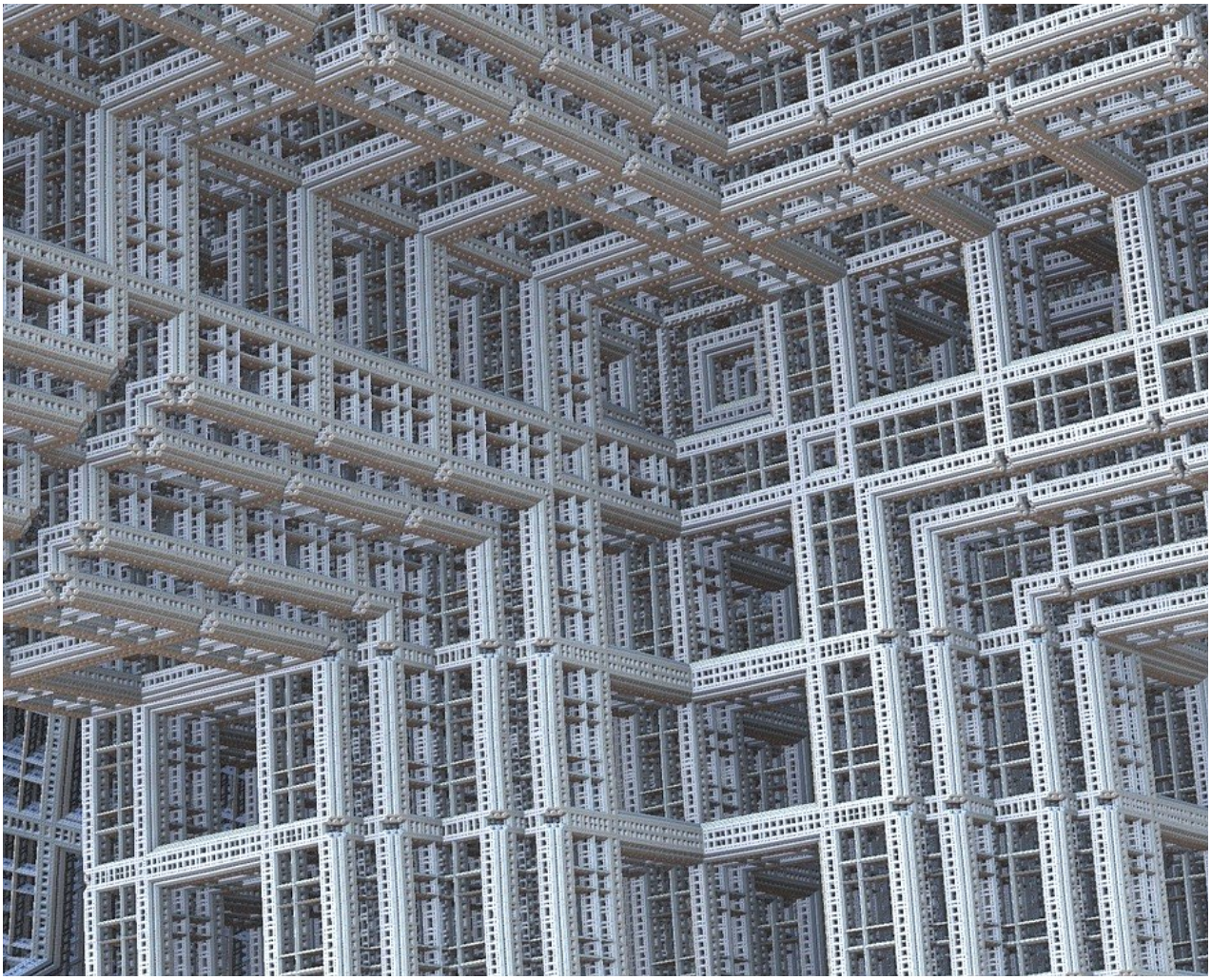
UNECE



BETWEEN BLOCKS AND CHAINS

a way to more efficient and sustainable trade

Prepared for: Virginia Cram-Martos, Markus Pikart

Prepared by: Gianguglielmo Calvi

Last revision: 25 September 2016

Version: 1.0

Revision: 3

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]**

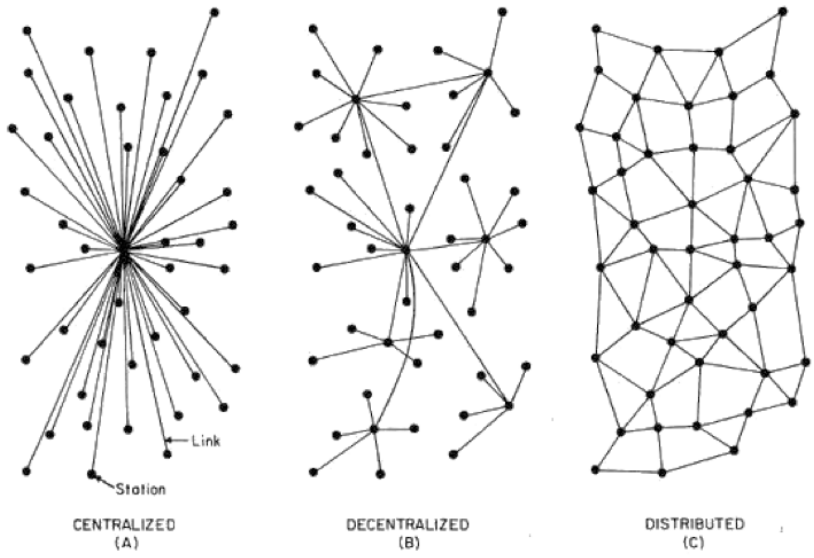


Fig 1. Network types

In a distributed network the responsibilities for data transactions and computations are not given to 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 contributions by each ant (i.e. Stigmergy[1]), 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 unique data or functions, 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 this context, blockchain tries to respond to the complexity of contemporary real world scenarios by offering a technology and a methodology for designing 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 blocks[2], in which data are stored across the network. Blocks are created by a physical device (i.e. a 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

[1] Stigmergy is a mechanism of indirect coordination, through the environment, between agents or actions. The principle is that the trace left in the environment by an action stimulates the performance of a next action, by the same or a different agent. The concept of stigmergy was introduced by Pierre-Paul Grasse in the 1950's to describe the indirect communication taking place among individuals in social insect societies.

[2] a small data structure with a private and public part.

existing blocks of the chain. The owner of the block is the owner of the private data (no one else can access them) and the owner of the key to share a public version of these data in the network. "It's a bit like your home address. You can 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 small programs embedding rules which govern the network. "The basic idea behind smart contracts is that a transaction's contractual governance[3] 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. **Proof of work (also proof of stake)**: "at the heart of a blockchain's operations is the key concept of proof-of-work". In order for a miner[4] to actually enter his block of transactions into the blockchain he will have to provide an answer, or a proof, to a specific challenge. This proof is difficult to produce (for example: generate an extremely large hash number out of some predefined values) but is very easy to validate by the network. A proof-of-work system can be compared to altruistic ethologic systems, where stronger individuals reinforce the trust that others have in them by taking care of the weaker individuals. For data "miners", the ability to generate blocks is a show of computational strength, which is just what a blockchain network needs to help verify all its transactions. At the same time, it is also a show of community spirit because by agreeing to follow the "rules" for generating the next block, they show themselves to be willing to respect the interests of the community rather than manipulate the block chain for self-interested purposes.

---

[3] "the use of a formalized, legally-binding agreement or a contract to govern the interfirm partnership" - more info

[4] an entity/program associated with a physical device that can read/write onto the Blockchain.

Those mechanisms, combined together, offer an information exchange environment that **guarantees: 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 in a network is of a financial nature or is associated with assets or goods in the real world. That is why, as also highlighted by Mr Vivek Ramachandran, global head of product and propositions for global trade and receivables finance at HSBC, the blockchain technology could be so disruptive to the way international trade operates:

"Over $2 trillion of trade today depends on the physical exchange of documents…"

"What we've shown is blockchain has the potential to take away paper, which could be completely revolutionary if commercialised."

"(Blockchain) makes the system much more efficient,"

"It's expensive to adopt it, but the upside is huge."

How Blockchain will transform International Trade

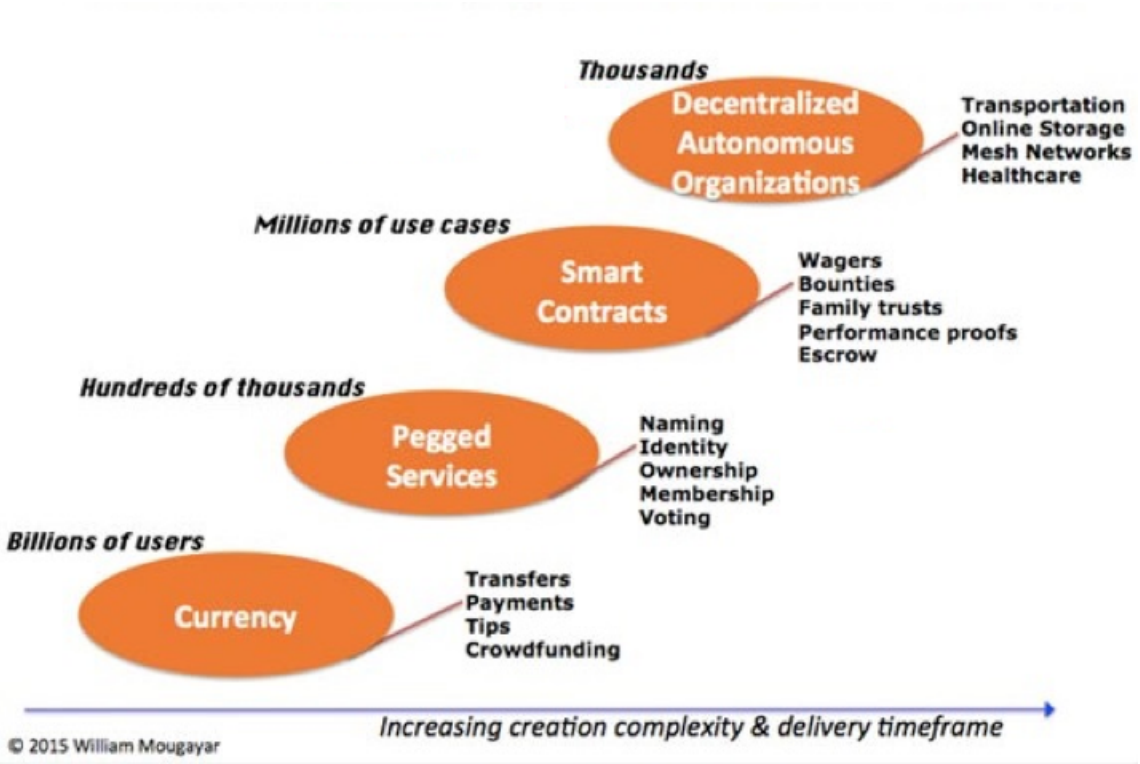


Fig 2. blockchain current and future applications

A distributed transactions system based on **blockchain technology by its nature implements a ledger**[5]. This concept is at the core of the regulatory activities carried out by a wide range of authorities, institutions and businesses (i.e. chart of accounting tables, banks, insurance companies, car license authorities, …). A more transparent, trusted and globally recognised accounting mechanism of this kind could dramatically facilitate and harmonise processes not only in e-Business but also in broader trade scenarios.

[5] 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**[6], has shown that the ledger works. The positive results of this only service have been so convincing that they have generated a worldwide consensus about the potential of blockchain technology 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]**

At least five[7], but potentially many more, progressively sophisticated scenarios are expected to involve this technology in the near future (Fig 2) and among them will be various efforts to resolve international-trade and supply-chain 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 develop 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-

[6] 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.

[7] Decentralized Internet of Things, Keyless Signature, Legal Proof of Existence or Proof of Possession, Security Trade Settlement, Anti-Counterfeiting **[8]**

Technology-To-Transform-International-Trade-137855 and https://www.blocknotary.com/

Solutions capable of embracing different combinations of the above scenarios and dealing 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 Ethers (ETH - the token system of Ethereum) which Creates DAO tokens" - https://daohub.org/about.html
- **The EdgeVerve Blockchain Framework for Financial Services**: "… is a permissioned ledger that allows banks to rapidly deploy blockchain-based services for varied business areas." - https://www.edgeverve.com/finacle/solutions/Pages/blockchain-framework-financial-services.aspx

Last but not least, some government offices, like the UK Government Office for Science, seem very much committed in recommending to look after this technology (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf) :

"We recommend that government should provide ministerial leadership to ensure that government provides the vision, leadership and the platform for distributed ledger technology within government. Specifically, the Government Data Service should lead work in government as a user of distributed ledgers and the DCMS Digital Economy Unit should lead work on government as an enabler of distributed ledgers "

The Core Component Library as a semantic for Blockchain blocks

Information carried in blocks has been so far limited to data values fitting predefined data structures which serve the purpose of a specific blockchain database implementations (example: Bitcoin). It is important to highlight that this simplification isn't inherent to blockchain technology, which has the potential to carry arbitrary, complex data patterns and even programs (see Ethereum efforts). Research to empower the semantic expressiveness of data in a block are already underway **[9].** In addition, visions, such has the one proposed by IBM of a universal

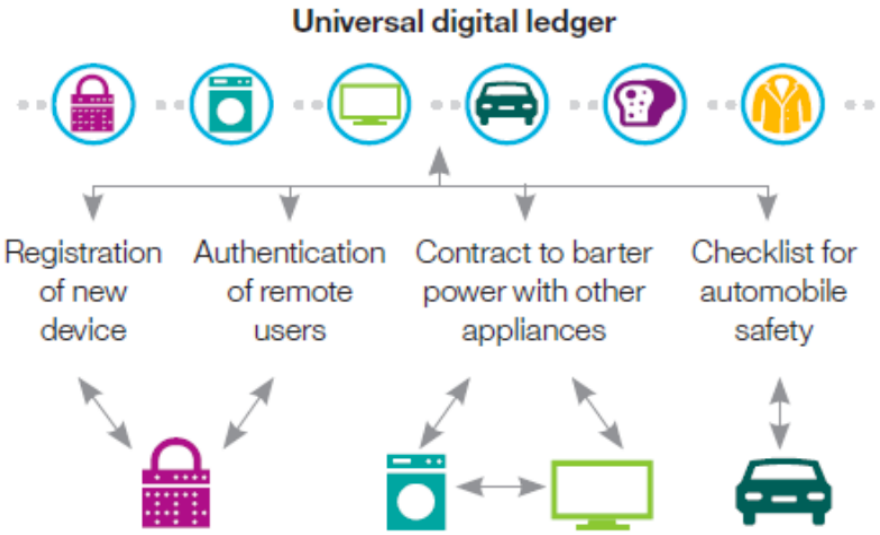


Fig 3. IBM Universal Digital Ledger via Blockchain

digital ledger (Fig 3), force potential users to consider which kind of semantic descriptions are necessary to cover the business aspects of their desired implementations.

At this level the UN/CEFACT Core Component Library could surely position itself as a general purpose business semantic library that can guarantee consistency and interoperability of those business processes implemented within a blockchain network.

What’s ahead?

Even if, at the current stage of development, blockchain technology hasn’t served directly the purpose of trade facilitation it is already clear that, in the next decade, its contribution could be substantial. These positive expectations shouldn’t prevent us from also evaluating the limitations of an international trade approach enabled by blockchain technology. 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 contracts 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]**

Conclusions

The role of UN/CEFACT, as a semantic hub[8] in the design of syntax neutral business processes, is extremely strategic for supporting the development of standards capable to take fully advantage of the disruptive characteristics of blockchain (i.e. privacy for the sensitive data, high tampering tolerance, consistency and transparency of transactions, …). A foreseeable scenario has some UN/CEFACT business standards, each coupled with a specific blockchain implementation guideline, implementing viable solutions to complex business processes, otherwise extremely difficult to address. In the following non-exhaustive matrix, we try to highlight some of these possible integrations leaving the investigation of all the details to future researches on this subject.

UN/CEFACT Standards / Blockchain Matrix (example)

	Blockchain (ledger)	**Blockchain (smart contracts)**
UN/CCL	BIE (Business Information Entities) in CCL could be linked, in a uniquely identifiable fashion, to a block of a distributed ledger. In this way each block generated in the chain could be used as a piece of a business transaction until a certain “reset” operation would make the network start again.	Blocks of a blockchain could carry information on how to agree about the content of certain BIE or ABIE involved in a business transaction. The way the agreement is reached would be syntax neutral as long as UN/CCL can be referenced to provide a common semantic ground.

[8] As stated in the UN/CEFACT Prospective Directions ECE/TRADE/C/CEFACT/2016/20 document

UN/EDIFACT	A distributed ledger could carry information associated with the status resulting from UN/EDIFACT message exchanges. This can be monitored by parties in the ledger that need to asses those statues to trigger business actions (ex: the emission of a e-invoice).	An entire UN/EDIFACT message exchange among two parties could be the result of creating multiple blocks under a certain agreed sequence in the blockchain. Other parties will be able to verify that the exchange has happened correctly or not by simply accessing the public information in the chain.

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] https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf

[8] https://vcoin-project.github.io/social/school/use-case-ideas/5-industry-scenarios.html

[9] http://cscubs.cs.uni-bonn.de/2016/proceedings/paper-10.pdf