Death of the Blockchain – exaggerated?

14 July 2016 | **Blockchain, Business Innovation, Digital Transformation** | **Immo Hüneke**
Reading time: 10 minutes

Mark Twain responded to his premature obituary in a newspaper: “The report of my death was an exaggeration”. The same may or may not be said about articles that have appeared recently on the “demise” of the blockchain.

It is undoubtedly true that a huge amount has been written and that much of it is probably ill-informed – on the part of detractors as much as of those who hype the technology well beyond the justifiable. Some seven years after the launch of Bitcoin, blockchain technology is entering the “trough of disillusionment” on the Gartner hype curve – the point where sufficient early adopters have got their hands dirty (and in some cases, their fingers burnt) to amount to a reality check on some people’s wildly optimistic initial expectations.

As technologies mature and users discover their true strengths and weaknesses, they usually move out of this trough and are deployed in roles where they contribute the greatest value – although in some cases, they disappear without trace. So it is worth examining whether blockchain technology might have a valuable role to play in products and services that individuals and organisations truly want to use.

What is a blockchain?

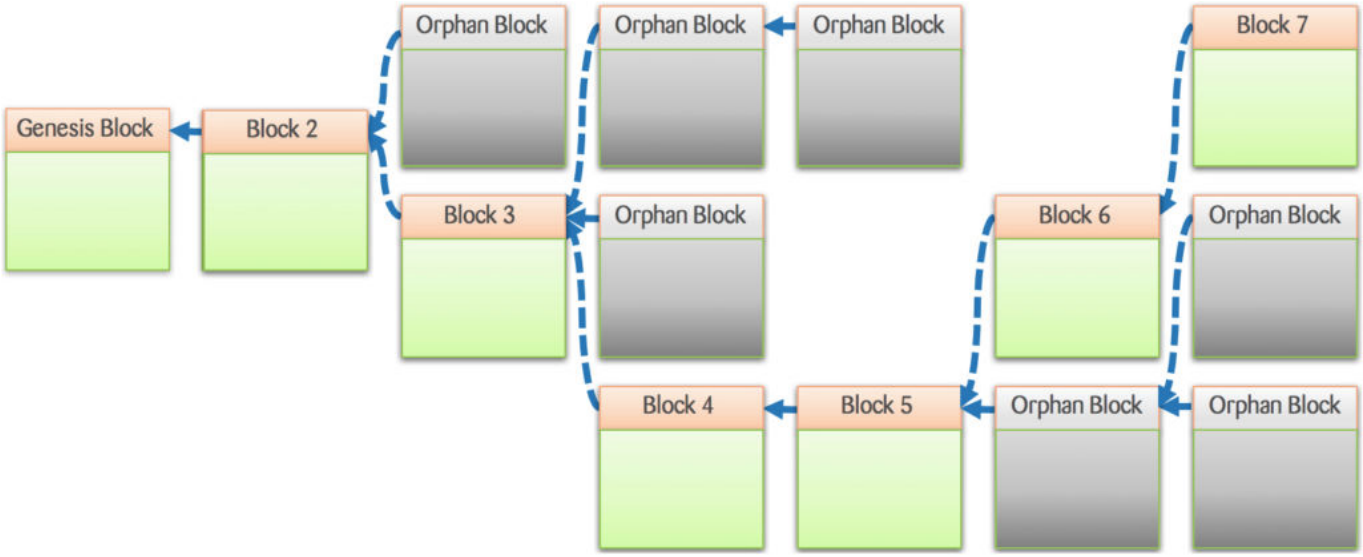
In essence, it’s a very big file replicated to thousands of locations – what is called a distributed ledger. Ledgers have been used since time immemorial to record important facts and forestall disagreements – for example, who owns a particular asset, or the date on which an asset was transferred to a new owner and what the new owner gave in exchange. Financial transactions are one important category of ledger entry, but by no means the only one – for example, you might record a put option, a sporting bet or your last will and testament in a blockchain. Because there are many copies of the file, once a record has been validly entered, it becomes tamper-proof for all practical purposes.

The name “blockchain” is derived from the fact that new information can only be added to the file in blocks that refer to their predecessor in the chain.

Not all blockchains are created equal

You should be aware that there is not just one blockchain. When people refer to “the blockchain”, they usually mean the one on which Bitcoin was implemented. Blockchain is also the name of a company that provides software products around this blockchain and around its cryptocurrency, Bitcoin, such as an online e-wallet, a blockchain explorer and many

different dashboards.



Blockchain Consensus Mechanism

There are many competing blockchain implementations, which are to a greater or lesser extent variations on the original. Each claims to offer some technical or business advantage, which usually comes at the cost of disadvantages in other areas. Although many of these focus on distributed ledger applications that have nothing to do with financial transactions, they nevertheless all implement some form of cryptocurrency. This is required as a means of regulating the supply and demand of computing resources. All currently viable public blockchain implementations rely on the application of prodigious amounts of distributed processing.

Recently, there has been much carping about blockchains – some commentators going as far as calling them “snake oil” and lead developer Mike Hearn disowning the whole Bitcoin project. In part, this stems from the very success of Bitcoin – the system is approaching its limits in terms of the rate of transactions it can support, as well as the total money supply.

The same limitations don’t necessarily apply to alternative blockchain technologies – for example, San Francisco-based start-up Chain has published the Chain Open Standard, an open-source set of technical standards for building a blockchain network that it claims can handle tens of thousands of transactions per second securely and privately. Private chains are open to vetted users only. This vastly reduces the amount of proof-of-work computing required and opens the way to speeding up and reducing the cost of operations such as real-time gross settlement by eliminating the need for a central clearing-house.

However, it is important to be aware that all blockchain technologies have technical restrictions of one kind or another, which deserve careful consideration before launching

products or services built around them.

Who's Who

Many private and public bodies are investing in research and development.

- The NASDAQ exchange, in collaboration with Chain, launched Linq, a ChainOS-based system to record trades in privately held companies, in December 2015. It radically cuts costs by eliminating middlemen such as auditors, legal experts, book keepers and consultants during the pre-IPO phase of a start-up
- The UK is one of the "Digital 5" group of nations, which also includes Estonia, Israel, New Zealand and South Korea. Estonia has already introduced its e-Tax system and a free public notary based on Keyless Signature Infrastructure from Guardtime, which uses blockchain technology, and its e-Residency platform based on NASDAQ's Linq
- Politicians seeking to clean up the Property Institute in Honduras have asked Factom Inc. to develop a prototype blockchain-based land registry
- Interest in the idea has also been expressed in Greece, which has no proper land registry and where only 7% of the territory is adequately mapped
- Bank of England Governor Mark Carney announced in June 2016 that the bank was investing in a variety of FinTech projects including several pilot blockchain applications. A research note it published in late 2014 had already concluded that distributed ledgers were a "significant innovation" that could have "far-reaching implications" in the financial industry
- UBS, Goldman Sachs, JP Morgan and dozens of other banks are investors in R3 CEV, which is developing a standardized architecture for private ledgers including the creation of a standard "settlement coin". Barclays Accelerator London Demo Day in April 2016 demonstrated a prototype of Barclays Smart Contract (see below) Templates on R3's prototype Corda distributed ledger platform. A special-purpose language named CLACK supports the prototype

Opportunities

An *Economist* article in October 2015 identified three main classes of opportunities:

1. Asset transfers of any kind. We are used to the idea of numbered banknotes, but not of numbered coins or even fractions of coins. Although Bitcoin transactions are denominated in cents, each bitcoin cent is divisible into one million units, each of which is individually addressable and programmable. The same principle applies to other blockchain implementations. Tel-Aviv-based startup Colu has developed a mechanism to "dye" very small transactions ("bitcoin dust") by adding extra data that can represent bonds, shares, diamonds, units of precious metal, and especially, local currencies such as the "Barbados Dollar" or "Pishpesh Shekel".
2. Protecting ownership and rights. Applications can use the blockchain as a repository of

indisputable information, by combining snippets of additional information with transactions that become embedded in the ledger. The blockchain thus becomes a registry of anything worth tracking closely – land, luxury goods, works of art, vehicle chassis and engines, intellectual property, even individual specimens of endangered species identified by DNA samples. Everledger helps to combat diamond- and fine-art-related crime, particularly insurance fraud, by partnering with insurers, law enforcement, galleries, auctioneers and the ten diamond certification houses across the world to provide indisputable proofs of provenance and ownership.

3. Smart contracts. Contracts are expressed not in legalese but in executable code, which is triggered when the circumstances match their preconditions. For example, bitcoin units may become available only under certain conditions – e.g. they can only be spent on specific categories of goods or services. The contract that pays Bitcoin miners for solving a puzzle stipulates that the payout is deferred until another 99 blocks have been added to the chain. But a smart contract can be applied to literally any electronically accessible resource. Lighthouse is a decentralized crowdfunding platform that lets users create projects and pledge bitcoin to those projects. Smart contracts ensure that the pledges are collected only if the funding target is reached. Other applications address the services sector: for example, breaches of service level agreements can automatically trigger compensation payments. Or a car bought on credit might not start in the morning if the repayments are in arrears.

Problems with Smart Contracts

Smart contracts on the Bitcoin blockchain and its close relatives are written in the deliberately restrictive Bitcoin scripting language (derived from the stack-based language Forth). It is neither expressive nor user-friendly. Consequently, smart contracts expressed in this language have tended to be quite rudimentary, which has resulted in no documented cases of hacking or exploitation so far.

An alternative, soon to be launched, is Bitcoin developer Jeff Garzik's Bloq Ora, which theoretically allows contracts to be coded in any Turing-complete language such as Javascript or Python. This is part of BloqEnterprise, which offers a blockchain operating system (BOS) for many different private and public blockchain implementations. It is reasonable to assume that distributed computing platforms such as blockchain require a standardized OS to allow developers to port their skills and applications from one to the others. However, as in more conventional OS, a never-ending evolutionary arms race may be anticipated with ever more sophisticated attackers.

Ethereum offers a range of programming languages for its smart contracts, including CLL, which resembles C; Serpent, which resembles Python; a Javascript API; and the C++-like Solidity, whose Turing-completeness is both its strength and weakness. A drawback of the language was dramatically demonstrated in June 2016 by a much-publicised "drain" of funds

from the Distributed Autonomous Organisation (DAO), an investment vehicle akin to Lighthouse. The unknown attackers exploited non-reentrancy in one of the DAO's contracts by causing it to be invoked recursively, triggering a race condition between the balance check preceding a requested payment and the balance decrement after it. Unfortunately, the defective smart contract is unalterably embedded in the Ethereum blockchain, and as yet nobody has devised a foolproof versioning mechanism that would allow such bugs to be fixed.

Formulating a Strategy

In this bewildering and rapidly changing and landscape, how can a forward-looking organization be sure that it is taking the right steps to adapt, survive and thrive? This calls for a plan.

1. Understand your objectives, which will stem from the overall mission statement, values and culture of the organization when measured against the blockchain challenge:
   - Are you simply going to defend your existing revenue streams against new disruptive competition?
   - Are you planning to make efficiency savings across your operations?
   - Are you looking to exploit new business opportunities? If so, will you develop and launch new blockchain-based products yourself, license them from someone else, or offer value-added services around someone else's products?
2. Survey the landscape:
   - Where are you today with respect to the objectives identified above?
   - What are your existing strengths and what approaches do these suggest?
   - What obstacles and hazards stand between you and where you want to be?
   - Can you plot an efficient path to the objective, avoiding the pitfalls?
3. Get moving as soon as reasonably practical, in order to
   - Identify resource needs
   - Verify assumptions
   - Gain knowledge
4. Monitor the situation:
   - Be ready to modify the plan in the face of unforeseen difficulties or emerging opportunities
   - Review the objectives and strategy regularly

Conclusion

Within the past year or two, blockchain has dramatically erupted into the collective consciousness as a potentially disruptive technology. While a great deal of caution must be deployed, its potential (in terms of both threats and opportunities) is too great to ignore. The organizational strategy must reflect this and may justify the investment of time, effort and

money in appropriate pilot projects sooner rather than later.