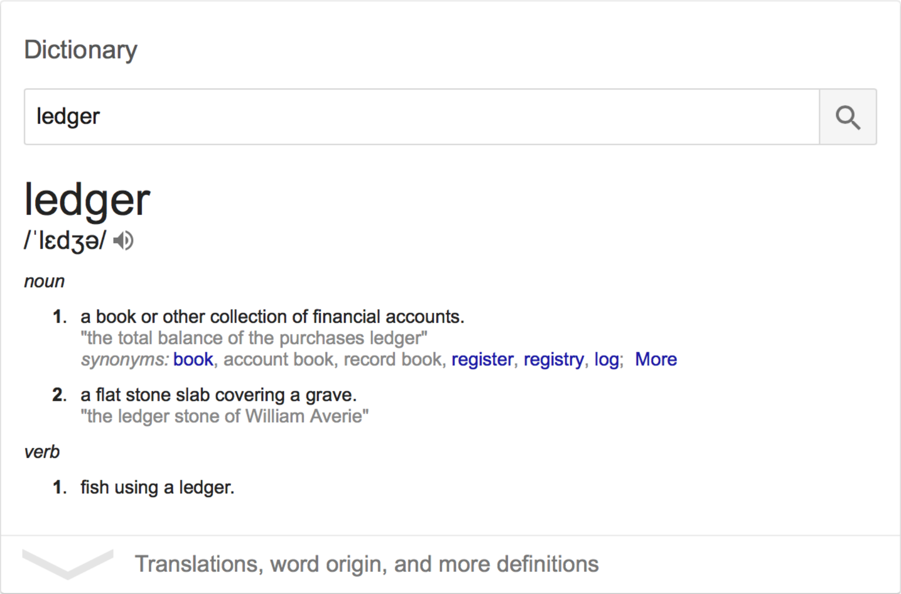
Heiko AYDT PhD (Computer Science)
Technology Enthusiast, Software Engineer

Blockchain Technology in a Nutshell

What is a Blockchain?

Conceptually, it’s a ***distributed ledger***.



Dictionary

ledger

ledger

/ˈlɛdʒə/ 🔊

noun

1. a book or other collection of financial accounts.
   "the total balance of the purchases ledger"
   synonyms: book, account book, record book, register, registry, log; More
2. a flat stone slab covering a grave.
   "the ledger stone of William Averie"

verb

1. fish using a ledger.

Translations, word origin, and more definitions

Example: simple ledger

Ledger A:

Date	Sender/ Receiver	Detail	Debit	Credit	Balance
2017/05/28		Initial Balance		$1,000	$1,000
2017/05/29	B	Transfer	$100		$900
2017/05/30	B	Transfer		$50	$950

Ledger B:

Date	Sender/ Receiver	Detail	Debit	Credit	Balance
2017/05/28		Initial Balance		$100	$100
2017/05/29	A	Transfer		$100	$200
2017/05/30	A	Transfer	$50		$150

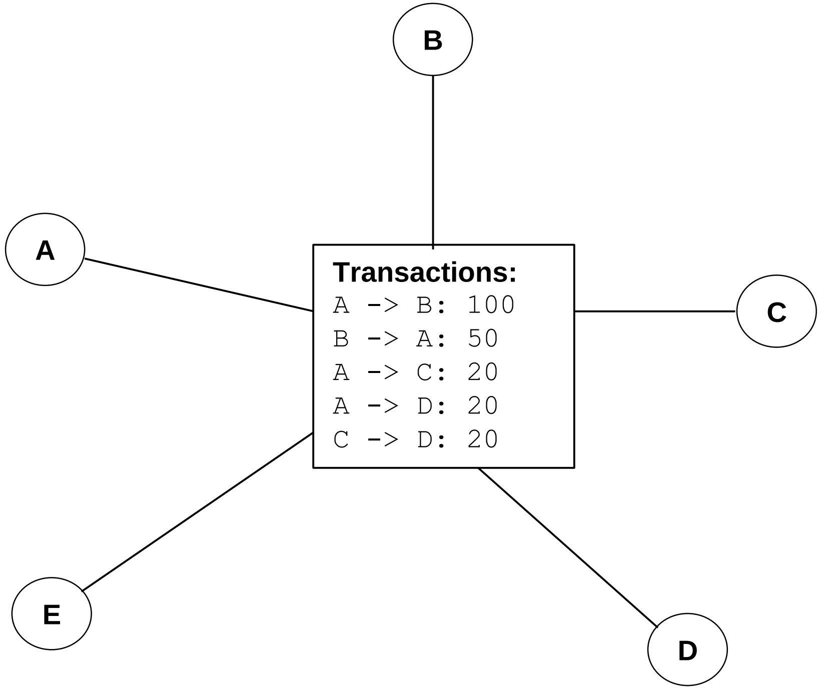
Transactions:

```
A -> B: 100
B -> A: 50
```

Unit of accounts:
USD (for example)

Centralised Ledger

Tusted central authority (e.g., government, banks) maintains records of accounts.



Transactions:

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Balances before:

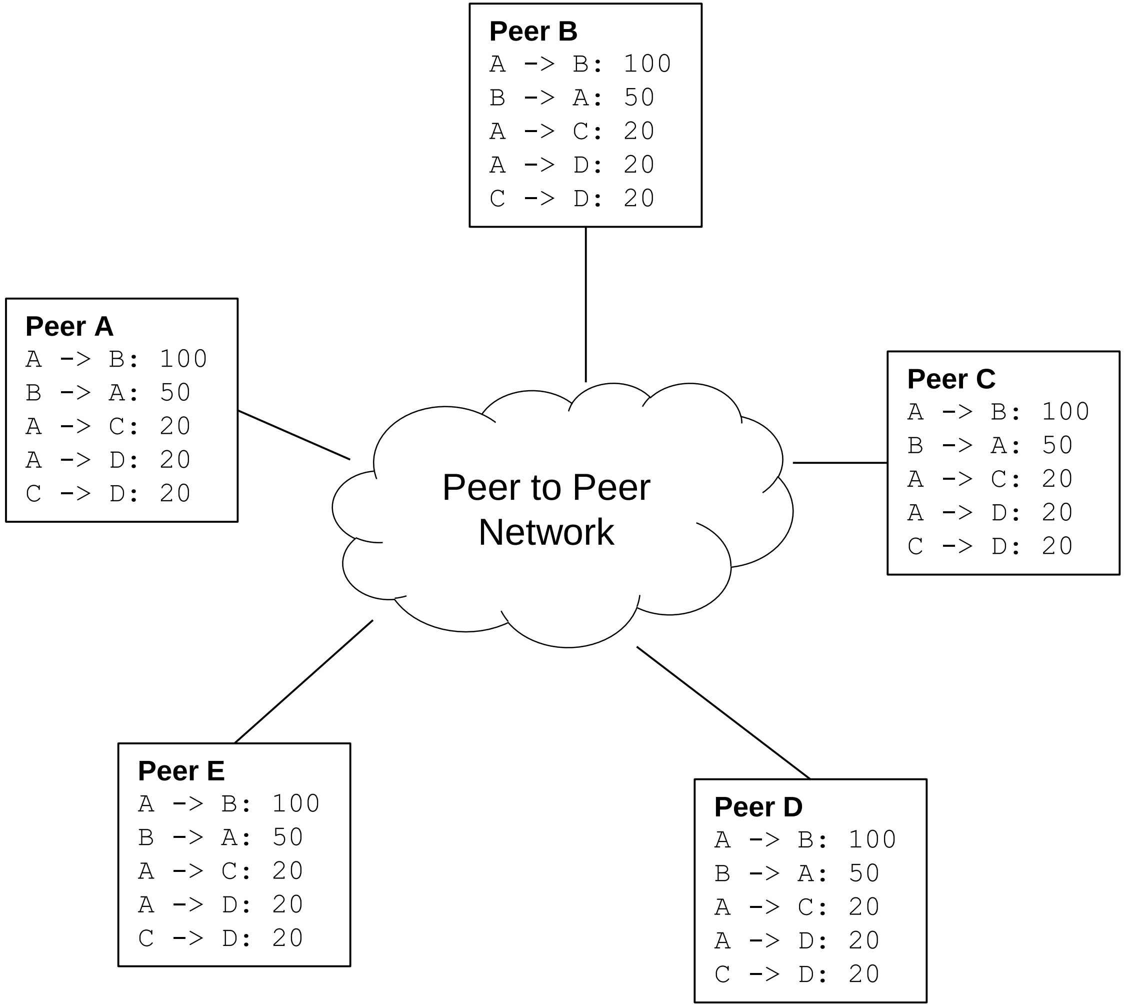
```
A = 100
B = 0
C = 0
D = 0
E = 0
```

Apply all transactions →

Balances after:

```
A = 10
B = 50
C = 0
D = 40
E = 0
```

Distributed Ledger



Peer B

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Peer A

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Peer C

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Peer E

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Peer D

```
A -> B: 100
B -> A: 50
A -> C: 20
A -> D: 20
C -> D: 20
```

Consensus of replicated, shared and synchronised data across multiple sites, countries, or institutions.

There is **no central authority!**

Balances before:

```
A = 100
B = 0
C = 0
D = 0
E = 0
```

Apply all transactions →

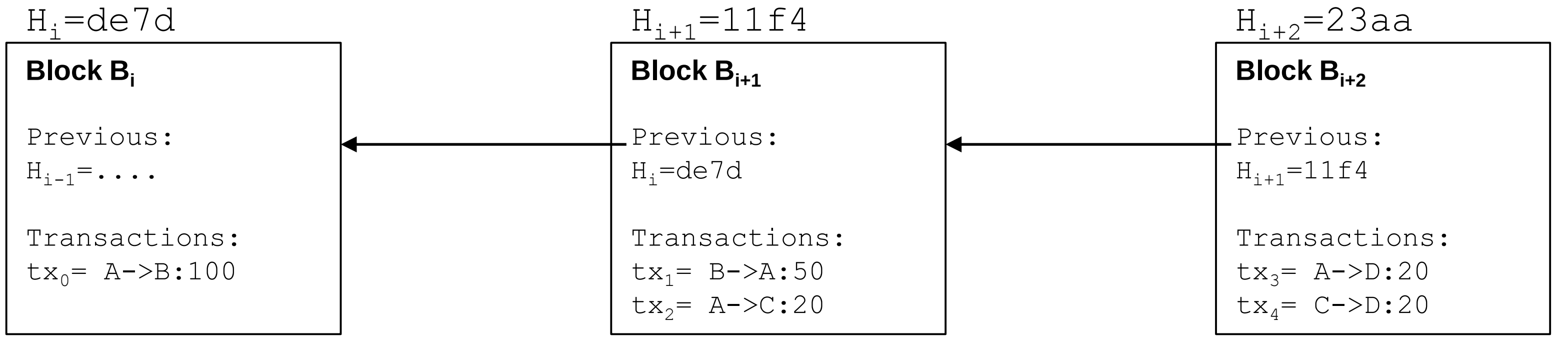
Balances after:

```
A = 10
B = 50
C = 0
D = 40
E = 0
```

What is a Blockchain?

Conceptually, it's a distributed ledger. Technically, it's realised as a continuously growing **list of blocks** which are **linked** and **secured** using cryptography.

Unit of accounts is referred to as ***"coin"***.



H_i=de7d

Block B_i

Previous:
H_{i-1}=....

Transactions:
tx_0= A->B:100

H_{i+1}=11f4

Block B_{i+1}

Previous:
H_i=de7d

Transactions:
tx_1= B->A:50
tx_2= A->C:20

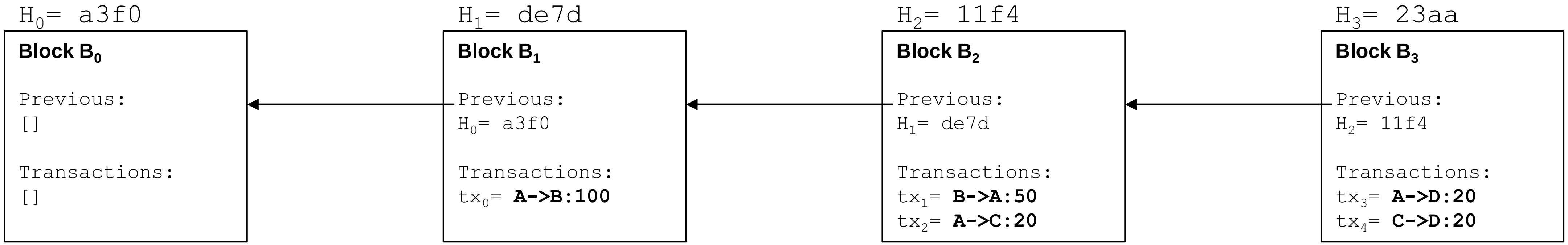
H_{i+2}=23aa

Block B_{i+2}

Previous:
H_{i+1}=11f4

Transactions:
tx_3= A->D:20
tx_4= C->D:20

How does the chain grow?



H_0= a3f0

Block B_0

Previous:
[]

Transactions:
[]

H_1= de7d

Block B_1

Previous:
H_0= a3f0

Transactions:
tx_0= **A->B:100**

H_2= 11f4

Block B_2

Previous:
H_1= de7d

Transactions:
tx_1= **B->A:50**
tx_2= **A->C:20**

H_3= 23aa

Block B_3

Previous:
H_2= 11f4

Transactions:
tx_3= **A->D:20**
tx_4= **C->D:20**

Initial Balances:

A = 100
B = 0
C = 0
D = 0
E = 0

Balances (after B_1):

A = 0
B = 100
C = 0
D = 0
E = 0

Balances (after B_2):

A = 30
B = 50
C = 20
D = 0
E = 0

Balances (after B_3):

A = 10
B = 50
C = 0
D = 40
E = 0

What to remember?

A blockchain is a **distributed ledger** with records of accounts.

Creating new blocks is **expensive**. Validating is cheap.

Retrospectively changing the history of a blockchain is **practically infeasible**.

Key features include:
Immutability
Decentralisation
Auditability

Use cases: cryptocurrencies, payment and accounting systems.

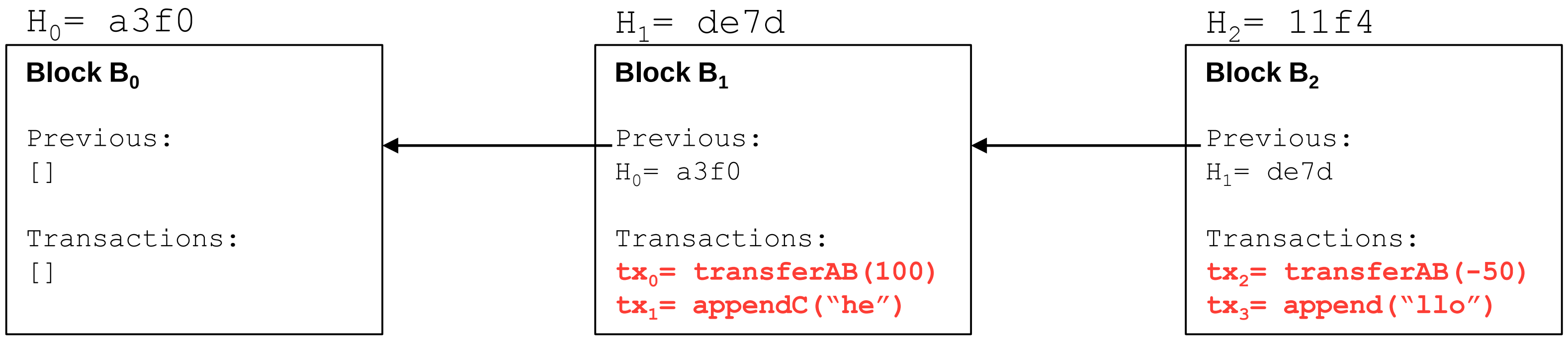
Disclaimer: selection of examples does not imply endorsement of any sort.

Distributed Executable Code Contract (EDCC)

a.k.a. ‘smart contract’

EDCC is a specification of **variables** and **functions**. Once published on the blockchain, it can be executed.

```
contract Example {
 uint256 A = 100;
 uint256 B = 0;
 string C = ””;

 function transferAB(uint256 x)
 {
  A = A – x;
  B = B + x;
 }

 function appendC(string s)
 {
  C = C . s;
 }
}
```



H_0= a3f0

Block B_0

Previous:
[]

Transactions:
[]

H_1= de7d

Block B_1

Previous:
H_0= a3f0

Transactions:
tx_0= transferAB(100)
tx_1= appendC(“he”)

H_2= 11f4

Block B_2

Previous:
H_1= de7d

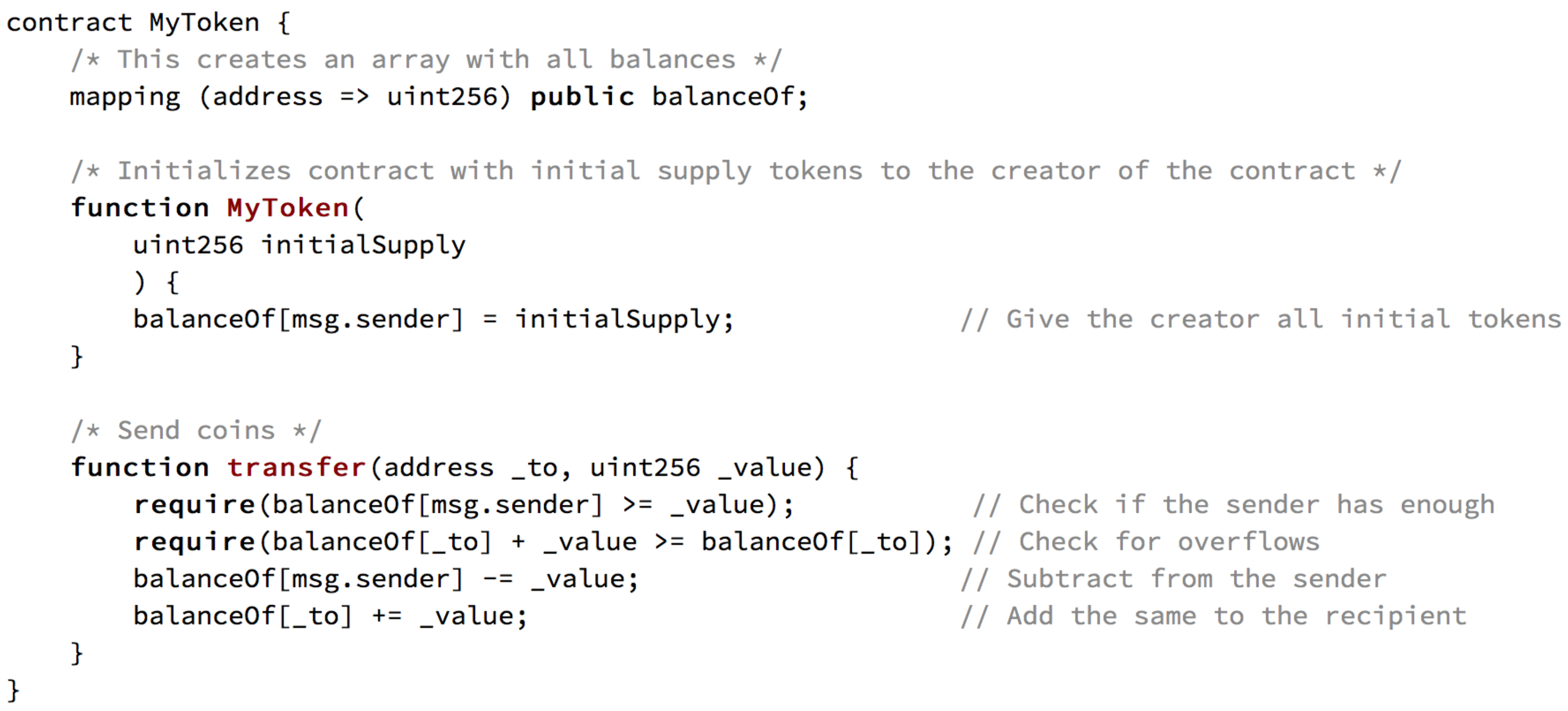
Transactions:
tx_2= transferAB(-50)
tx_3= append(“llo”)

Initial State:
A = 100
B = 0
C = “”

State (after B_1):
A = 0
B = 100
C = “he”

State (after B_2):
A = 50
B = 50
C = “hello”

Example: token contract



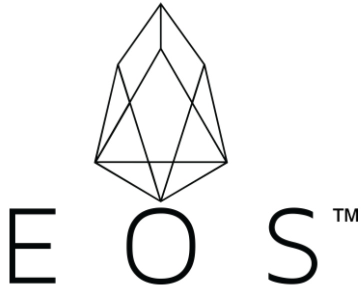
```
contract MyToken {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function MyToken(
        uint256 initialSupply
        ) {
        balanceOf[msg.sender] = initialSupply;              // Give the creator all initial tokens
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

A coin is **native unit of accounts** of a blockchain (e.g., bitcoin, ether, …).

A token is a **EDCC-based unit** that is created and used on a blockchain (e.g., MyToken).

“Tokens in the Ethereum ecosystem can represent any fungible tradable good: coins, loyalty points, gold certificates, IOUs, in-game items, etc.”

Source: https://www.ethereum.org/token (image and quote)



What to remember?

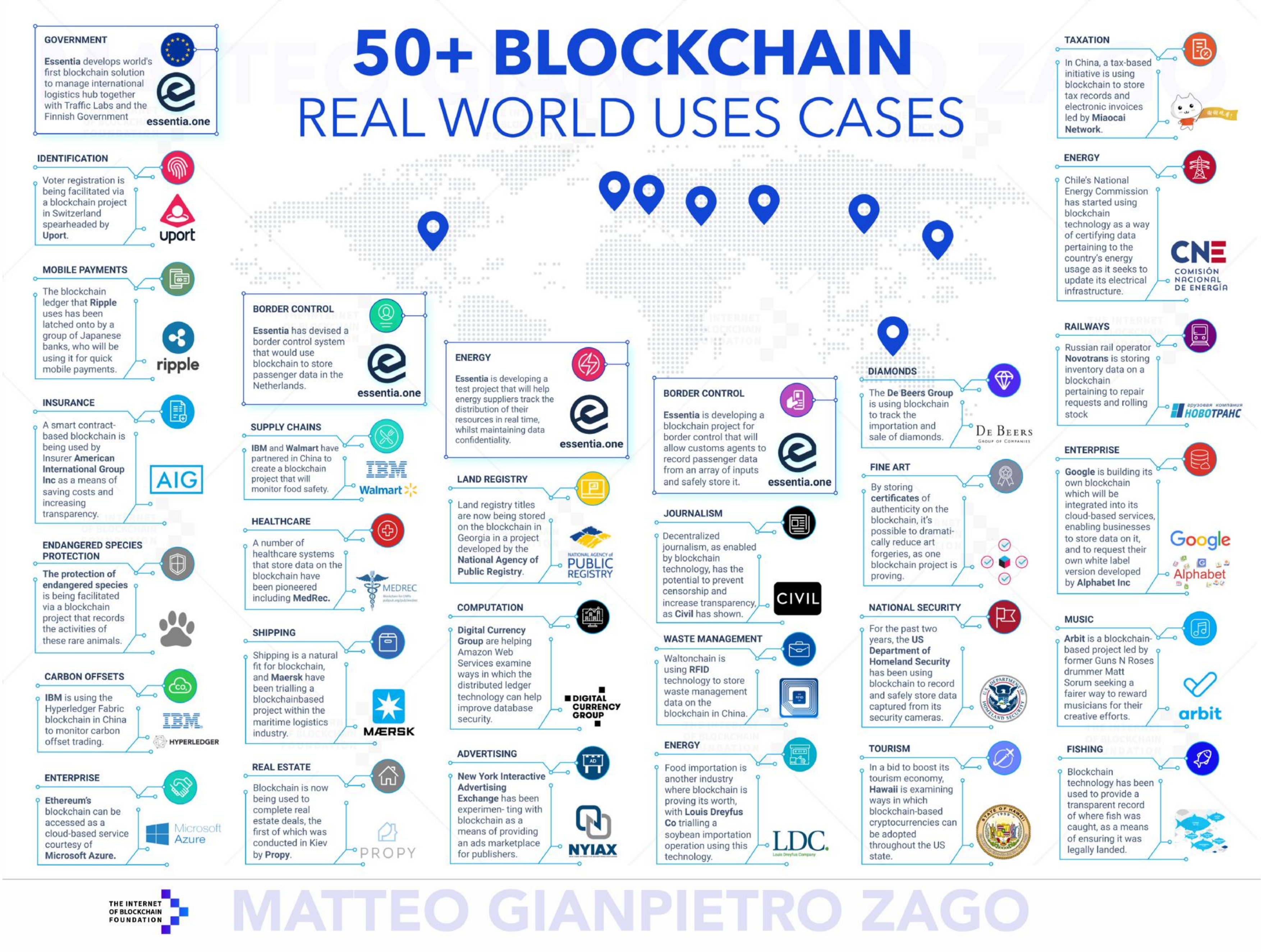
General case of blockchain stores arbitrary states and executes code: World Computer.

Key features include:
Immutability
Decentralisation
Auditability
EDCCs

Use cases: platform for distributed applications (based on EDCCs), tokenised economy, **more to come…**

Disclaimer: selection of examples does not imply endorsement of any sort.

Applications



50+ BLOCKCHAIN REAL WORLD USES CASES

GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers Group of Companies

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock.

грузовая компания НОВОТРАНС

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

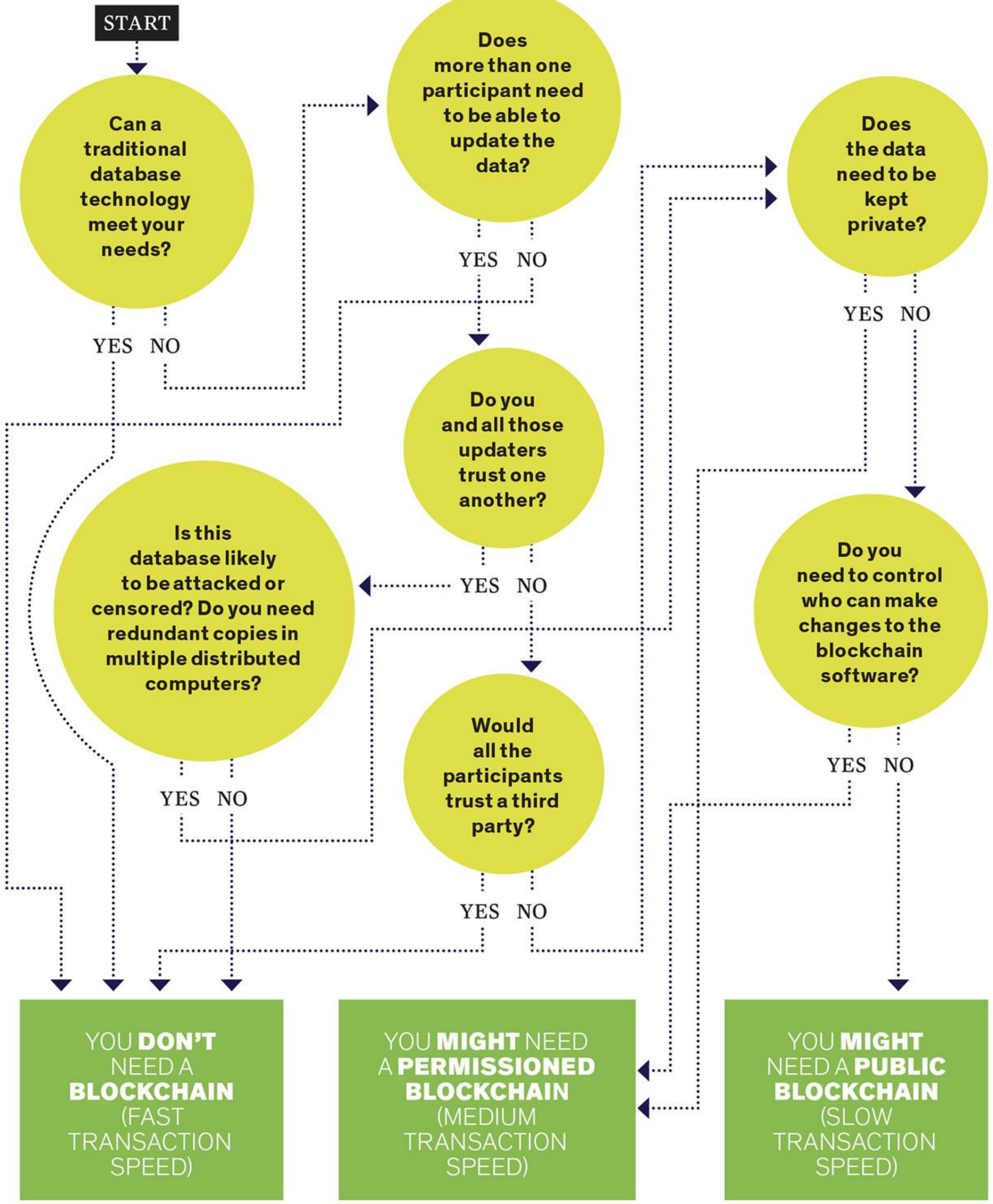
FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

MATTEO GIANPIETRO ZAGO

Source: https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b


START
Can a traditional database technology meet your needs?
YES
NO
Does more than one participant need to be able to update the data?
YES
NO
Do you and all those updaters trust one another?
YES
NO
Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?
YES
NO
Would all the participants trust a third party?
YES
NO
Does the data need to be kept private?
YES
NO
Do you need to control who can make changes to the blockchain software?
YES
NO
YOU DON'T NEED A BLOCKCHAIN (FAST TRANSACTION SPEED)
YOU MIGHT NEED A PERMISSIONED BLOCKCHAIN (MEDIUM TRANSACTION SPEED)
YOU MIGHT NEED A PUBLIC BLOCKCHAIN (SLOW TRANSACTION SPEED)

What’s next?

There won’t be a single blockchain. Instead: diverse ecosystem of public and private/permissioned solutions.

What to look out for?
Regulation
Standardisation
Interoperability

Image: https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain