Blockchain technology in financial institutions[1]

Sander van Loosbroek, Director Distributed Ledger Technologies, Cegeka

Blockchain is a shared, distributed ledger that is secured by cryptography. Computers in a network, called nodes, process and store transactions. A blockchain network can span the globe and predictably reconcile transactions. It is very secure because all transactions are appended to the ledger and cryptographically chained. If you want to change 1 transaction you'll have to rewrite history. It is built on proven technologies that we use today for securing our websites.

The internet was designed to copy data reliably between nodes. Transferring data from party X to party Y was not possible in the internet without a third partie to confirm the transfers of data that respresented some form of ownership or IOU. There are generally two types of blockchain: public (open) and private (closed). The generalized features of both can be summarized as follows:

- Public blockchains facilitate open read access and write access by a consensus mechanism, which is at the moment proof-of-work and proof-of-stake, has a identity which is anonymous or pseudonymous and usually requires a native asset.
- Private blockchains has a permissioned read and or write access, is faster, is secured for pre-approved participants, works only with known identities and does not require a native asset.

[1] Report written by Frank Lierman, based on the speech given by mister Sander van Loosbroek, Director Cegeka Distributed Ledger Technologies, for the Belgian Financial Forum in Antwerp November 6, 2017.

But there are many more variations of blockchain applications:

#	Item	Bitcoin	Ethereum	Fabric V0.6	Corda
0	Purpose	Censorship resistant digital cash payment	Execute smart contract on a distributed network	Design for variety of use cases in business	Enterprise grade platform for financial transaction
1	Data sharing model	Broadcast	Broadcast	Broadcast (Encrypted)	"Need-to-know" basis
2	Transaction validation	Proof of Work	Proof of Work	PBFT	Validated by parties to the transaction
3	Consensus	Proof of Work	Proof of Work	PBFT	Uniqueness service provided
4	Transaction Style	UTXO model	Account base	Blockchain + Key value store	UTXO model
5	Regulatory requirement	No	No	No	Enable regulatory nodes
6	Scripting language	Python, LLL	Solidity	Go	Kotlin, Java
7	Crypto currency	Yes	Yes	No	No
8	Participation	Anyone	Anyone	Permissioned network	Permissioned network
9	Smart contracts	Limited, deterministic	Turing-complete	Turing-complete	Turing-complete
10	Virtual machine	Native code	Ethereum virtual machine	Native code	The Java virtual machine
11	Legal prose	"Code is law"	"Code is law"	Legal Documents can be referenced	Legal Documents can be referenced
12	Finality	No	No	Yes	Yes

Blockchain is a hot topic. It receives a lot of attention in recent years. Already in November 2015 the Bank of International Settlements launched an CPMi working Group to undertake an analysis of the crypto-currencies. The emergence of distributed ledger technology could present a hypothetical challenge to central banks, not by replacing a central bank with some other kind of central body but mainly because it reduces the functions for a central body and, in an extreme case, may obviate the need for a central body entirely for certain functions.

In February 2017 the BIS stated that the developments to date suggest that DLT bears promise but that there is still a long way to go before that promise may be fully realized. DLT provides analytical framework with key questions for further exploration and analysis. And in September 2017 the BIS wrote: as it stands, cash is the only means by which the public can hold central bank money... A Central Bank Crypto Currency (CBCC) would allow consumers to hold central bank liabilities in digital form. But this would also be possible if the public were allowed to have central bank accounts, an idea that has been around for a long time. We argue that the main benefit that a consumer facing retail CBCC would offer, over the provision of public access to central bank accounts, is that the former would have the potential to provide the anonymity of cash peer-to-peer transfers allow anonymity vis-a-vis any third party. If third party anonymity is not of sufficient importance to the public, then many of the alleged benefits of retail CBCCs can be achieved by giving broad access to accounts at the central bank.

BANK FOR INTERNATIONAL SETTLEMENTS

February 2017

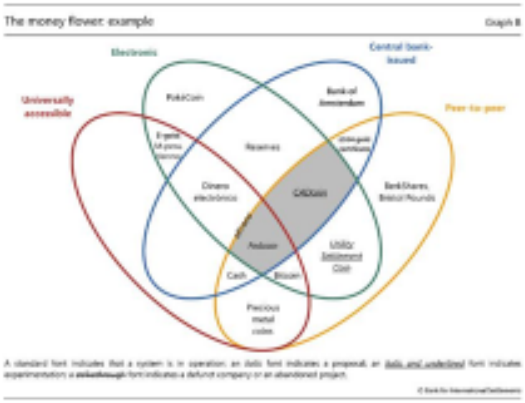
- Developments to date suggest that DLT bears promise but that there is still a long way to go before that promise may be fully realized
- **Provides Analytical Framework with Key Questions** for further exploration and analysis

https://www.bis.org/cpmi/publ/d157.pdf cegeka

BANK FOR INTERNATIONAL SETTLEMENTS

September 2017

- As it stands, cash is the only means by which the public can hold central bank money ... A CBCC would allow consumers to hold central bank liabilities in digital form. But this would also be possible if the public were allowed to have central bank accounts, an idea that has been around for a long time. We argue that the main benefit that a consumer-facing retail CBCC would offer, over the provision of public access to (centralised) central bank accounts, is that the former would have the **potential to provide the anonymity of cash**. In particular, peer-to-peer transfers allow anonymity vis-à-vis any third party. If third-party anonymity is not of sufficient importance to the public, then **many of the alleged benefits of retail CBCCs can be achieved by giving broad access to accounts at the central bank.**

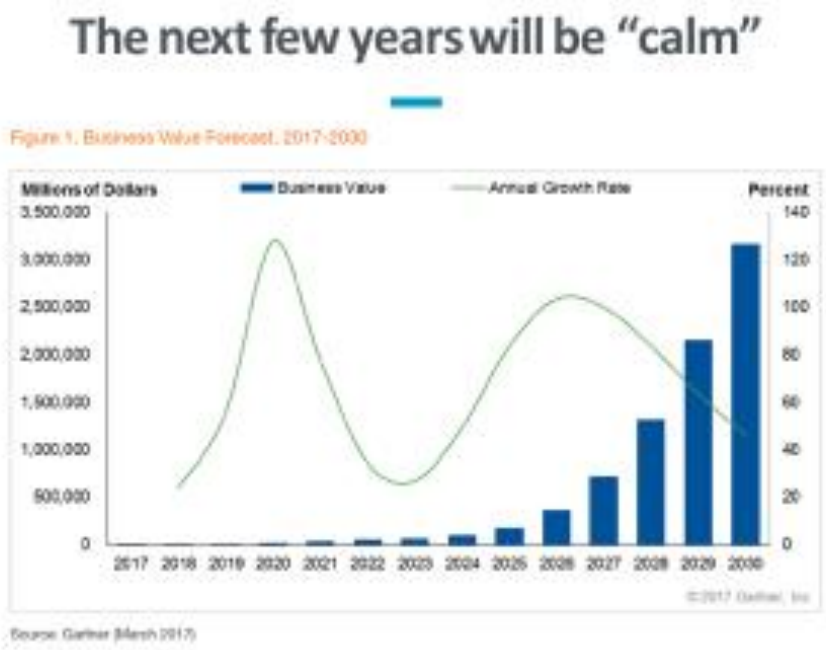


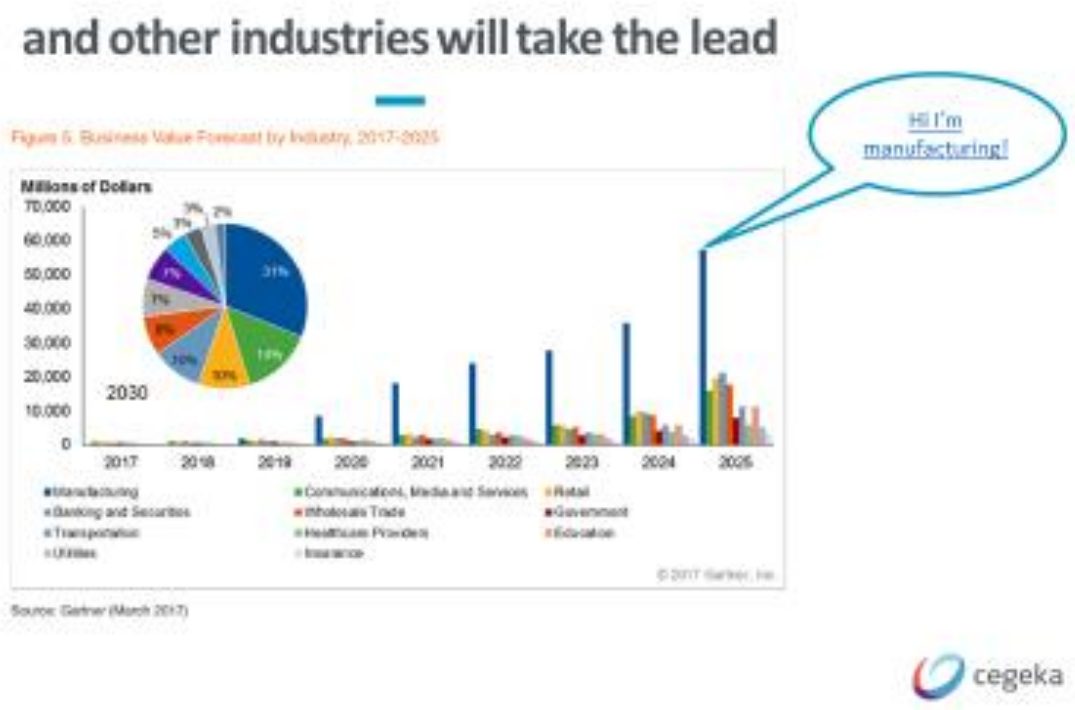
https://www.bis.org/publ/qtrpdf/r_qt1709f.htm cegeka

Meanwhile central banks in different countries are moving forward with test, such as those of India, Singapore, England, Papua New Guinea. But some tests appear to fall short as it is the case for the those of the ECB and the Bank of Japan.

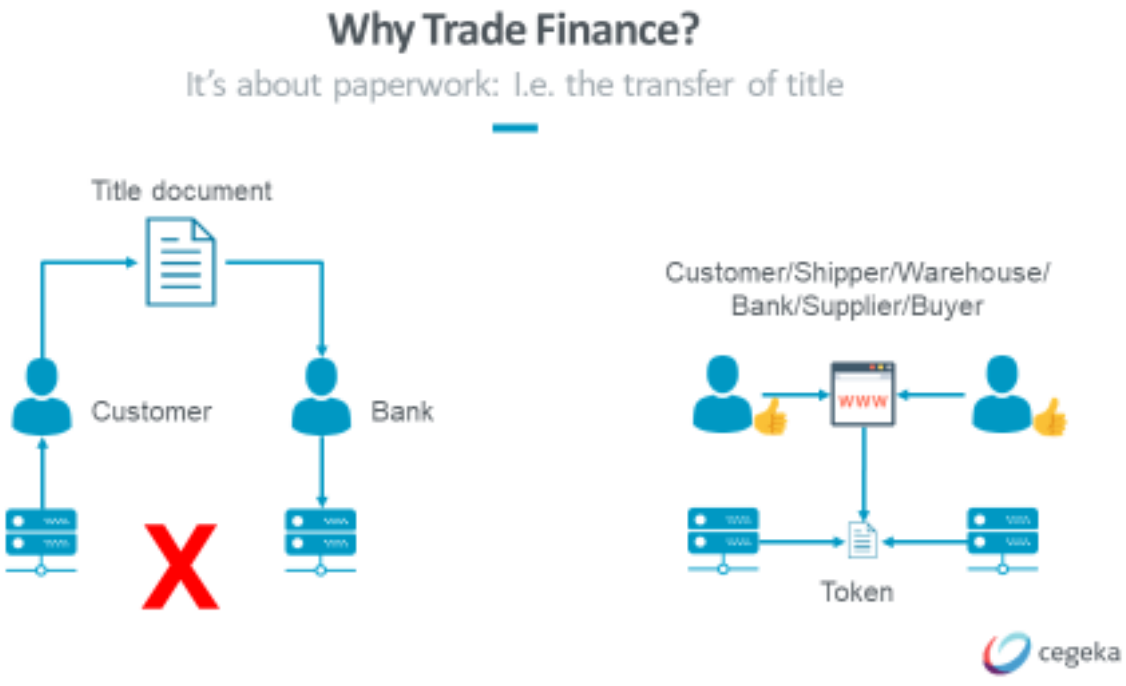
Nevertheless, the first solutions begin to emerge. Mastercard launched an open-up access to blockchain API for partner banks and merchants. The company tested and validated its blockchain and will initially implement the technology in the business to business space to address challenges of speed, transparency and costs in cross-border payments. ILM is doing it with Stellar, R3 with Corda and 22 banks, Ripple is offering for the last 3 years and fintechs like Cashaa were doing with Bitcoin.

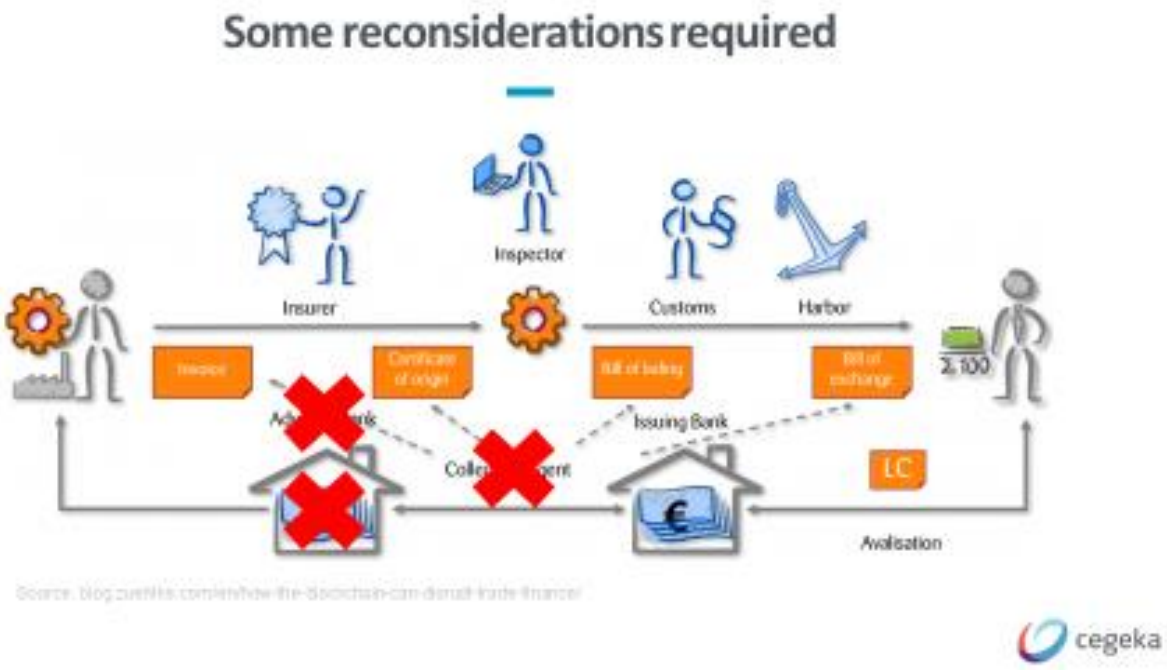
It is possible that the next few years will be calm and other industries will take the lead.





Banks are now most focussing on clearing and settlement, payments, trade finance, identity and syndicated loans.

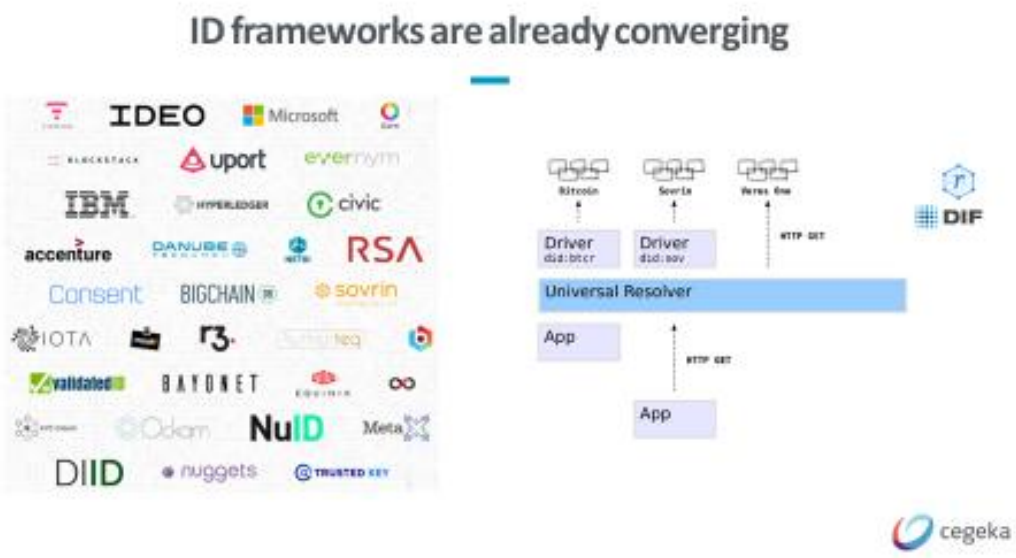


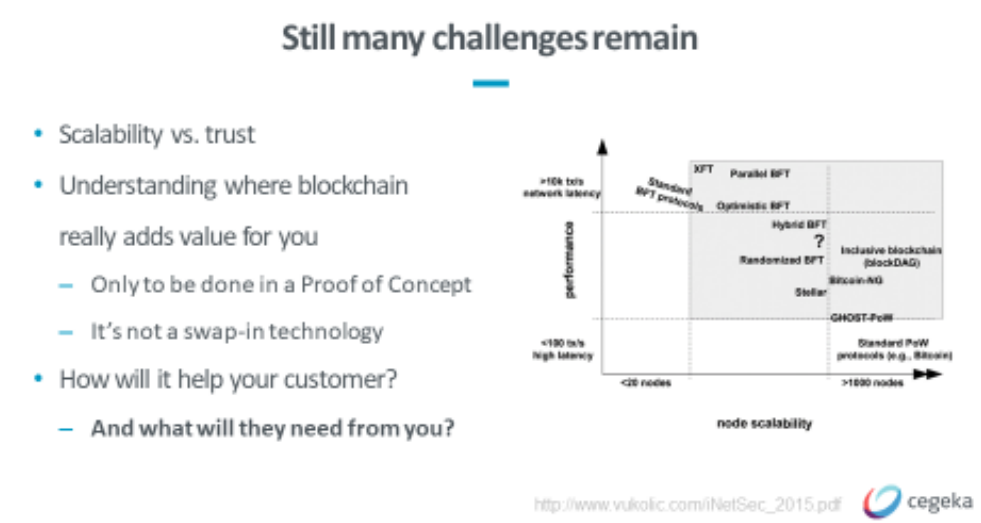


On the topic of Trade Finance there's already a lot going on today: Digital Trade Chain Consortium launched "we.trade", banks team up with IBM in trade finance blockchain, Amsterdam Trade Bank uses blockchain for commodity trade finance, Maersk unveils first industry-wide cross –border supply chain solution, ING and R3 make trade finance easier, commodity traders, energy majors and banks join forces to create a blockchain based digital platform for the energy commodity trading industry.

There is also a lot of traction on the topic of identity. Banks have been trying for years to set up a shared digital utility to record customers' identities and keep them updated. They have failed to find the right formula, undone by conflicting demands and the problem of deciding liability. Some believe that blockchain could offer a solution because of its cryptographic protection and its ability to share a constantly updated record with many parties. It is applicable for KYC (Know your customer), AML, WwFT. It is crucial to understand who is attempting what and exchange your findings with your financial peers will reduce fraud. Verifying an ID is essential for any online solution. Following figure illustrates that ID frameworks are already converging. Nevertheless, there are still many remaining challenges: scalability versus trust, understanding where blockchain really adds value which in sonly possible via a proof of concept because it is not a swap in technology. Other questions are: how will it help your customer? And what will they need from you?

But also, distractions lie ahead: the public Ethereum blockchain presents itself a global stock exchange. Now you need ETH to invest, soon Z-Cash, which is even more anonymous. Every start-up is doing an ICO, which is an unregulated anonymous IPO.





The main take-aways are:

- This technology is here to stay, but you will need to experiment with it to understand where and if it can add any value;
- New business models will merge over time, possibly threaten core revenue streams from banks;
- Most of all this technology will enable your clients to benefit, make sure you're ready to support them.