2018

BLOCKCHAIN IN THE SUPPLY CHAIN

Orchestrate resource planning in frictionless fashion

FULVIO FAMULARO

InfiniLedger
DIGITAL INNOVATION & CONSULTING

The following notes are meant to be a general overview on Blockchain, some definitions, some high-level benefits, a potential use case, general factors to consider in assessing a potential implementation and the challenges this technology wave is facing and will face for a wide adoption. It is not mean to be a deep dive analysis, neither in regards of the "engine room" of the technology nor in the detailed nuances of the supply chain various architectures. At the end of this document there is a partial list of readings to continue your journey in this exciting space.

INTRODUCTION

During the last couple of years almost everybody has been following the rapid expansion of Bitcoin and the hundreds of crypto currencies around the world. Bitcoin was developed as a digital cash system enabling people to make direct payments between themselves without a need of a central authority or third-party intermediary to regulate the transactions flow.

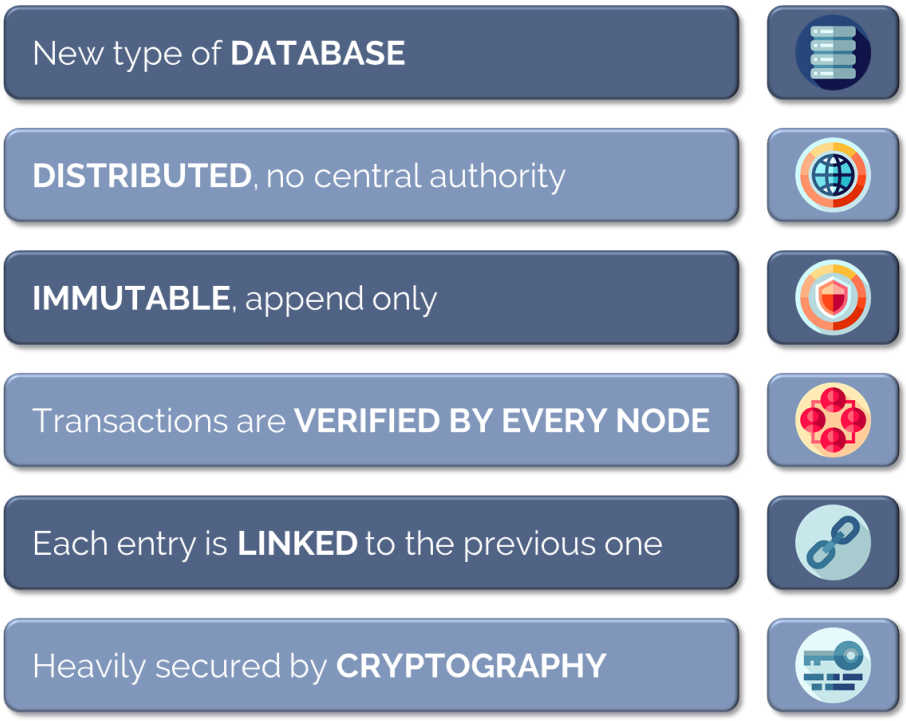
While Bitcoin, with a world-wide and explosive success, changed some of its original characteristics and usage over time, its underline technology attracted the interest of the financial community first and countless additional industries after. This key layer is the so called Blockchain and understanding it enable to grasp a disrupting wave coming for countless industries and applications in the years to come. A wave comparable to what internet did for our modern society in the last 25 years.

BLOCKCHAIN DESCRIPTION

Blockchain is essentially a new type of database, distributed without a central control hub. Its immutable and the entries are append-only, without the possibility of modifications. The transactions and data are verified by each node and grouped in blocks. Each block is heavily secured by cryptography and chained together with additional crypto hashing algorithms.

All the participants in the network have the same, unchangeable, tamper proof, distributed database (or ledger) containing the history of all the transactions.

Full programming capabilities could be added to the Blockchain, thus enabling the creation of so called "smart contracts". Those powerful tools allow not only to record transactions in a more efficient way but could also make these agreements autonomous and self-enforcing.



BLOCKCHAIN BENEFITS

There are at least four major areas where Blockchain could bring significative advantages across different industries.

Security Gains. This is probably the most evident benefit a Blockchain implementation can bring. As mentioned, all data are encrypted with hash functions. The data in the blocs and the blocs themselves cannot be modified by can only be added in a sequence. The blocks in this sequence are concatenated to the previous one with additional cryptographic mechanism, further enhancing the security of the whole chain. One attempt to modify and change an element will disrupt the sequence and the synchronization with all the other copies of the chain on the participant nodes.

Efficiency Gains. Having the same copy of the database synchronized and shared among multiple nodes brings considerable efficiency in large corporation or extensive business networks. With the possibility to embed programming modules in the blockchain itself, there is the possibility to automate several steps in a potential transaction, reducing at the same time manual intervention. Finally, having such automatism mechanism in place allows a significant increase of standardization and reduction of manual intervention.

Time Savings. One of the main characteristics of the Blockchain architecture is the distributed nature of the database. That means no central hub or authority is required, thus rendering several layers of intermediaries unnecessary. This brings a reduction of obstacles and bottle necks in the execution process with significant time gains.

In addition to that, having automatic mechanism in place such as smart contracts, allows a significant reduction of transactions time, in some sectors from days to hours or even close to real time.

Cost Savings. The first factor which influence a cost reduction is due to the shared database nature of Blockchain. With each node having the same copy of the database in real time creates an automatic redundancy architecture with major advantages against a central, hub-and-spoke framework. Less oversight and active control, being the network self-policed by modular consensus mechanisms, and ultimately by the participants themselves. Less security cost to single protect the hub, central authority. Less hardware investments to power up the central hub, the whole IT infrastructure could be implemented on a leaner and lighter HW/SW infrastructure.

BLOCKCHAIN IN THE SUPPLY CHAIN

Supply chain management is one of the most important part of the Enterprise Resource Planning (ERP) architecture present in modern companies. Supply chain management orchestrate the flowing of funds, raw materials, components, and finished products, as they move from suppliers, to manufacturers, to wholesalers, to retailers, to consumers. Those flows can occur both within one company, or among several companies. As term, conditions, assets and participants change over time, the supply chain models need to reflect those changes in almost real time, and alignment mechanisms need to be synchronized along the whole chain.

For instance, good supply chain management will keep product quality consistent, and prevent either understocking or overstocking of inventory. Stocking the right amount of inventory over time is also known as *supply demand synchronization* and represents one of the key components in a just-in-time lean manufacturing and distribution implementation. In other words, companies plan to ensure that products are available when needed, but overstocking inventory is most of the time a costly option. Companies that overstock perishable goods are obliged to discard items that pass the expiration date. And in the case of excess inventory of non-perishable goods, the capital used for those goods are blocked in this inventory posts and cannot be used for other purposes until the stock is released. An additional risk is represented by negative market conditions or price changes, where high level of unnecessary inventories could bring significant additional costs.

And the number of weak points increase when multiple ERP systems need to interface and synch across different organizations. One of the problems is that data doesn't flow very well through the handshakes or interface points between systems with different characteristics and typology. The consequences come in sight during transference of ownership or change in status between two parties. For instance, visibility is limited at the hand-off points of funds, raw materials, components, or finished products.

It must be said that, in some specific cases, this lack of transparency is intentional, as companies don't want to expose their competitive advantages (e.g., an inexpensive supplier who delivers quality products on time). And a company could be cut out of a supply chain if members start transacting directly with that company's suppliers.

But the weak points mentioned previously strongly affect the efficiency and the economics of maintaining a modern supply chain management system.

With smart contracts and additional automatic mechanisms, Blockchains implementations provide a powerful set of tools to bring harmony in a fragmented array of proprietary systems in high need to frictionless communicate to each other.

ENHANCED AUDITING

Another aspect where Blockchains brings additional value is in regards of auditing and provenance. Blockchains are used by eliminating the need for a trusted third party to certify raw materials, components, or finished products, as they travel through a supply chain. Every participant, or node, contains a copy of all transactions. And each participant, verify and approve the new transaction entry on the database. This also provides an audit trail for every transaction that has occurred in the system, without the possibility to alter or modify the records saved in the chain.

A change would be validated or rejected by the nodes in the system. Because all participants have a copy of all past transactions in the network, any participant can detect if a product is not as advertised. And Instead of examining raw materials, components, or finished products at several points in the supply chain, a record of the inspection would

be available and bound to the item as it flows through the supply chain. Although a record of the transaction is public and tied to the movement of physical items across the network, details such as the quantity of goods, their price, and the identity of the parties transacting, can be rendered private with the use of dedicated crypto keys.

A Blockchain implementation for supply chain management therefore provide better insight into products as they move through their lifecycle. And large enterprises are not the only parties to benefit from this increased visibility. Consumers gather more transparency and assurance on product origin, quality and authenticity.

ENHANCED PROVENANCE

The record of ownership used as a guide to authenticity, quality or origin is also called provenance. The additional costs involved in traditional provenance records are very high, and therefore, mainly available for very large ticket items, such as works of art, diamonds or in general, high ticket luxury items. With the efficiencies gained from blockchain technology, provenance records can be available for a wider range of goods. This improved information can be particularly useful to aid consumers as they could make much more informed purchasing decisions.

Currently for consumers it is quite difficult to know if a purchased item is an authentic one. And authenticity is important for various reason, not necessarily of the same degree for all the consumers. For instance, some consumers may want to make sure that fair trade and fair labor standards are upheld in the products they purchase. While others would be more interested none of their products have been tested on animals. Others again may be more concerned with the use of harmful chemicals during product manufacturing. Those consumers are willing to pay a premium to make sure that they are not funding operations that are not in line with their values.

And counterfeit products, as we know, take advantage of the higher price point a brand that upholds strict standards can command. Their profits are much higher than the authentic brand since they cut corners during production.

Counterfeit products are one of the top global problem affecting several industries. For example, the European Union Intellectual Property Office (EUIPO), in collaboration with the International Telecommunication Union (ITU), estimates that $48 billion worth of smartphone sales were lost to counterfeit phones in 2015 (Karen Gilchrist, cnbc.com, 2017). Also, "*the Interprofessional Council of Bordeaux Wine estimates that 30,000 bottles of fake imported wine are sold per hour in China*", whereby some estimate half of the wines retailing for more than $35 in China are counterfeit (Pamela Ambler, forbes.com, 2017).

And this problem is way more acute in other industries like the pharmaceutical industry, baby food and critical components for safety systems. Time and again we witnessed dangerous examples like the counterfeit drug Avastin scandal in USA. The Center for Medicines in Public Interest estimated that global counterfeit medicines trade is worth some $75 Billion. In 2008, 6 infants were killed and 54.000 hospitalized for a baby food

scandal in China involving fake baby milk powder. In 2015 more than half million Toyota cars were affected by the discovery of fake brake parts in the supply chain.

To be certain that a product is authentic, it is necessary to have either a record of all the transactions for the life of the item, or a trusted third party. Trusted third parties certify the authenticity or quality of an item but in doing that, they function as a new data layer between data silos, and thus increase costs of transactions by charging for providing data and certifying products.

Blockchains can serve the function of these trusted third parties by uniquely identifying products and certifying their authenticity. Alternatively, these trusted third parties can leverage blockchains by recording their audits and inspections on blockchains. This would reduce the overhead needed to certify products, streamlining costs and saving time in collecting and delivering the related documents. For example, a manufacturer could prove that its sources also abide by the certification authorities' standards if those sources are listed on blockchains as having passed all requirements. And the time stamp of the source's original certification and renewals could be viewed by any interested party.

From a consumer perspective, there is a very attractive advantage with this technology. In reading from a blockchain, a consumer would be able to verify a product's authenticity by seeing the full chain of custody for an item. Dedicated user interfaces and blockchain frameworks allow consumers to view important data attached to the goods, without necessarily viewing exactly who conducted each transfer down the supply chain line. In this way there is a clear means to be assured that the product consumers are purchasing is an authentic product, without necessarily allowing the public to view the single purchasing habits or disclosing additional private information.

IMPLEMENTATION STEPS

In framing a Blockchain use case, it would be wise to start from some general questions on the potential compelling reason to implement such a solution.

- There is a Business Problem to be solved, that cannot be solved by existing or mature technologies.
- There is an identifiable Business Network, with participants, assets and transactions.
- There is a need of Trust, together with Consensus, Immutability, Finality and Provenance.

Being able to gather an initial feedback on those characteristics could greatly help to further explore the business case and added value for a blockchain implementation.

Crafting a custom pilot project would include the below building blocks:

- **Assets** – in digital form or a digital representation of the items to be tracked.
- **Participants** – as examples: manufacturers, sub-system builders, suppliers, customs, logistics, agents, insurers, regulators, banks.
- **Transactions** – asset creation, assembly, modification, ownership change, disposal.
- **Processes** – all additional interactions with existing systems associated with the transactions type above.
- **Access control** – write and read policies for the participants in the network. (Who can do what transaction and who can see the result).

CHALLENGES

Blockchain is an emerging technology and it is important to underline the challenges which characterize the early stage of such an innovation wave.

In regards of technical scaffolding and its implementation, we can see a fragmented landscape, where there are several incompatible protocols, lack of compatibility and lack of strong standardization across industries or use cases. Some open source platforms are gaining momentum and starting to aggregate enough critical mass in forming the beginning of a common fabric. Among others, IBM is leading with the Hyperledger platform, Ethereum foundation with its alliance and r3 with its Corda platform.

There is also a significant lack of technical know-how, best practice examples, use cases references, and knowledgeable developers. A lack of regulatory and legal frameworks bring also uncertainty in key potential segments, such as financial services and smart contracts.

About the technical implementation in an enterprise environment, the following factors still need significant improvements: *performance* (Bitcoin currently can only process 7 transactions per second; *speed* (measured in milliseconds. Bitcoin and Ethereum transactions can take an average of 10 minutes and 12 seconds, respectively, from confirmation to settlement); *scalability* (networks need to be able to adjust immediately,

based on node joining, number of transactions and transaction history to store); safeguards (mechanisms and emergency brakes to intervene in fully automated contract executions or transactions flows).

Finally, there is a need to have successful implementation of large scale use case, in order not only to showcase the significant added value Blockchain may bring, but also to overcome the natural resistance for the legacy infrastructure representatives to change costly existing systems.

CONCLUSIONS

There is great momentum and enthusiasm around Blockchain, and one of the best quote I found is from Babs Rangaiah, IBM iX's executive partner of global marketing. *"You can say that blockchain will do for transactions what the Internet did for communications, which is a huge statement. But this is like 1992 for the internet when we had no idea what was possible and when. We had an idea of what it could do, but not how soon we'd get there. That's where we're at with blockchain."*

The internet took some time to go through all the phases from initial, single use case to wide spread adoption and deep transformation tool. But it is undeniable that today, that foundation technology touch or is at the core of much of the business and the way we live and interact with each other.

Blockchain could represent such a disruptive technology wave. As the internet has been the foundation for the digital on-line age, so Blockchain could be the foundation of the trusted transaction age, where each single business or individual could interact with each other in a secure way without the need of intermediaries. Where assets, data and identities can be secured and verified by everybody. Where the Internet of Things could become the Network of Intelligence, with each node automatic exchange and execute actions with a trusted and tamper proof communication highway.

Author: Fulvio Famularo

München, 2018

Further reading

- "The Truth About Blockchain", Marco Iansiti and Karim R. Lakhani, HBR January-February 2017 issue.
- "The Blockchain Will Do to the Financial System What the Internet Did to Media", Joichi Ito, Neha Narula, and Robleh Ali, , HBR March 2017
- "Blockchain for Dummies, IBM Limited Edition", Manav Gupta, Wiley Inc., 2017
- "Survey on Blockchain Technologies and Related Services", Nomura Research Institute, March 2016
- "The future of financial infrastructure", World Economic Forum, August 2016
- "Realizing the Potential of Blockchain", World Economic Forum, June 2017
- "Global Blockchain Benchmarking Study", Dr Garrick Hileman & Michel Rauchs, Cambridge Center for Alternative Finance, 2017
- "Blockchain, cryptography and consensus ", Christian Cachin, IBM Research, ITU Workshop on „Security Aspects of Blockchain ", Geneva, Switzerland, 21 March 2017
- „A Gentle Introduction to Blockchain Technology ", Antony Lewis, Bits on Blocks, 9 September 2015
- „So you want to use a blockchain for that?", Antony Lewis, Bits On Blocks, 18 July 2016
- „ Confused by blockchains? Revolution vs Evolution", Antony Lewis, Bits on Blocks, 9 May 2016
- „No, "Blockchain" is not a solution looking for a problem ", Antony Lewis, Bits on Blocks, 17 June 2016
- „A gentle introduction to immutability of blockchains ", Antony Lewis, Bits on Blocks, 29 February 2016
- „Banking on Blockchain ", Finextra and IBM, January 2016
- „Building the trust engine ", Alex Batlin, Hyder Jaffrey, Christopher Murphy, Andreas Przewloka and Shane Williams, UBS 2016
- "Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008
- "Blockchain Basics. A Non-Technical Introduction in 25 Steps", Daniel Drescher, Apress 2017
- "Encyclopedia of Cryptography and Security", edited by Henk C.A. van Tilborg, Springer 2005
- "Understanding Cryptography", Christof Paar, Jan Pelzl, Springer 2010
- "Introduction to Modern Cryptography", Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC, 2008
- "Crypto 101", Laurens Van Houtven, 2013-2017
- "Blockchains in 2016: status quo and scaling challenges", JP Aumasson, Kudelski Security. Philipp Jovanovic, Decentralized and Distributed Systems Lab, EPFL, 2016

Disclaimer

This document has been prepared by Fulvio Famularo at nBloc GmbH.

This document is for distribution only as may be permitted by law. It is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial instruments or to participate in any trading strategy. No representation or warranty, either expressed or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document ('the Information'), except with respect to Information concerning nBloc.

nBloc does not undertake to update or keep current the Information. Any opinions expressed in this document may change without notice and may differ or be contrary to opinions expressed by other parties in nBloc. Any statements contained in this report attributed to a third party represent nBloc's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

nBloc specifically prohibits the redistribution of this document in whole or in part without the written permission of nBloc and nBloc accepts no liability whatsoever for the actions of third parties in this respect. Images may depict objects or elements that are protected by third party copyright, trademarks and other intellectual property rights. All rights reserved.