Deloitte.

Distributed Ledger Technology e Capital Markets

Paolo Gianturco // Deloitte Consulting

Milan, 27th of June 2017

The evolution of data storing

Let’s take a step back: databases, from centralized to distributed ones

Centralized Database

- Data are stored and maintained in a **single location**
- The common choice for the storage of data is using **Relational database Management System** (RDBMS)
- In RDBMS data are organized in **tables** and a **query language** (typically SQL) is used to access to them
- RDBMS is the **standard used** for the storage of information for financial records, manufacturing and logistical information, personnel data, and other applications since the 1980s

Distributed Database

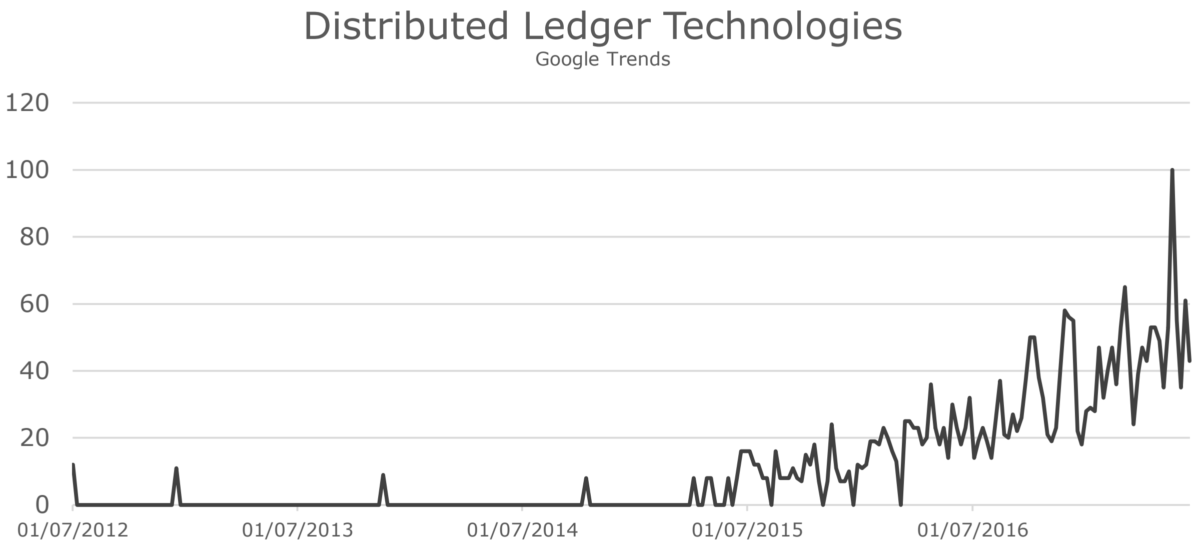
- Data are stored and maintained in multiple instances **across a network**
- The **Distributed Database Management System** (DDMS) become popular with the diffusion of internet
- The distribution of the nodes guarantees a **high resilience** of the network and a **faster access** to the shared information
- DDBMS needs **consensus mechanisms** to ensure fault-tolerant communications between different nodes[1]
- There are a lot of **different types** of Distributed Database, on of them is the **Distributed Ledger (DL)**

[1] “Blockchain – a very special kind of Distributed Database”, S. Meunier

So, what makes a Distributed Ledger so special?

Distributed Ledger Technologies

The architecture underlying the Blockchain



A Distributed (shared) Ledger **is a type** of Distributed Database (DDBMS) contributed by different parties across different locations. It is basically an **ordered log of sequential updates** validated by the network through a consensus algorithm.

To work efficiently and reach a consensus on the information shared a Distributed Ledger has to:

- Be accessible only to **vetted nodes**[2] (*permissioned*)
- Leverage **cryptography** to provide a decentralized multi-version consensus over the state of the ledger and verify it

Blockchain is a particular type of Distributed Ledger

[2] "Bitcoin, Blockchain and DLT: Hype or Reality", F.M. Ametrano's presentation

And what is a Blockchain?

The chain of blocks

Something more, without losing any feature of a Distributed Ledger

Blockchain is the most known DLT.

It’s a distributed ledger that solves some typical problems of distributed networks like **trust**, data security and **immutability** opening the participation to shared ledger to anyone

As the term suggests is a *chain of blocks* based on **hash values** proving the coherence and **security** of the whole chain, so that any edit in the middle of the chain implies the reprocess of the following blocks

In the first formulation – the **Bitcoin** protocol – the *chain of blocks* represents a practical solution to the *Byzantine General Problem*

Blockchain uses the **incentives**, as defined in game theory, as an instrument to make the users **keepers** of the network security

Immutable by design

Thanks to the Proof-of-Work a change on a previous record of the ledger implies the redoing of all the subsequent blocks

Immutable

Permission-less

Trust-less

Immutability of data is reached using Blockchain: this is a fundamental property very hard to reach in digital realm

How is it possible?

Blockchain is an **append-only database** where the information stored are organized in an ordered, **cryptographically secure**, **back-linked** list of **blocks**. Every subsequent blocks is linked to the previous one through **hash pointers**. A change in a block **break the validity of the chain**, therefore it is easy and immediate **to spot any change** in the blockchain

> [Bitcoin] Is a remarkable cryptographic achievement. The ability to create something which is not duplicable in the digital world has enormous value.
>
> Eric Schmidt, Alphabet Chairman

Permission-less open to everyone and restrictable by no one

Anyone can join and contribute, but no one can arbitrary exclude a node from the network

- Immutable
- **Permission-less**
- Trust-less

Permission-less blockchain means that anybody can join the network and create or add data into the shared ledger

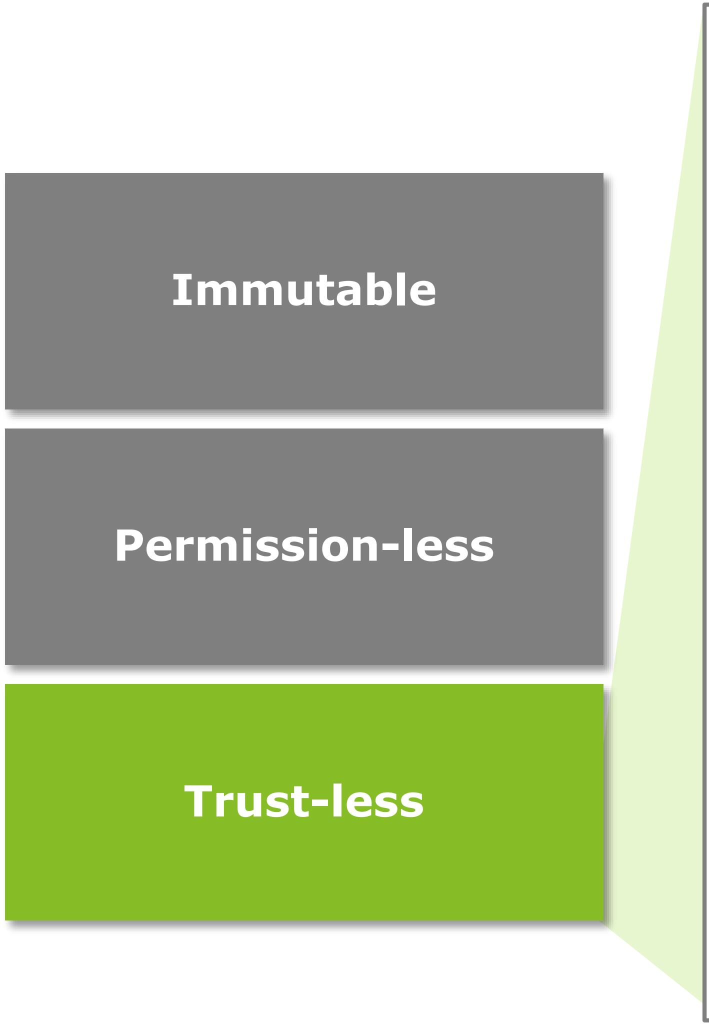
How is it possible?

Blockchain is shared over the network and there is not a central authority, or a group, that holds the right access to the shared database. **Every single node is equal to another one** and every data shared flow through a peer-to-peer transfer protocol.

> A private blockchain is an intranet, and a public blockchain is the internet. The world was changed by the internet, not a bunch of intranets.
>
> Brian Forde, MIT

Trust-less is more trusty

In this symmetric information context no one need to trust another node, because every one can simply verify by itself



Trustless blockchain means that the network can run without the need of a trusted authority responsible of the data.

How is it possible?

The problem of reaching a **consensus on the state of the network** in an uncoordinated environment is known as the Byzantine General Problem. This problem has an insolvability proof in computer science. Nakamoto found a **probabilistic solutions** to this problem leveraging **economic incentives** and **cryptographic calculation**: the **Proof of Work** (PoW)

> “Proof-of-work has the nice property that it can be relayed through untrusted middlemen. It doesn't matter who tells you a longest chain, the proof-of-work speaks for itself.
>
> Satoshi Nakamoto, Bitcoin Creator

Why is this revolutionary?

It is not just the technology, but the combination of different elements that makes Blockchain technology really disruptive

Area	References	Relevant parts
Game Theory	▪ *Hashcash*, **Adam Back**, 1997 ▪ *Reusable P-o-W*, **Hal Finney**, 2004	▪ **Consensus Design: Proof of Work**
Cryptography	▪ *Ecash*, **David Chaum**, 1982 ▪ *Elliptic curves in cryptography*, **Victor Miller**, 1985	▪ **Digital Signature** ▪ **Elliptic Curve Cryptography**
Networking	▪ *B-Money*, **Wei Dau**, 1988 ▪ *Bit gold*, **Nick Szabo**, 1998	▪ **Distributed Database** ▪ **Sequential money creation**

Could Distributed Ledger Technology really help the financial industry?

The Capital Markets Industry

A quick overview about the Industry and the infrastructure layers to be changed

Industry Efforts

To-date more than **$1.1bn has been invested in various start-ups.** The average deal size has increased from $2.6M in Q4 2015 to $11.4M in Q1 2016

WEF reports that, by 2027, **10% of the global GDP** could be stored on blockchain technology

200+ companies are involved in the research and development of blockchain ecosystems and use cases

A Banco Santander report states that DLTs (Blockchain) could **help banks save $15bn-$20bn annually, by the year 2022**

Capital Market Layers[3]

In the Capital Market infrastructure three main layers could benefit from DLTs innovation:

👍 **Securities Ownership Registry**
The security ownership process is one of the most control-driven in the Capital Markets with physiological loss of efficiency in terms of delivery timing and overall costs: DLTs will bring improvements if they manage to store, in the block, state information with transaction

👍 **Clearing and Settlement**
Unlike the trading process, there is no necessity to aggregate orders, so the decentralized process of DLT will bring some benefits such as high availability

👎 **Trading Reconciliations**
The underlying concept of order aggregation does not really fit with DLT's decentralized processing architecture, and it is hard to bring improvement if there is already an effective centralized order processing facility

[3] "Applicability of DLT to CM Infrastructure", Japan Exchange Group

During last years the CM Industry has widely explored the DLT world

Use cases and PoC have been developed for different CM processes and layers

Processes	As Is	With DLT
Exchange of Value Is the process of **exchanging value** between different subjects, like individuals or financial institutions including branches of the same institute	This process is **centralized** and **needs trust** in the central counterpart (or a group of) that provides the service	Most common example of Exchange of Value over DLTs is Bitcoin, but banks are interested in **cross-border** transfers and any solution aimed to reduce liquidity absorption
Timestamping (Ownership) A timestamp is an information on a document that **proves the existence** of the document itself prior a specific point in time	Timestamps are today performed by **notaries** and therefore needs and high level of **trust** and are **expensive**	With the blockchain features, such as the **absence of trust** and **immutability**, it is possible to create very **tamper proof timestamps**
Know Your Customer (KYC) The KYC is the process used to **identify** a client verifying their identity through the analysis and keeping of some documents	Every different bank have to perform the KYC process by itself even if the same process has been performed **a lot of time** by different companies	It is possible to create a **common platform** where one of the participant performs the required KYC and **stores the results**

Conclusions

A brief summary about DLTs and CM Industry

1 **Distributed Databases and Ledgers**

Ledgers have to be intended as a sequential log of updates with a heavy use of cryptography to assure the consensus process, while distributed databases are relational and just need *a* consensus mechanism

2 **Not a Panacea**

DLT & Blockchain are not a panacea for the Capital Markets industry, they’re an advanced technical instrument and, like any instrument, they’re useful for a precise set of problems

3 **Processes before technology**

Financial Institutions are highly interested in DLTs: unluckily most of them put all their efforts in forcing these solutions to fix their present processes instead of taking the opportunity to review those as-is processes and improve them *with* DLTs

“

If I had asked people what they wanted, they would have said faster horses.

Henry Ford

Deloitte.