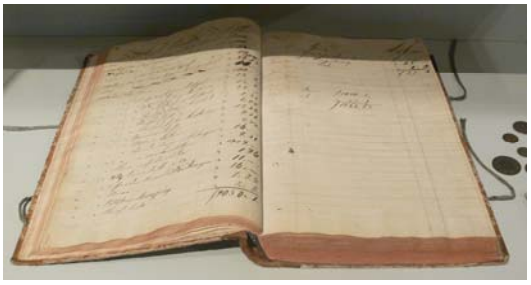
UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
KATEDRA ZA PRIMENJENE RAČUNARSKE NAUKE

Blockchain Technology and Distributed Secure Document Storage

Dr. Dušan Gajić, University of Novi Sad, Serbia
18 September 2019, Vrdnik, Serbia
e-mail: dusan.gajic@uns.ac.rs

Ledger

- **Double entry bookkeeping** – each entry to an account has a corresponding entry to a different account – **debit** and **credit**
- A **ledger** is the principal book for recording and totaling transactions, with **debits and credits** in separate columns and a beginning monetary **balance** and ending monetary balance for each account

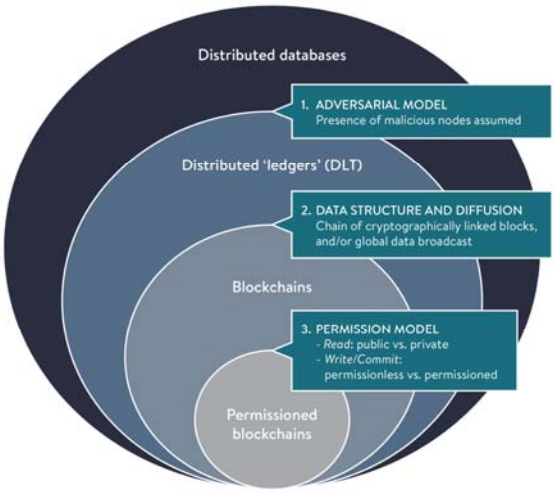


Source: https://en.wikipedia.org/wiki/Ledger#/media/File:Hauptbuch_Hochstetter_vor_1828.jpg

Distributed Database, Ledger, and Blockchain

- A **distributed database** is a database that consists of data stored on different sites (computers)
- A **distributed ledger** or **distributed ledger technology** (**DLT**) is a special kind of distributed database which assumes existence of **malicious users** (nodes), a **consensus** of **replicated**, **shared**, and **synchronized digital data** geographically spread across multiple locations
- A **blockchain** is a **distributed data structure** which implements a **distributed ledger**, it is composed of a **chain of cryptographically linked blocks** containing **sets of transactions**. In the general case, a broadcast of all the data to all the network participants is performed
- **Blockchain and cryptocurrencies are not one and the same**

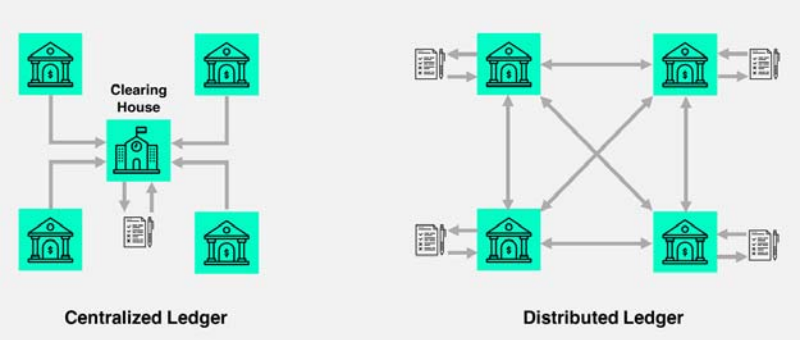
Distributed Database, Ledger, and Blockchain



Source: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$FILE/ey-global-blockchain-benchmarking-study-2017.pdf

Distributed Ledger Technology – DLT

- **Centralized** and **distributed ledger**:



Source: https://tradeix.com/distributed-ledger-technology/

Blockchain

- **Combination** of a **consensus mechanism** with a **specific data structure** allows blockchain to solve the **double spending problem** – same digital file is copied and sent multiple times – **without the need for a centralized ledger** or an **authority which would prevent users from duplicating or spending the same digital file multiple times**
- **Blockchain** can, therefore, be used for **managing transactions of assets or other data without the need for the central authority** in which everyone needs to trust

Blockchain

- So **blockchain** is, for most intents and purposes a **database**
- What makes it **unique among databases**:
  - It only **allows changes if several parties independently can agree** on **which changes need to be made**
  - **Distributes all the data** among multiple peers
  - **Every change is stored permanently** and is **cryptographically protected from being altered** and **can't be deleted** without destroying all the data

A Blockchain Use Case: Distributed Secure Document Storage

The Problem

- The **correct storage of certain documents** which can **guarantee** their **integrity and security** requires:
  - **Replication.** Making sure that **sufficient copies exist** to make sure their **contents are difficult to lose**
  - **Counterparty guaranteed integrity.** Making sure that **all the copies are identical** and making sure **multiple parties** in the system **can guarantee this**
  - **Tamper-resistance.** Making sure that a **malicious participant** in the system **cannot change their copy** of the document and **have that change propagated**
  - **Access control.** Making sure that **access to the documents is only possible under the correct circumstances** and with the **correct form of authorization**
  - **Leak control.** Making sure that **if a document should leak**, it can be **traced back to the leaker**

The Use Case

- Who would want such properties? **Anyone storing**:
  - **Personal identity information**
  - **Medical records**
  - **Intellectual property documentation**
  - **Financial records**
  - **Banking records**
  - **Large project documentation** & **safety information**
  - Ultimately, any type of **sensitive** and **vital document**

The Use Case

- An effective example – **storing land registry documentation**
- These documents themselves are the **principal guarantors of ownership over real-estate** which makes up an approximate **87% of the world's total wealth**
- Furthermore there is **every incentive for a malicious person with control over the land registry to alter those documents** and, by doing so, effectively be able to steal vast sums
- **Even without malice**, the **loss of such documents** or their **mistaken alteration can cause untold damage**

The Solution

- **Replication** is achievable by using a **distributed file storage system**—storing copies of the file in multiple locations with automated propagation of changes
- **Counterparty-guaranteed integrity** is achievable by **keeping the signatures and metadata** stored **on a distributed ledger** and using **smart contracts to enforce rules** on how they may be changed
- **Tamper-resistance** is achievable by systematically using **sophisticated digital signature solutions**, guaranteeing that the **file cannot be changed without this change being evident**
- **Access control** is achievable by **granting smart contracts the ability to enforce access rules** by applying multiple cryptographic methods
- **Leak control** is achievable by using **dynamic keyed steganographic solutions with cryptographically secure timestamps and steganographic keys logged indelibly on the blockchain**

Technology Stack

- The **Interplanetary File System** solution and the **ActorDB distributed database** provide the basis for **storing files in a distributed fashion**
- **Hyperledger Fabric** provides best-of-class distributed ledger technology
- **Digital signatures** are provided using **a security-by-diversity approach** using RSA-4096/Blake2b plus Ed25519/SHA512 plus ECDSA-secp256k1/SHA-3
- **Smart contracts** are written in **Go** and the **crypto-shredding** and **access control security** is provided by AES-256 in GCM mode

- **Hyperledger** is an open-source initiative led by the **Linux foundation**
- **Hyperledger Fabric** is an **enterprise-grade private, permissioned blockchain** allowing **great engineering potential** – it can be used to construct some **truly disruptive solutions**
- **Disruptive**? **Not really.** Everything's disruptive these days but, in truth, enterprise-grade blockchain, especially Hyperledger Fabric isn't really built for that. It is built for being **constructive**.
- Its **extreme flexibility and unprecedented control allows** for blockchain-based solutions to **conform to existing regulations and workflows without demanding alterations** to conform to the often inflexible logic of more primitive blockchain implementations

Benefits – Resistance to Attack

Risk	Response
Files in storage are destroyed.	As long as at least one copy remains in the system they can be restored.
Files in storage are modified illegally.	As long as at least one copy remains anywhere, they can be repaired, and the modification is noted using digital signatures and hash-based checksums.
Cryptographic algorithm we rely on is broken.	We avoid cryptographic single points of failure—as long as one of the signature schemes work, we can recover.
An illegal attempt is made to propagate a change to files through the system.	Automated smart contracts can detect illegitimate changes and resist the changes recording their dissent and the original data indelibly on the global distributed ledger.

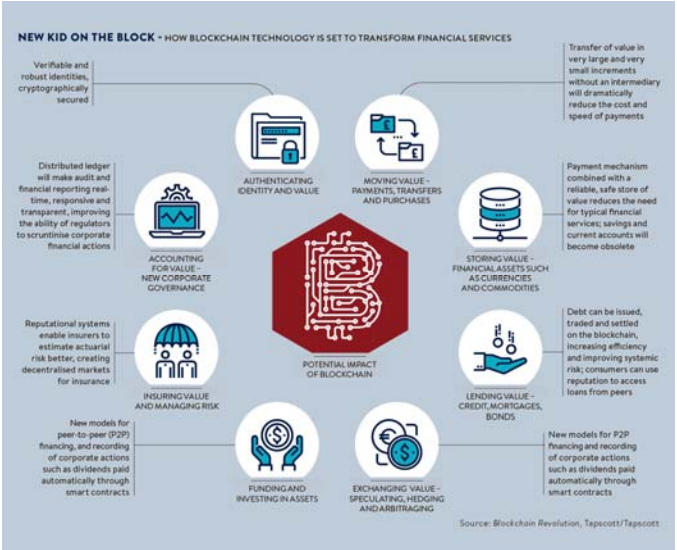
Benefits – Resistance to Attack

Risk	Response
A participant tries to access files illegally.	Lack of primary authorization is noted by the system before it even gets to deeper security system an the attempt is rebuffed and logged indelibly on the blockchain.
A participant tries to access files illegally with stolen primary authorization.	The malicious user is stopped at the first hurdle as they cannot decrypt the first cryptographic barrier coded to a private key available only to a legitimate user of the file.
A participant tries to access files with stolen primary authorization and the private key.	The malicious user is stopped by the first line of smart contract access control defense by checking secondary authorization and not issuing decryption privileges.

Benefits – Resistance to Attack

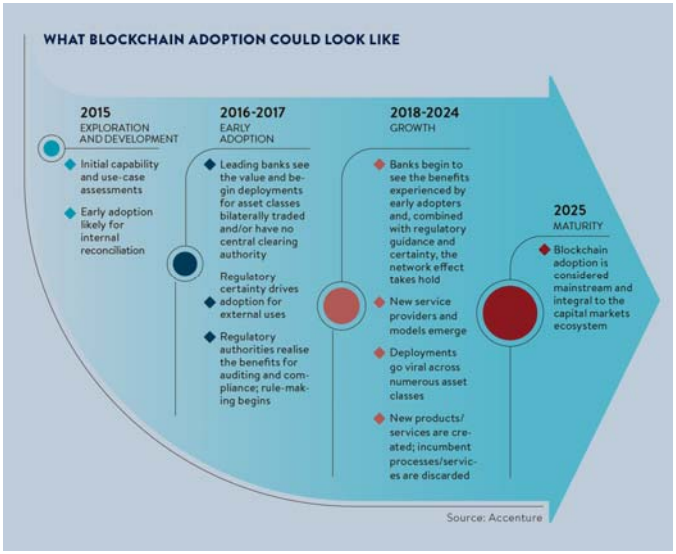
Risk	Response
A participant has stolen primary authorization and the private key and has subverted the hardware of the first-line decryption node.	The second-line decryption node notes the subversion attack and locks down the file.
A participant tries to access the file without leaving trace of it.	Impossible due to the nature of blockchain logging without subverting the entire network at the same time.
A user has gained legitimate access to the document and then leaks it anonymously.	Impossible to prevent absolutely, but may be traced by marking every document steganographically with an encrypted string which identifies the user under whose authorization the document has been accessed.

Conclusions – The Value of Blockchain



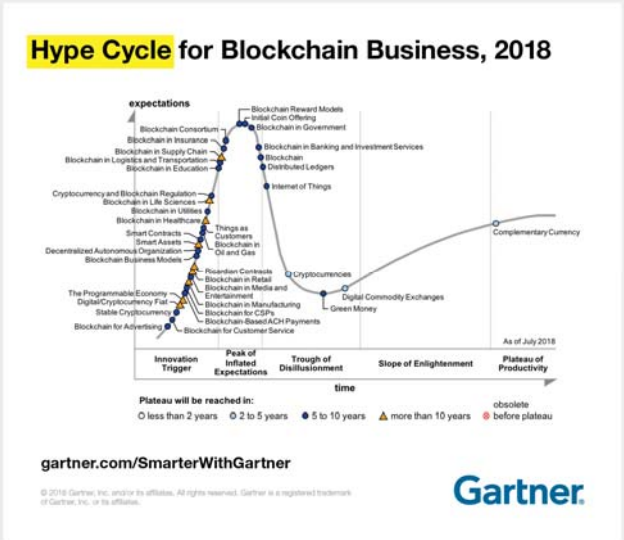
Source: https://www.raconteur.net/business-innovation/the-future-of-blockchain-in-8-charts

Conclusions – The Future of Blockchain



Source: https://www.raconteur.net/business-innovation/the-future-of-blockchain-in-8-charts

Conclusions – The Future of Blockchain



Source: https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/

UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
KATEDRA ZA PRIMENJENE RAČUNARSKE NAUKE

Blockchain Technology and Distributed Secure Document Storage

Dr. Dušan Gajić, University of Novi Sad, Serbia
18 September 2019, Vrdnik, Serbia
e-mail: dusan.gajic@uns.ac.rs