Blockchain Technology

Plan

Introduction

What’s Blockchain ?

Why Blockchain ?

Blockchain Principles

Technical overview

Types of Blockchains

Blockchain 1.0: Currency

Blockchain 2.0: Smart Contracts

Blockchain 3.0: Decentralized applications

Introduction

- An undeniably ingenious invention that is creating the backbone of a new type of Internet.

- A technology that allows participants to interact with each other without the need for a central authority nor the need for trusting other person we are sending “transactions” to.

- Blockchain has applications that go way beyond obvious things like digital currencies and money transfers.

- From electronic voting, smart contracts and digitally recorded property assets to patient health records management and proof of ownership for digital content.

What’s Blockchain ?

> *“The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.”*

Don & Alex Tapscott, authors Blockchain Revolution (2016)

- A decentralized ledger (database) of all transactions in a peer-to-peer network.

- Every node on the blockchain have a copy the ledger (no central version).

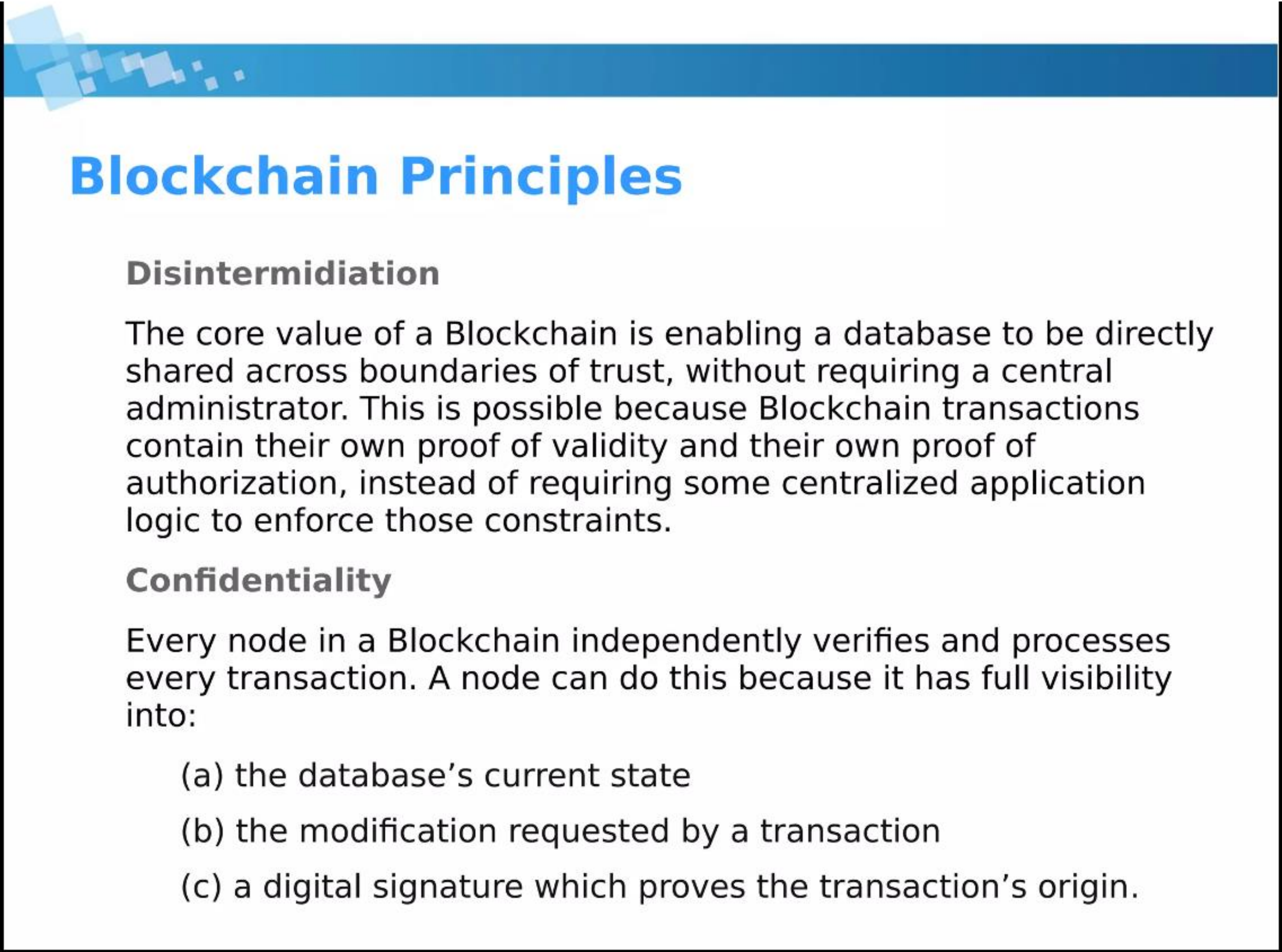
- Every change added to the database should be verified by all the nodes.

Why Blockchain ?

→ **Limits of the traditional system**

- Single point of failure: server failure causes the entire system to stop operating.
- Centralization: the system is controlled by a central authority.
- Intermediaries: participants should rely on a third party to maintain trust.
- Security: central systems are easier to be targeted and tempered with.

→ **Blockchain is designed to solve those issues.**



Blockchain Principles

Disintermidiation

The core value of a Blockchain is enabling a database to be directly shared across boundaries of trust, without requiring a central administrator. This is possible because Blockchain transactions contain their own proof of validity and their own proof of authorization, instead of requiring some centralized application logic to enforce those constraints.

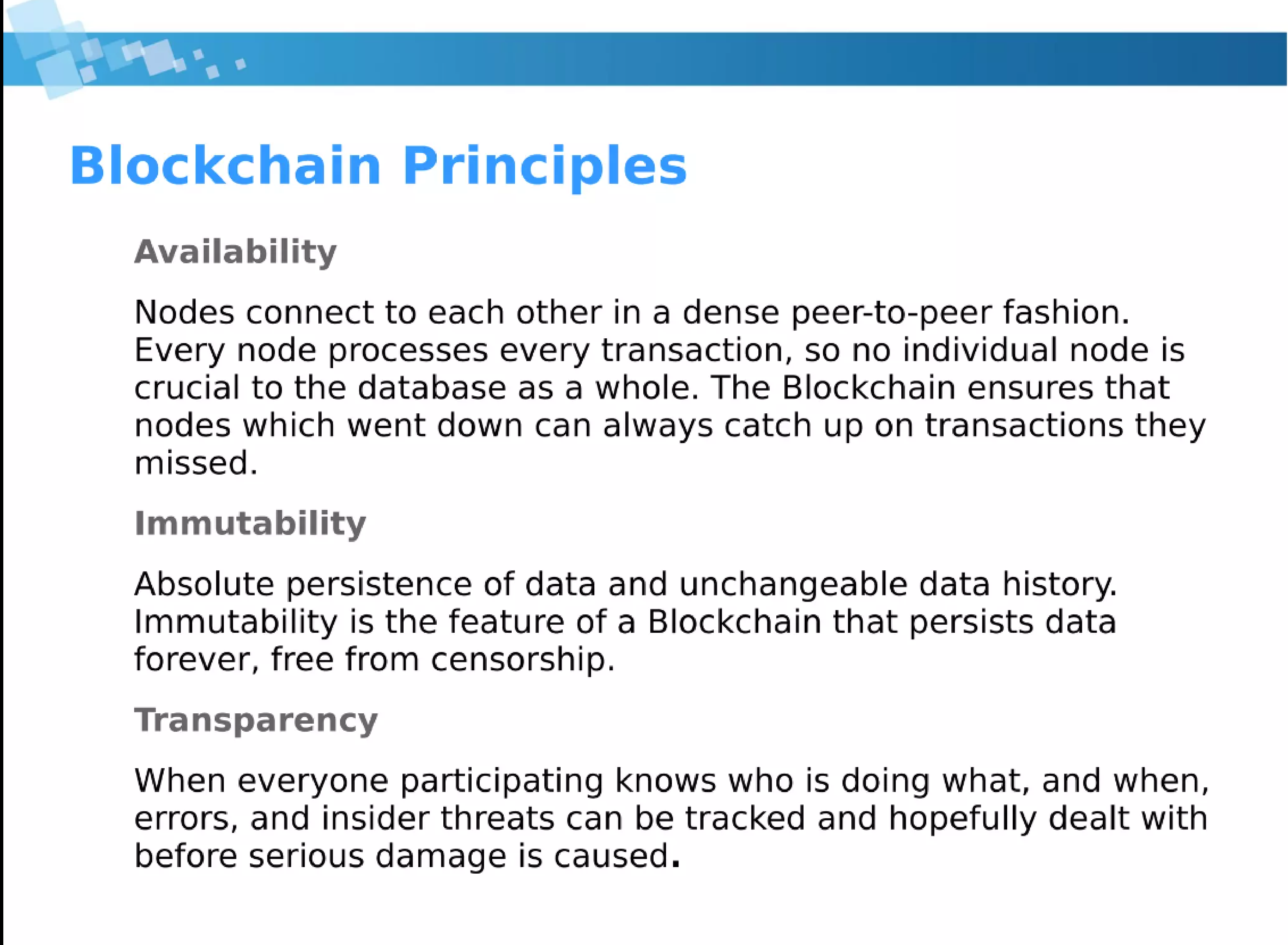
Confidentiality

Every node in a Blockchain independently verifies and processes every transaction. A node can do this because it has full visibility into:

(a) the database’s current state

(b) the modification requested by a transaction

(c) a digital signature which proves the transaction’s origin.



Blockchain Principles

Availability

Nodes connect to each other in a dense peer-to-peer fashion. Every node processes every transaction, so no individual node is crucial to the database as a whole. The Blockchain ensures that nodes which went down can always catch up on transactions they missed.

Immutability

Absolute persistence of data and unchangeable data history. Immutability is the feature of a Blockchain that persists data forever, free from censorship.

Transparency

When everyone participating knows who is doing what, and when, errors, and insider threats can be tracked and hopefully dealt with before serious damage is caused.

Technical Overview

- Transaction (tx)
- Block
- Blockchain
- Mining/Miner
- Cryptography
- Digital signature

Transaction (tx)

Transactions are the most important part of the Blockchain system.

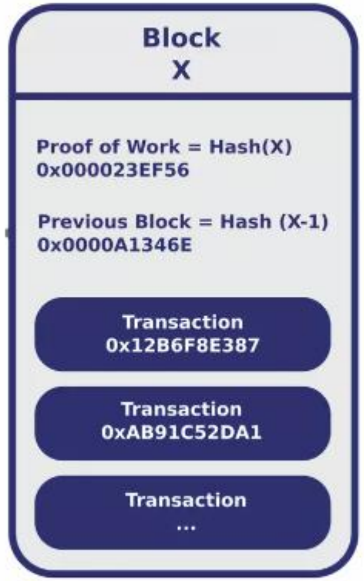
Everything else is designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions (the Blockchain).

Transactions are data structures that encode the transfer of value between participants. Each transaction is a public entry in the Blockchain, the global double-entry bookkeeping ledger.

Blocks

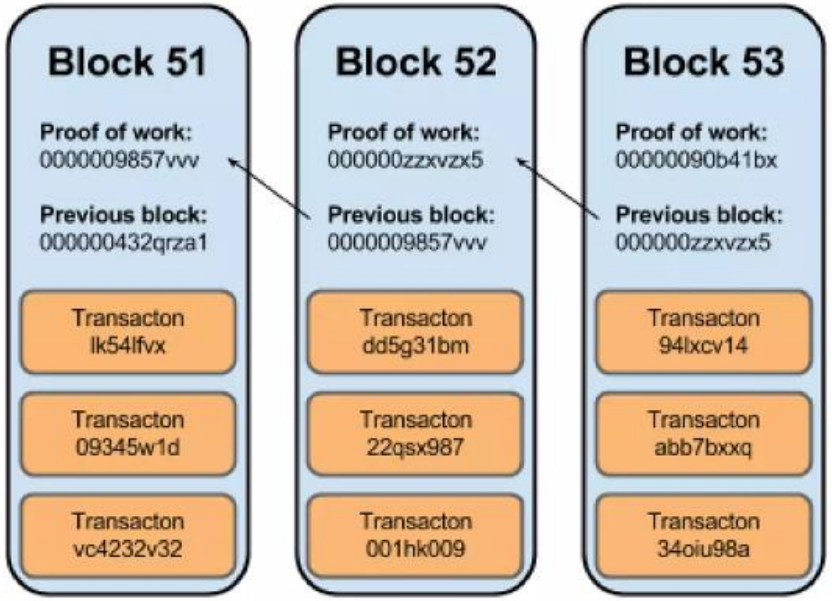
A block is a container data structure that aggregates transactions for inclusion in the public ledger, the Blockchain.

The block is made of a header, containing meta-data, followed by a long list of transactions that make up the bulk of its size.



Blockchain

The Blockchain system orders transactions by placing them in groups called blocks, and linking those blocks together in something called the block chain. The block chain is used to order transactions. Transactions in the same block are more likely to happen at the same time. Each block has a reference to the previous block, and this is what places one block after another in time.



Nodes

Full Node:

A node that have all the history of the chain.

Light Node:

A node that just uses without verification

Mining/Miner

Mining is the process by which blocks are added to the Blockchain. It’s purpose is to verify transactions, and safeguard the block chain.

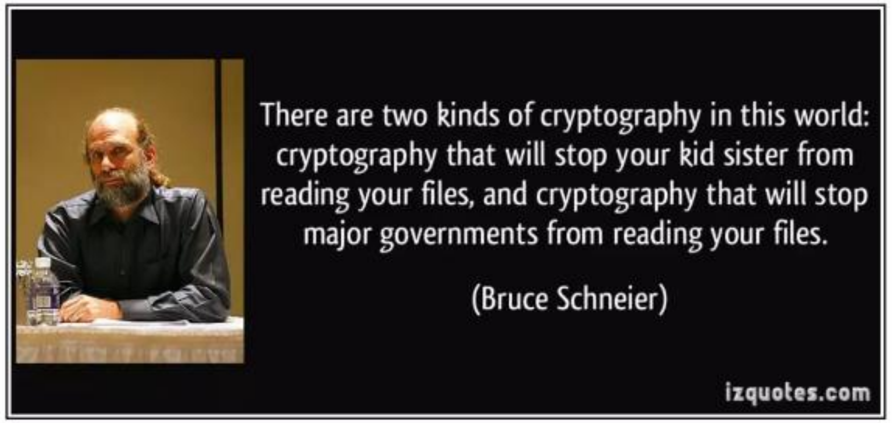
Miners provide processing power to the network in exchange for the opportunity to be rewarded.

Miners validate new transactions and record them on the global ledger. A new block, containing transactions that occurred since the last block, thereby adding those transactions to the Blockchain. Transactions that become part of a block and added to the Blockchain are considered "confirmed".

Cryptography

Public-key cryptography represents an advance over symmetric-key cryptography as far as communications are concerned. Instead of using a single key for both encryption and decryption, separate keys are used for both. A user generates a pair of keys that are mathematically linked to each other.

One key (the public key) is used for encryption and the other (the private key) is used for decryption. The algorithm is designed in such a way that it is infeasible for an attacker to derive the private key from a given public key.



There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

(Bruce Schneier)

izquotes.com

Digital signature

Public-key cryptography has a second benefit beyond just the encryption and decryption of data. It can be used to create something called a digital signature which can be used to simultaneously provide authentication, data integrity, and non-repudiation.

A digital signature is generated by combining a user’s private key with the data he wishes to sign in a mathematical algorithm. Once the data is signed, the corresponding public key can be used to verify that the signature is valid.

Types of Blockchains

We can distinguish three types of blockchains:

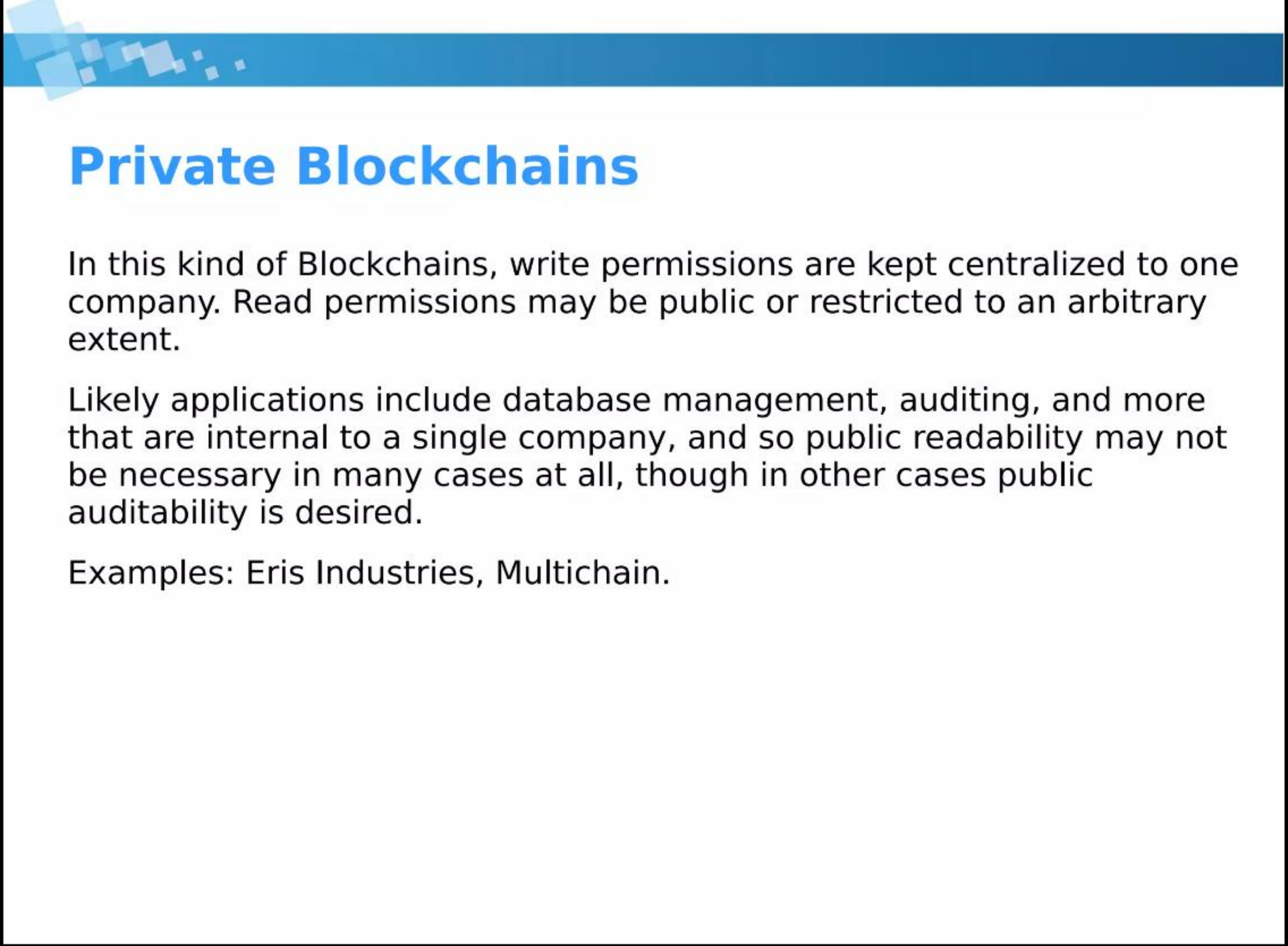
- Public blockchains
- Private blockchains
- Consortium blockchains

Public Blockchains

Anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is.

Public Blockchains are open-source and everyone can be part of them.

Examples: Bitcoin, Ethereum..

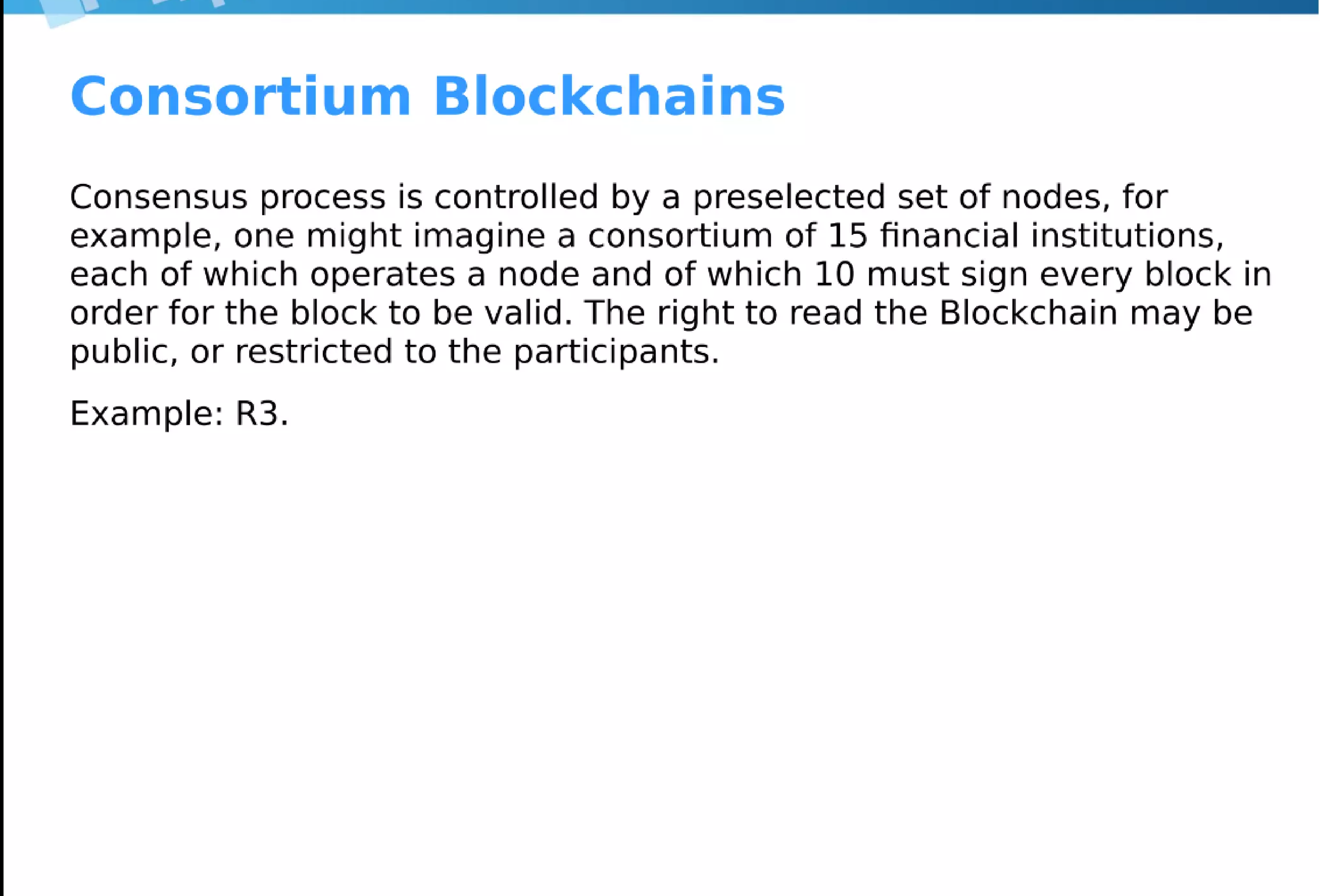


Private Blockchains

In this kind of Blockchains, write permissions are kept centralized to one company. Read permissions may be public or restricted to an arbitrary extent.

Likely applications include database management, auditing, and more that are internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired.

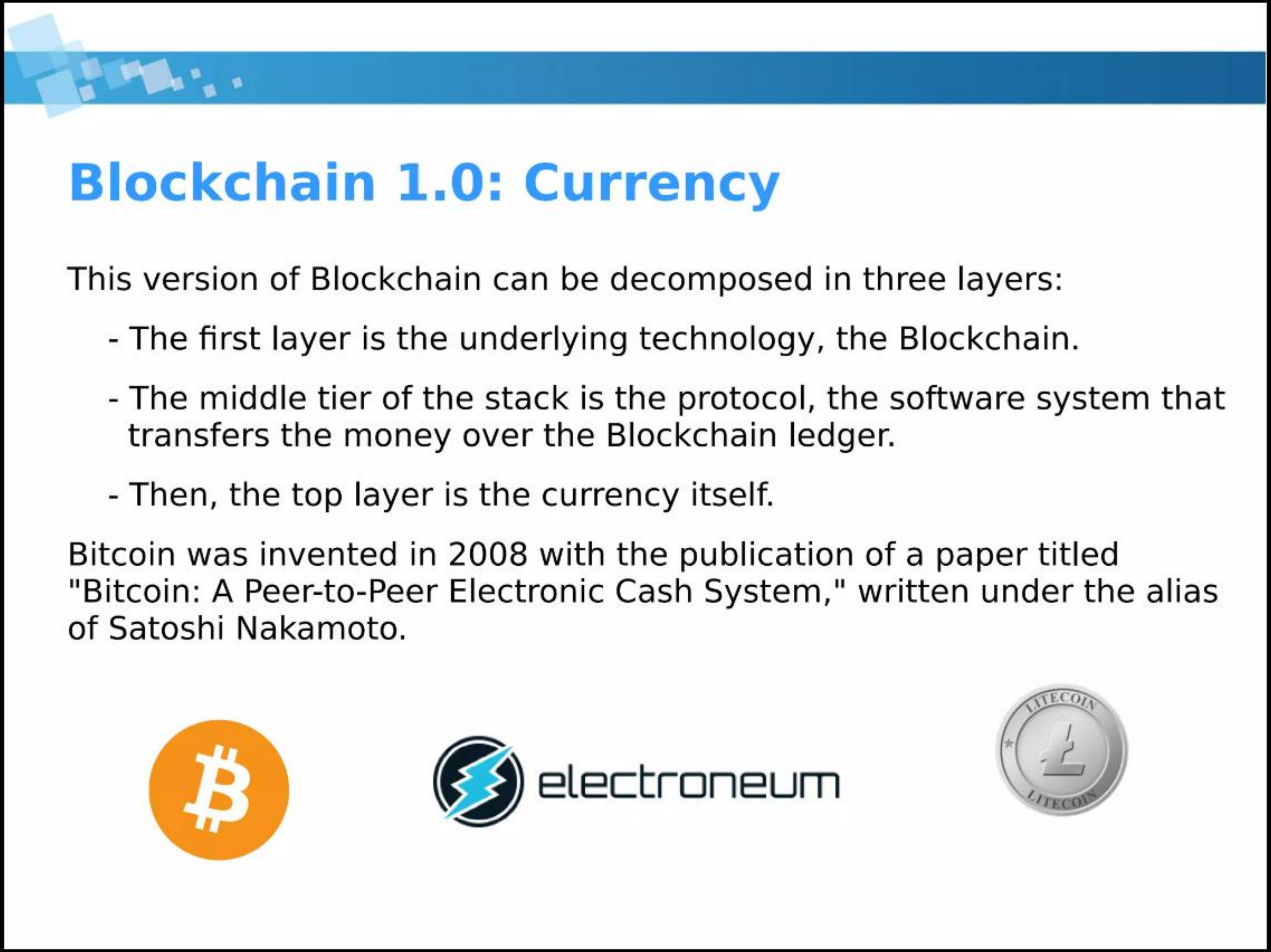
Examples: Eris Industries, Multichain.



Consortium Blockchains

Consensus process is controlled by a preselected set of nodes, for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the Blockchain may be public, or restricted to the participants.

Example: R3.

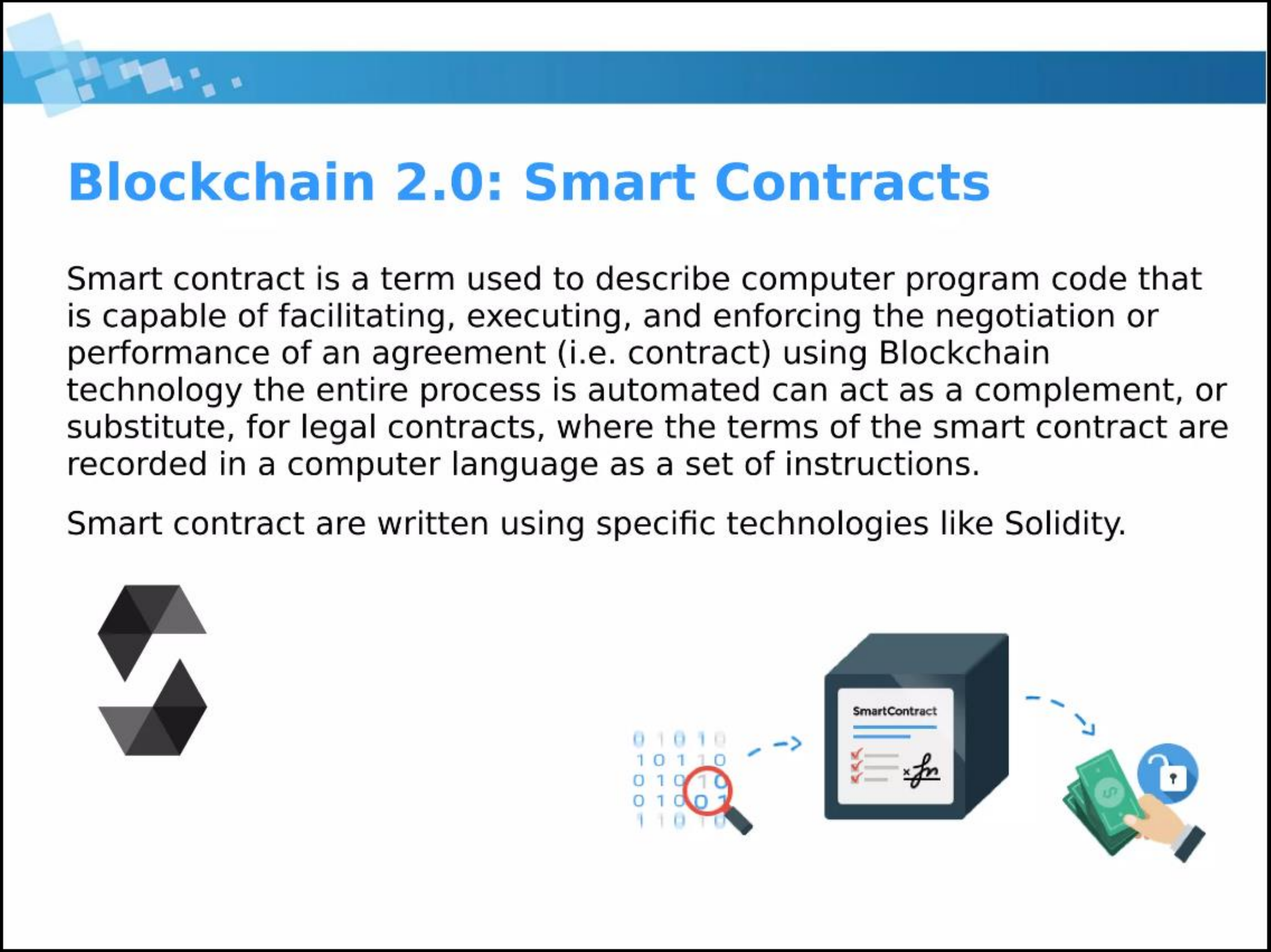


Blockchain 1.0: Currency

This version of Blockchain can be decomposed in three layers:

- The first layer is the underlying technology, the Blockchain.
- The middle tier of the stack is the protocol, the software system that transfers the money over the Blockchain ledger.
- Then, the top layer is the currency itself.

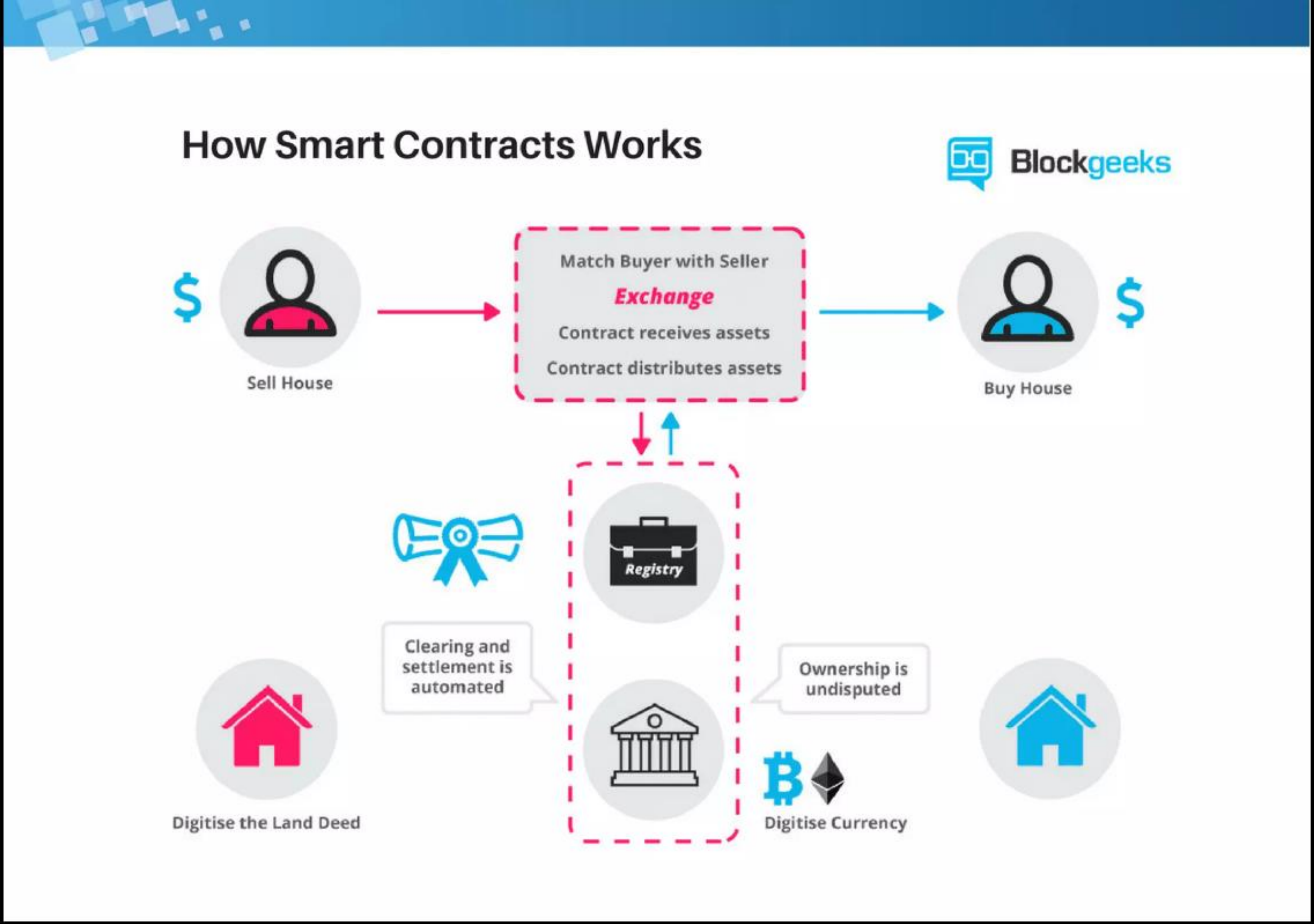
Bitcoin was invented in 2008 with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System," written under the alias of Satoshi Nakamoto.



Blockchain 2.0: Smart Contracts

Smart contract is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement (i.e. contract) using Blockchain technology the entire process is automated can act as a complement, or substitute, for legal contracts, where the terms of the smart contract are recorded in a computer language as a set of instructions.

Smart contract are written using specific technologies like Solidity.



How Smart Contracts Works

Blockgeeks

Sell House

Match Buyer with Seller

Exchange

Contract receives assets

Contract distributes assets

Buy House

Registry

Clearing and settlement is automated

Ownership is undisputed

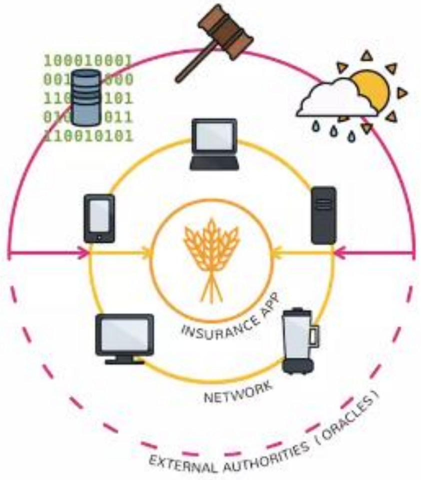
Digitise the Land Deed

Digitise Currency

Blockchain 3.0: Decentralized Apps

One broad way of thinking about the use of blockchain concepts is applying them beyond the original context in the areas of government, health, science, literacy, culture, and art.

Exp: Voting application, OpenBazar, HealthCare.



Thanks