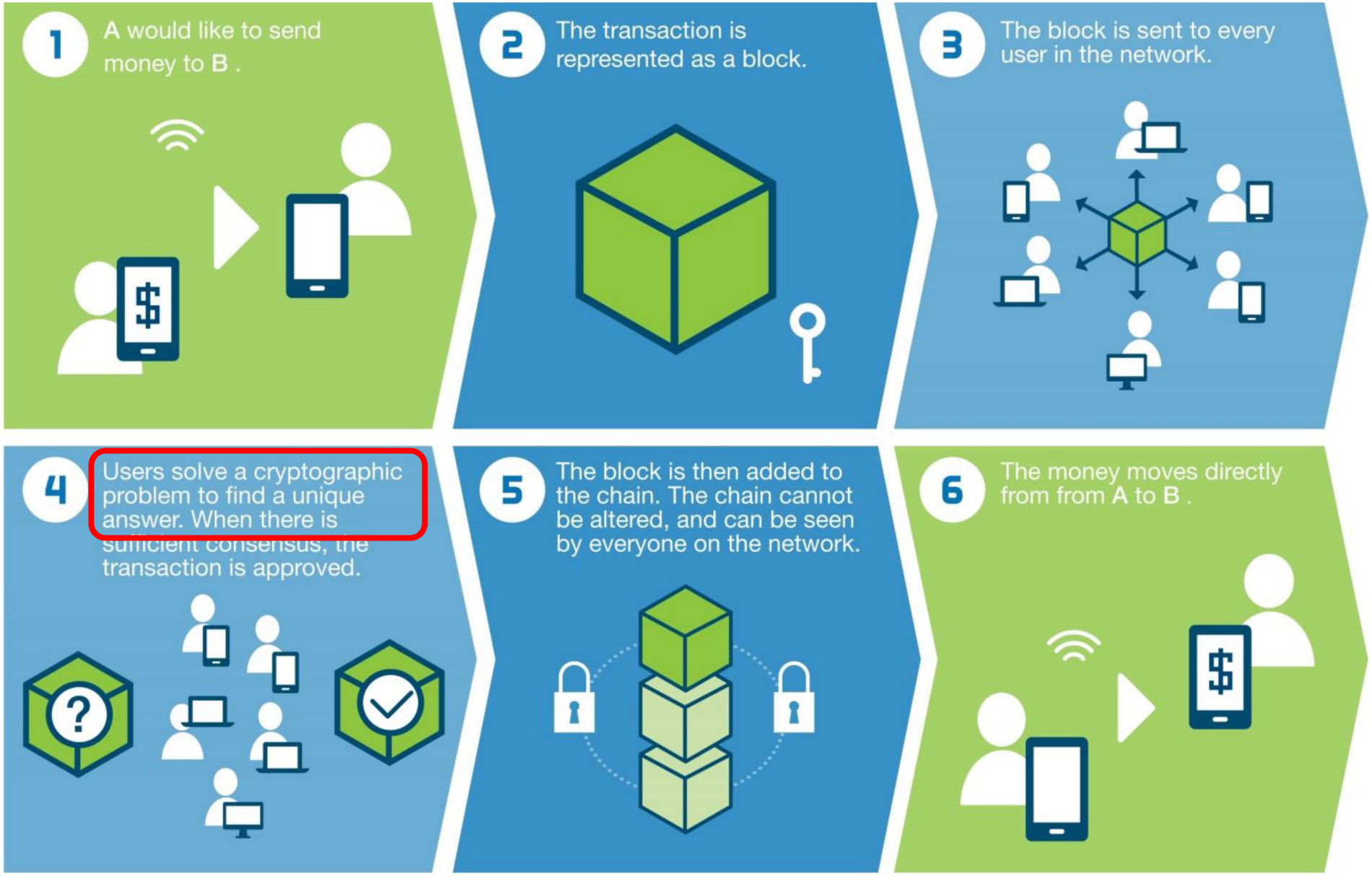
- “A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you create a so-called transaction which is required to be accepted by all others. The word transaction implies that the change you want to make (assume you want to change two values at the same time) is either not done at all or completely applied. Furthermore, while your transaction is applied to the database, no other transaction can alter it.
- “As an example, imagine a table that lists the balances of all accounts in an electronic currency. If a transfer from one account to another is requested, the transactional nature of the database ensures that if the amount is subtracted from one account, it is always added to the other account. If due to whatever reason, adding the amount to the target account is not possible, the source account is also not modified.
- “Furthermore, a transaction is always cryptographically signed by the sender (creator). This makes it straightforward to guard access to specific modifications of the database. In the example of the electronic currency, a simple check ensures that only the person holding the keys to the account can transfer money from it.”
    - “Introduction to Smart Contracts, http://solidity.readthedocs.io/en/develop/introduction-to-smart-contracts.html

Figure 1. Understanding Blockchain – Payment example



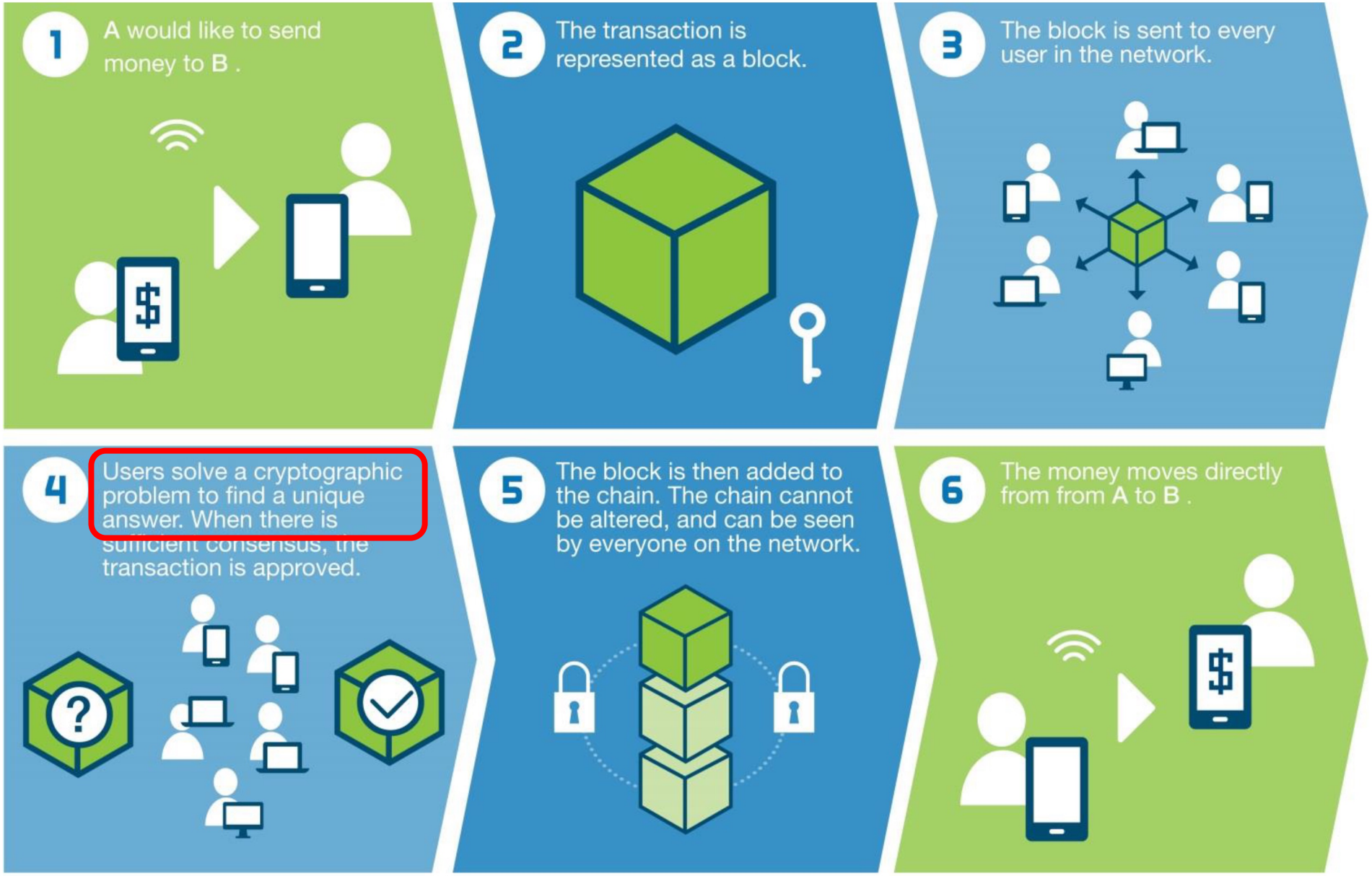
Source: OECD, "Blockchain Technology and Competition Policy" DAF/COMP/WD(2018)47

Figure 1. Understanding Blockchain – Payment example



Source: OECD, "Blockchain Technology and Competition Policy" DAF/COMP/WD(2018)47

Figure 1. Understanding Blockchain – Payment example



Potential Shift from "Proof of Work" to "Proof of Stake" method of achieving consensus

Source: OECD, "Blockchain Technology and Competition Policy" DAF/COMP/WD(2018)47

Applications

- Track financial transactions
- Clear securities trades
- Basis of cryptocurrencies and ICOs
- Track goods in supply chain
- Share patient data among health-care providers
- Digital registries of land titles
- NFTs in art

Varieties

- “public” – anyone can access
  - a.k.a. “permissionless”; “open”
- “private” – participants are limited
  - A.k.a. “permissioned”; “closed”

Inchoate Standardization

← Technical Committees

ISO/TC 307
Blockchain and distributed ledger technologies

About

Secretariat: SA

Committee Manager: Ms Emily Dawson

Chairperson (until end 2023): Mr Craig Dunn

ISO Technical Programme Manager [TPM]: Ms Monja Korter
ISO Editorial Manager [EM]: Ms Christelle Gansonre

Creation date: 2016

Quick links

Work programme
Drafts and new work items

Business plans
TC Business plans for public review

Working area
Working documents (user account required)

Inchoate Standardization

9

published ISO standards *

under the direct responsibility of ISO/TC 307

7

ISO standards under development *

under the direct responsibility of ISO/TC 307

42

Participating members

22

Observing members

Smart Contracts

Smart Contract

- Self-executing agreement in digital form
- Whereas traditional contracts create legal obligations, which require state intervention to support, “smart contracts” enforce the obligations automatically and without state involvement
    - Potential state involvement through *rescission*

Potential examples

- Bet
- Trade of securities
- Mortgage
- Transaction Tax