

BETWEEN BLOCKS AND CHAINS

a way to a more efficient and sustainable trade

Prepared for: Virginia Cram Martos, Markus Pikart

Prepared by: Gianguglielmo Calvi

Last revision: 3 August 2016

Version: 1.0

Revision: 2



What is Blockchain?

In its broader and more encompassing form **blockchain** can be defined as a **technology to develop trusted processes and data transactions on an open and distributed network via decentralized consensus among computer systems.**

In its more common, widely used form "a **blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.**" [1]

"A distributed network (Fig 1 - C) is a type of computer network that is spread over different networks. This provides a single data communication network, which can be managed jointly or separately by each network. Besides shared communication within the network, a distributed network often also distributes processing" [2]

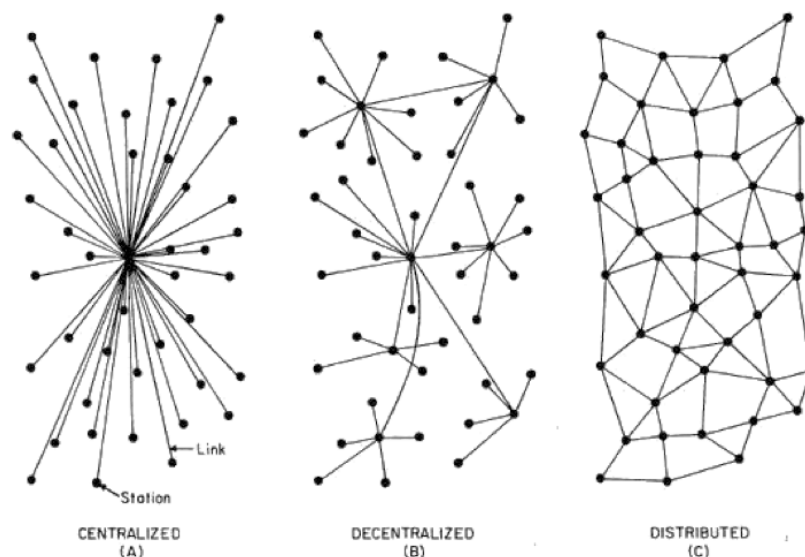


Fig 1. Network types

In a distributed network the responsibilities for data transactions and computations do not collapse on any specific node, on the contrary they are spread across the network, which is responsible as a whole for the results of a given process. Like in some biological eco systems, such as an ant community, where the construction of an ants'

nest is the result of independent and trusted contributions by each ant (i.e. Stigmergy), blockchain technology guarantees that the overall behaviour of the distributed network, programmed to execute a certain process, is trustworthy.

In centralized and decentralized network scenarios, there are always nodes which retain data or functions uniquely, becoming the only points of validation or manipulation for the information they own. These topologies make the implementation of processes that are naturally distributed in the real world (example: the exchange of a currency) more complex and difficult to adapt to continuous changes; moreover, they oblige the owner of such nodes to put in place complex data retention, data availability and information management policies to guarantee the necessary trust in their function.

In such context, blockchain tries to answer to the complexity of the contemporary real world scenarios by offering a technology and a methodology to design distributed applications that operate with private data in an openly verifiable way.

How does it work?

In order to fully understand how blockchain and its applications work it is important to introduce five key building "blocks" that characterize the technology:

- 1. decentralized consensus (also emergent consensus):** is a mechanism to determine if an operation in the distributed network is trustworthy:
"...consensus is not achieved explicitly — there is no election or fixed moment when consensus occurs. Instead, consensus is an emergent artefact of the asynchronous interaction of thousands of independent nodes, all following simple rules. " **[4]**
- 2. the blockchain:** is the data structure, a very long list of blocks¹, in which data are stored across the network. Blocks are created by a physical device (i.e. computer system) that identifies them in a unique way in the network by generating a unique hash number, function of all the previous hashes in the existing blocks of the chain. The owner of the block is the owner of the private data (nobody else can access them) and the owner of the key to share a public version of those data in the network. "It's a bit like your home address. You can

¹ a small data structure with a private and public part.

publish your home address publicly, but that doesn't give any information about what your home looks like on the inside. You'll need your private key to enter your private home, and since you have claimed that address as yours, no one else can claim the same address as theirs." [3]

3. **the smart contracts:** are programs, short, embedding the regulatory aspects of the network. "The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker, or gatekeeper." [3]
4. **trustless transactions:** are transactions without the need for a trusted third party. Peer to peer applications implement the simplest form of trustless transaction in a distributed network.
5. **the proof of work (also proof of stake):** "at the heart of a blockchain's operations is the key concept of "[proof-of-work](#)," an integral part of Satoshi Nakamoto's original vision for the blockchain's role as the unequivocal authenticator of transactions. The "proof of work" is a "right" to participate in the blockchainsystem. It is manifested as a "big enough hurdle" that prevents users from changing records on the blockchain without re-doing the proof of work." [3]. Proof-of-work(s) are extremely computational demanding algorithms for reaching consensus in the blockchain.

Those mechanisms, combined together, offer an information exchange environment that **guarantee privacy for the sensitive data** of each actor, **redundancy** of data, **consistency and transparency of the transactions** initiated by any party in the network, **isolation of misbehaving** nodes, **scalability** to theoretically infinite nodes, **extremely high tampering tolerance** [6]. All these characteristics are at the core of transactions, in scenarios where the information exchanged between parties of a network is of financial nature or is associated with assets or goods in the real world. That is why the blockchain technology could be so disruptive to the way international trade operates.

How Blockchain will transform International Trade

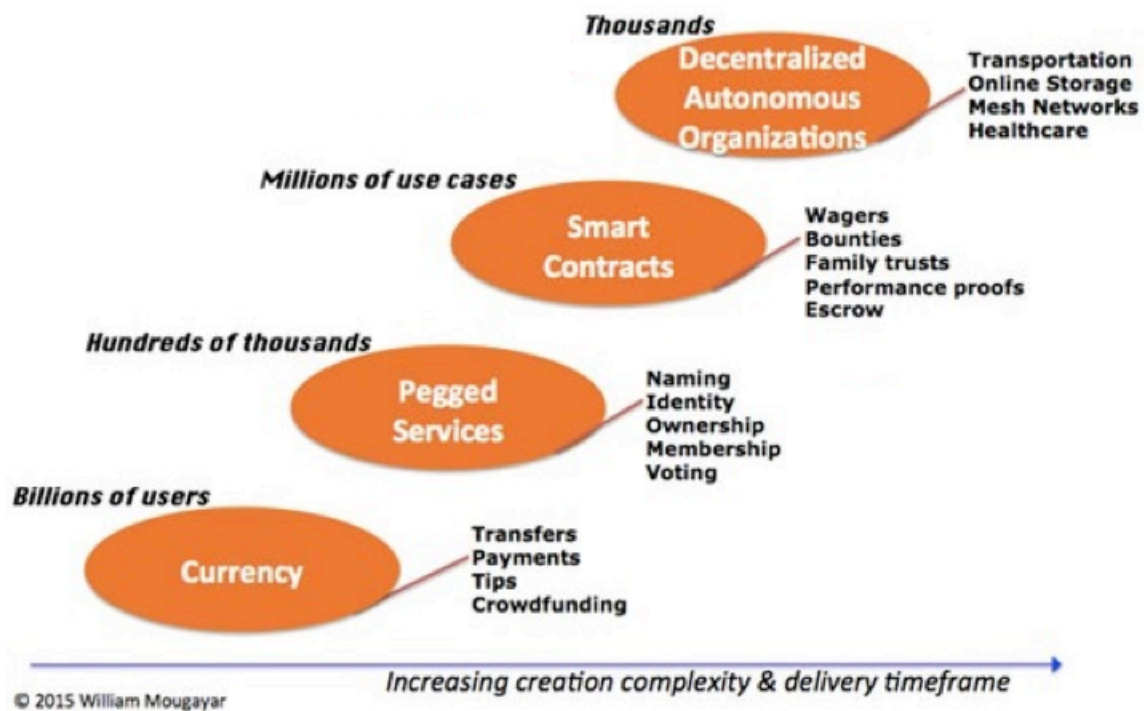


Fig 2. blockchain current and future applications

A distributed transactions system based on **blockchain technology naturally implements a ledger**². This concept is at the core of the regulatory activities carried on by a wide range of authorities, institutions and businesses (i.e. land registry, chart of accounting tables, banks, insurance companies, car license authorities, ...). A more transparent, trusted and globally recognised accounting mechanism of this kind can dramatically facilitate and harmonise processes not only in e-Business but also in broader trade scenarios.

² a ledger is the principal book or computer file for recording and totaling economic transactions measured in terms of a monetary unit of account by account type, with debits and credits in separate columns and a beginning monetary balance and ending monetary balance for each account.

In this context, the only globally used and proven solid application of blockchain technology, **Bitcoin**³, has shown that the ledger works. The positive results of this only service have been so convincing to generate a worldwide consensus about the future developments of the blockchain and its impact in the technological landscape of this century:

“We stand at the edge of a new digital revolution. The Internet is beginning a new phase of decentralization. After over twenty years of scientific research, there have been dramatic advances in the fields of cryptography and decentralized computer networks, resulting in the emergence of a profound new technology—known as the blockchain— which has the potential to fundamentally shift the way in which society operates.” [7]

A certain amount of progressively sophisticated scenarios are expected to involve this technology in the upcoming future (Fig 2) and among them various will try to cope with international trade and supply chains problems.

- "blockchain-based solutions to both physical and financial supply chain issues are being proposed by a number of startups." - <http://www.nasdaq.com/article/how-blockchain-technology-is-reinventing-global-trade-efficiency-cm626503#ixzz4Fh4Jugej>
- "The Hyperledger Project is a collaborative effort created to advance blockchain technology by identifying and addressing important features for a cross-industry open standard for distributed ledgers that can transform the way business transactions are conducted globally" - <https://www.hyperledger.org/>
- "Oris Valiente's group – founded in 2015 and officially known as Rubix by Deloitte – is positioning itself to help build out the business applications that would underpin blockchain-based supply chains" - <https://godistributed.com/ledger/32/> and <http://rubixbydeloitte.com/>
- "Coming to international trade, blockchain could help to ensure that shipping transactions are auditable; chains of custody of goods can be verified; transportation records cannot be altered and malicious entities cannot dispute the authenticity of records." - <http://www.econotimes.com/blockchain->

³ there are other services based on Blockchain but none of them has yet the numbers - users and transactions - to be considered a global proof of concept.

[Technology-To-Transform-International-Trade-137855](#) and <https://www.blocknotary.com/>

Solutions capable to embrace different combinations of the above scenarios to deal with them as a single blockchain eco-system are already present and well established:

- **Ethereum:** "... is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference." - <https://www.ethereum.org/>
- **Decentralized Autonomous Organization ("DAO"):** "... is a new breed of human organization never before attempted. The DAO is borne from immutable, unstoppable, and irrefutable computer code, operated entirely by its members, and fueled using ETH which Creates DAO tokens" - <https://daohub.org/about.html>

In conclusion, even if at the current stage of development the blockchain hasn't served directly the purpose of trade facilitation it is already clear in which way its contribution, in the next decade, will be substantial. These positive expectations shouldn't prevent us to evaluate the limitations that could be introduced by embracing an international trade approach fully enabled by blockchain, as for example in the context of legally binding agreements among traders:

"Smart contracts may facilitate the execution of complex agreements with greater clarity, they also present a series of new challenges. They implement, by default, a zero-tolerance policy where parties have no choice but to execute the contract. In the current legal framework, the law establishes a series of rules that people must abide to. Nevertheless, everyone is free to infringe these rules (at the risk of being held liable for damages) because legal enforcement takes place ex post, after the act. As opposed to traditional contracts, where parties can decide whether or not to fulfil their obligations, smart contract cannot be breached. Once the contracting parties have agreed to be bound by a particular clause, the smart contract's code immutably binds them to that clause without leaving them the possibility of a breach." [7]

References

- [1] [blockchain technology - Beyond Bitcoin](#)
- [2] <https://www.techopedia.com/definition/27788/distributed-network>
- [3] [BlockChains - Why Block and Why Chains?](#)
- [4] http://chimera.labs.oreilly.com/books/1234000001802/ch08.html#_decentralized_consensus
- [5] <https://godistributed.com/ledger/26/>
- [6] <http://research.microsoft.com/en-us/um/people/venkie/jakubowski09tts.pdf>
- [7] [DECENTRALIZED BLOCKCHAIN TECHNOLOGY AND THE RISE OF LEX CRYPTOGRAPHIA](#)