Blockchain

From hype to realistic expectations

Ir. Hardwin Spenkelink and Gys Hough

In 2016 we have seen blockchain (distributed ledgers) going mainstream with more and more corporations and governments around the world running various experiments. Distributed ledgers are used to describe a wide array of solutions that are implemented to help optimize transactions and business processes across value chains. In this article we will discuss the basics of blockchain as well as the distinction between different types of blockchain. We will describe the most prominent pros and cons of the two main types of distributed ledgers and provide the reader with guidance to help assess whether a distributed ledger solution can deliver benefits in a specific use case.

Ir. H. Spenkelink
is senior consultant at KPMG IT Advisory.
spenkelink.hardwin@kpmg.nl

G. Hough
is senior consultant at KPMG IT Advisory.
hough.gys@kpmg.nl

Blockchain hype and the reason behind it

Corporations and governments all over the world are talking about blockchain and every respectable bank seems to be in a blockchain consortium. This culminated in Gartner calling 2016 the year of blockchain hype. It declared that blockchain was at the peak of its famous hype cycle and is suffering from 'inflated expectations' (see Figure 1). Interestingly though this does not mean that Gartner dismisses the potential of blockchain, on the contrary:

'As a portent for the rise of the programmable economy, the potential of this technology to radically transform economic interactions should raise critical questions for society, governments and enterprises, for which there are no clear answers today.' ([GART16])

This begs the question of why blockchain is seen as such a transformative technology with different applications across different industries. The answer to this question lies in the automation of trust which is achieved by means of digital scarcity.

What is blockchain?

Distributed ledgers are challenging to understand on an intuitive basis because it is in actual fact a collective term for five complimentary technologies. The most essential being cryptography (1) and specifically three types namely private and public key pairs, hash algorithms and Merkle trees. This cryptography is used to achieve consensus (2) between nodes (often referred to as miners) that interact with each other over a peer to peer network (3). The end result being a decentralized ledger (4) that runs on auditable open source code (5). This is just a primer but in future article we will be delving deeper into the subject matter.

For those interested, see also [KPMG16] and this video (in Dutch): http://bit.ly/1riW4EO.

Whether a bank facilitates a payment or investment or whether an insurer pays out a claim they are basically delivering two trust-based services:

1. keeping record of their clients' asset balances;
2. executing accurate changes to these asset balances based on a specific set of circumstances.

The vast majority of these asset balances are stored digitally. As we know digital information, unlike other value stores such as precious metals, can be easily copied. Financial institutions are obliged to go to great and expensive lengths to keep their digital files safe and scarce. Their trusted services therefore depend upon the maintenance of digital scarcity. So if you can create digital scarcity you can automate trust.

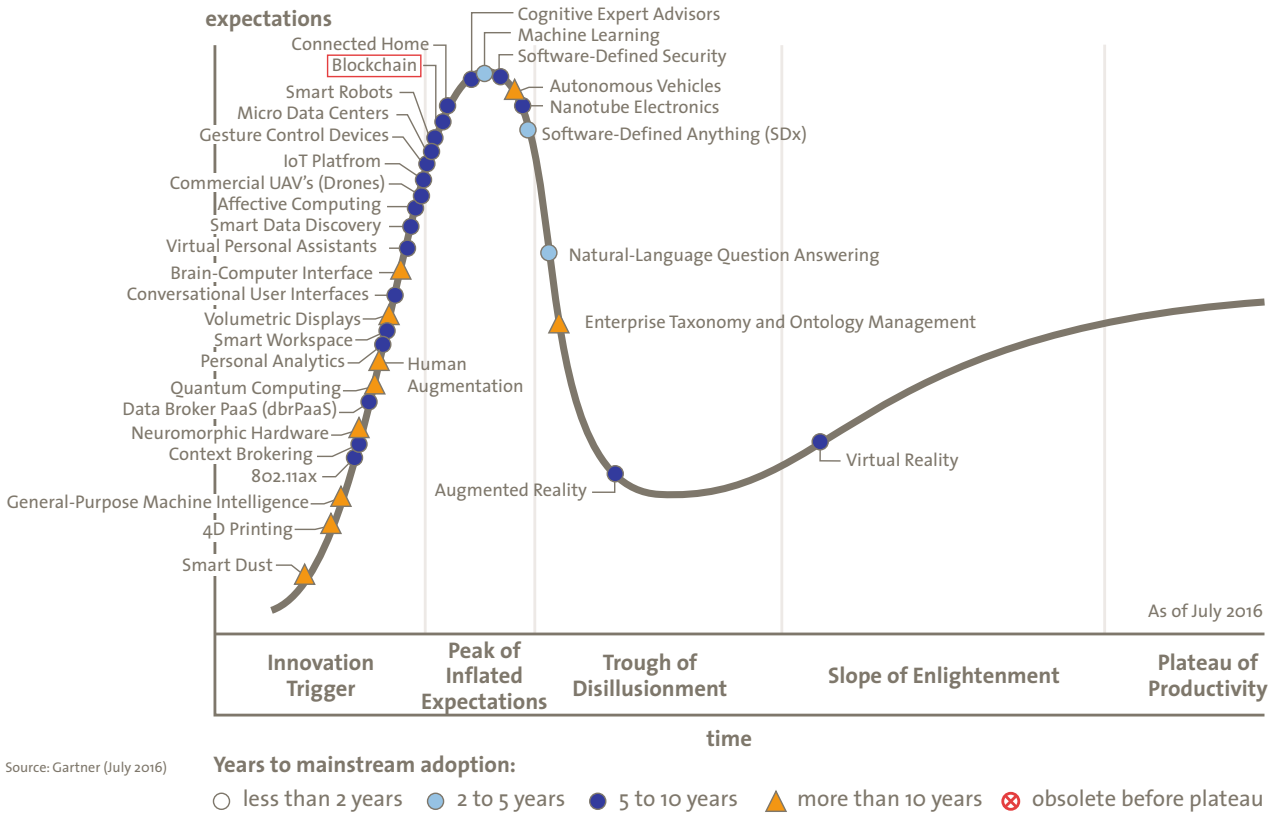
The digital currency Bitcoin was invented in 2008. Bitcoin's underlying technology, the blockchain, dealt with the issue of digital scarcity by recombining well-known and well-used cryptographic methods to create an immutable and transparent digital ledger on which transactions can happen on a peer-to-peer basis. The use of cryptographic methods mean that blockchains achieve this feat without (human) trusted third parties, but with auditable computer code.

The ability to maintain complex, transactional networks without relying on centralized third parties has also paved the way for novel approaches towards prediction market platforms and asset registries. Some industry experts even talk about a blockchain-based rethink of corporate structure.

As soon as one starts looking at business from a transactional perspective then one sees the applications of blockchain in healthcare, real estate, banking, insurance, supply chain, forensics and the public sector to name a few. One will also see that many of the bottlenecks and potential process improvements have a transactional aspect to them.

Evolving business considerations

Based on the abovementioned potential one could be forgiven for thinking that blockchain is the complete remedy for all business process issues. The technology is still maturing and a single global standard has not (yet)



Source: Gartner (July 2016)

Figure 1. **Gartner hype cycle for emerging technologies ([GART16]).**

Public distributed ledger has at its basis a cryptocurrency, this gives the ledger a built-in economic incentive for participants as currency is earned for participating in the network, for instance by providing processing power

emerged so predictions are difficult to make, but what is certain is that the business considerations surrounding blockchain are always evolving.

Initially, Bitcoin the currency drew bad press due to its use by criminals to purchase drugs and use in the infamous cryptolocker[1] viruses that encrypt the entire computer of the victim, only to release the files after payment of Bitcoin (so-called 'ransomware'). After a stringent distinction was made between cryptocurrencies and the actual blockchain technology the focus shifted to transactional privacy in a cross-organizational setting as well as transactional speed and capacity.

This new set of considerations brought about a very important distinction in the types of blockchain. When banks are sharing data on a blockchain, they would want to make sure that all transactions are private and that there is only a select group of members that can join the network. A public blockchain such as the Bitcoin blockchain does not allow for privacy and selective participation. Private blockchains were therefore developed of which Hyperledger Fabric developed by IBM is an example. During this time, the overarching term distributed ledgers also came to the forefront to refer to both private and public blockchains. This convention is used within KPMG and also for the rest of the article.

Private distributed ledgers

A private distributed ledger is a type of blockchain which has a permissioned access to the network. The private ledger is set up in such a way that after a party has received access to the network, transactions remain private. This can be beneficial if many parties in an industry want to cooperate, however they do not want to have all transactions public. The ledger works in such a way that transactions are only visible for the parties that are involved in the specific transaction, giving a higher level of transaction privacy than in a public distributed ledger. Examples of private distributed ledgers are Hyperledger (financial industry) and BigchainDB (provenance tracking).

Public distributed ledgers

Bitcoin is the quintessential example of a public distributed ledger. In such an open distributed network, transactions are transparent and every user can join or leave the network at any time. These properties make it suitable for a large number of widely distributed parties to work together and create value. The fact that transactions are transparent, the network access is unrestricted and the code is open source means that anybody can check transactions or build applications on top of the distributed ledger. A public distributed ledger has at its basis a cryptocurrency, this

1 https://en.wikipedia.org/wiki/CryptoLocker

	Public distributed ledger	Private distributed ledger
Participation in network	Open	Closed
Transactional privacy	Not prioritized except for so-called anon-coins	Adjustable to the wishes of the participants
Economic incentive for participation	Built-in	Contractually organized
Transaction volume supported	Low	High
Commonly used for	Payments, Remittances, Prediction Markets, Distributed Storage, Paid Social Networking, Asset Exchange	Asset servicing, FX (Foreign eXchange), Provenance Tracking

Table 1. **Key differences between public versus private distributed ledgers.**

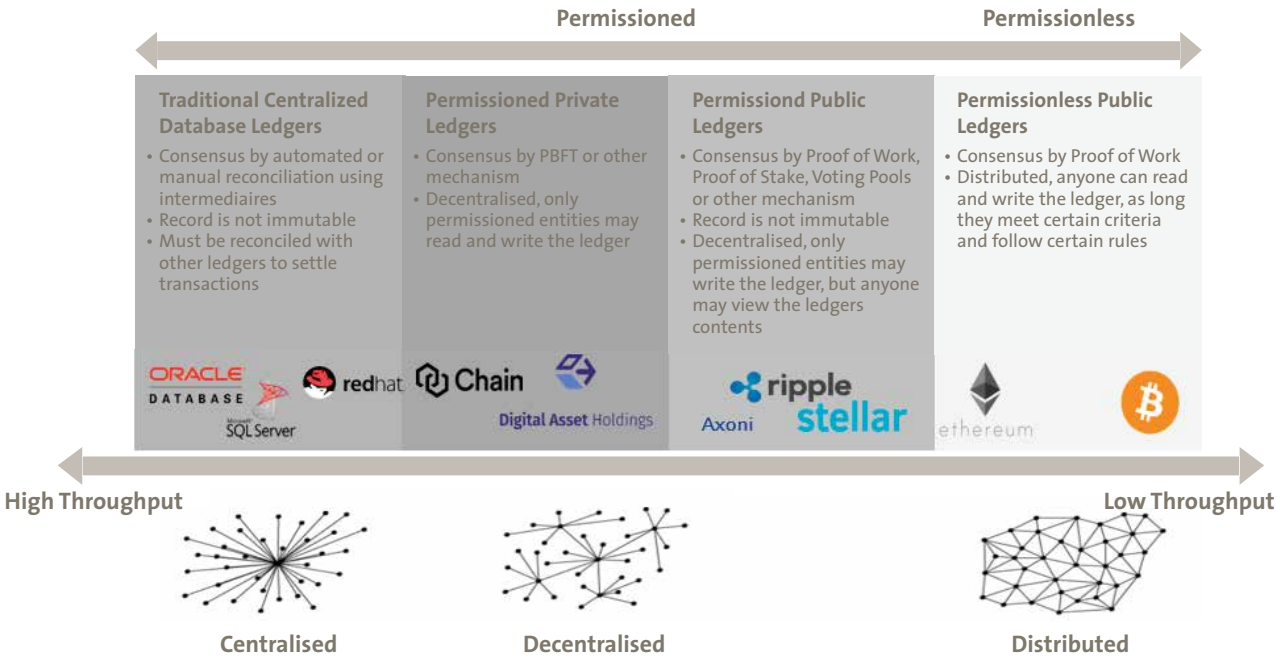


Figure 2. **KPMG continuum for level of ledger distribution.**

Distributed ledgers at KPMG

The potential of distributed ledgers in their private or public form is massive and KPMG acknowledges this. It is therefore no surprise that Distributed Ledger Services teams were launched within KPMG in more than 30 countries. This happened as recently as mid-2016 but interesting projects in transport, banking, insurance, capital markets and healthcare are already underway.

Seeing that blockchain technology is applicable to many industries and processes our teams are more than willing to educate and collaborate with different business units. The combination of your business knowledge and our knowledge of distributed ledgers is bound to lead to new ways to create customer value.

A distributed ledger delivers unique benefits in situations where multiple parties have a need to interact and share data with each other (1). A distributed ledger enables the logging of actions of these interacting parties (2), in such a way that the participants can trust that these actions that are recorded are valid (3) by the design of the network and consensus algorithms. A distributed ledger removes the 'central authority' intermediary to reduce cost (e.g. fees), a dominant party in an industry sector and complexity (e.g. multiple reconciliations) (4) and hereby also reducing delays and automating paper processing (5). Lastly a distributed ledger delivers value when transactions are interdependent (6).

provides the ledger with a built-in economic incentive for participants since currency is earned for participating in the network, for instance by providing processing power. This is in contrast to a private distributed ledger where the incentive for participation is not built into the system but contractually organized. Examples of public distributed ledgers are: Bitcoin (currency), Ethereum (smart contract platform) and Steem (social networking).

Although transactional privacy is the main concern due to their architecture other differences between public and private ledgers exist. The main ones are summed up in Table 1.

The distinction between public and private ledgers becomes more granular based on the anticipated need from different industries for both public and private distributed ledgers to come in permissioned versions. Meaning

The potential of distributed ledgers in their private or public form is massive

participation in the network can be open or closed based irrespective of whether the transactions in the distributed ledger are public or private. Figure 2 illustrates this continuum.

To use distributed ledgers or not to use distributed ledgers

The level of collective knowledge on distributed ledgers is growing fast. With this new level come new business considerations. The most current consideration is on the optimized usage of distributed ledgers. Distributed ledgers, especially private distributed ledgers, can be very close in function to usual databases. For instance, during the recent Hyperledger Hackathon 17 out of the 21 use cases were dismissed by the jury for not being distributed ledger use cases. KPMG has therefore defined the following six criteria to determine whether a use case can be helped by using a distributed ledger.

Conclusion

A distributed ledger solution is much more than simply introducing new IT; existing business processes and even entire business models will be changed by adopting this innovation. Distributed ledgers deliver most of their value in having multiple parties work together in an efficient and effective manner, therefore the process of redesigning existing business processes is not a standalone action. One has to get the entire value chain 'on board' and start using distributed ledgers.

We can conclude this article with the notion that distributed ledgers are available in a multitude of different manifestations. Some solutions lean more towards the public distributed ledger approach, while some solutions have more in common with a private distributed ledger. This does not mean that one approach is necessarily better than the other; they all have their own unique use cases and pros and cons.

This is the introductory article of a series on the interesting world of distributed ledgers. Be on the lookout for the next article in future issues of Compact.

References

[GART16] Gartner.com, *Gartner Hype Cycle for Emerging Technologies*, **2016, http://www.gartner.com/newsroom/id/3412017.**

[KPMG16] KPMG, *Consensus Immutable agreement for the Internet of value*, **2016, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf.**

About the authors

Ir. Hardwin Spenkelink first got interested in cryptocurrencies and distributed ledgers in 2013 when he started mining his own cryptocurrencies. In 2014 he graduated with a masters degree at the University of Twente on the topic of the adoption of cryptocurrencies. In the same year he started working at KPMG IT Advisory as a Senior Consultant and has kept very active in the distributed ledger space. Last year (2016) he joined the newly formed global KPMG Distributed Ledger Services team.

Gys Hough's first foray into cryptocurrencies was in 2012. The initial interest in price speculation developed into a passion for distributed ledgers and what decentralization could mean for industry and society. He has consulted on the topic in the payments industry at a European level and has worked together with Dutch banks and regulators. As a recent addition to the Distributed Ledger Services team at KPMG as a Senior Consultant he is committed to making distributed ledgers an integral part of the KPMG value proposition.

The authors would like to thank Dennis de Vries as Lead of KPMG Digital Ledger Services for his review of previous versions of this article.