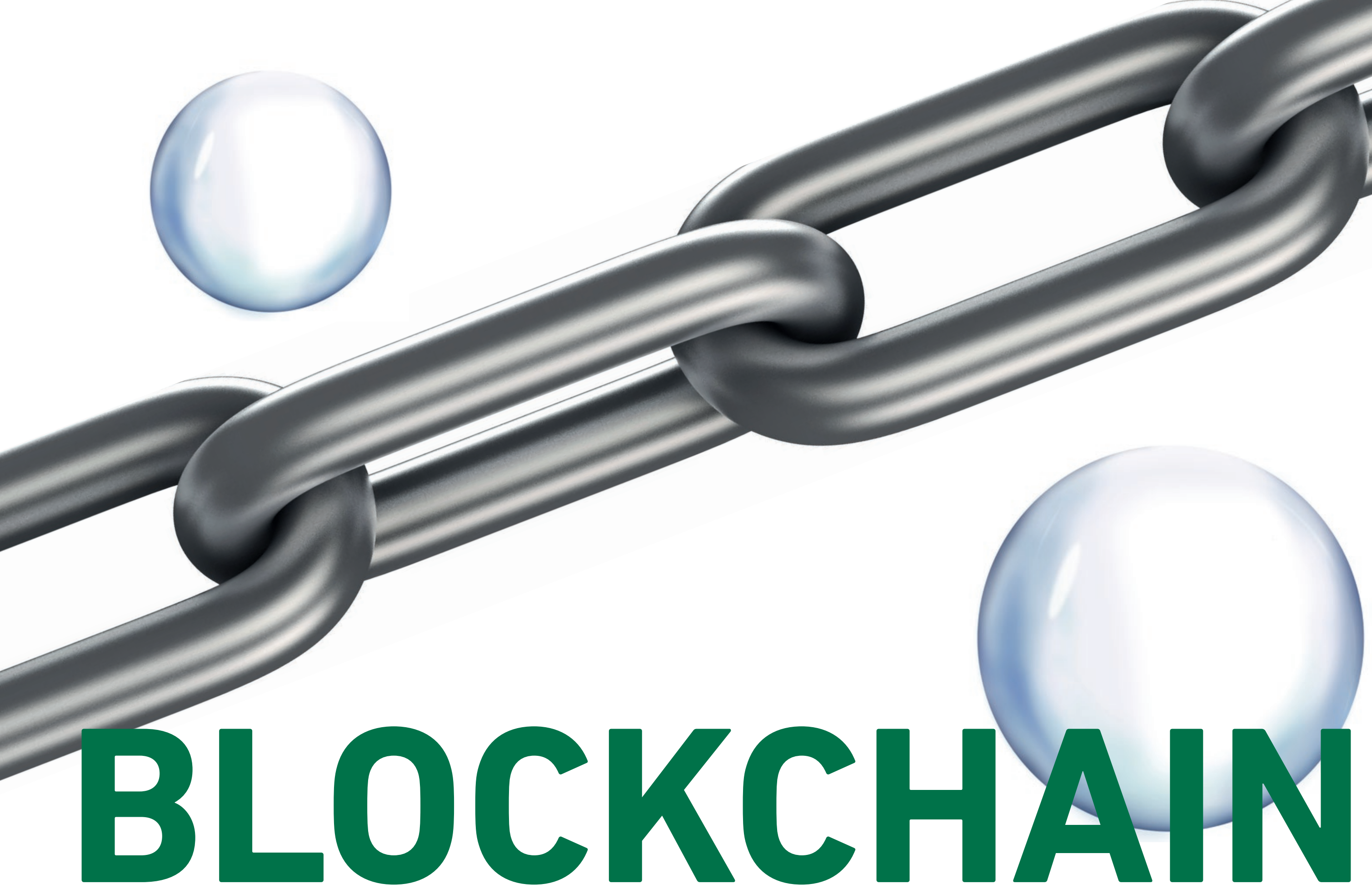


BLOCKCHAIN

DOUBLE BUBBLE OR DOUBLE TROUBLE?

Something very exciting is happening on the internet and, depending on whom you ask, it could be as game changing as the internet itself, or as mundane as just another protocol layer on it. The noise, hype and media coverage surrounding blockchain has reached fever pitch over something that is conceptually simple, technically straightforward and potentially super-disruptive. BCS DRM blogger Jude Umeh brings some clarity and perspective on the blockchain and explores what is required for it to either live up to the game-changing expectations or end up as yet another faddish internet bubble.

Images: Thinkstock/TimArbaev (chain) and WaveBreakMedia (bubble)

doi:10.1093/itnow/bwv026 ©2016 The British Computer Society

The hype is on overdrive - A simple Google search for 'blockchain' returns over 4.9M results within 0.7 seconds, whilst the result for 'Bitcoin' is higher by an order of magnitude, returning 94M results in 0.31 seconds. This is unsurprising given that bitcoin cryptocurrency was first on the scene, in terms of public perception, rather than its underlying blockchain.

What is bitcoin? Bitcoin is a decentralised digital cryptocurrency, which is created and held electronically, without any government controls. Bitcoins are produced by people or organisations running mining computers all around the world with software that solves mathematical problems, which constitute 'proof of work', in return for new bitcoins. According to tech investor Marc Andreessen, the value of bitcoin as a digital currency is directly linked to the volume and velocity of payments going through the system, as well as speculation on future use of the payment system. This latter speculation, no doubt fuelled by incessant hype, has helped to increase adoption and valuation of bitcoin (i.e. currently over $400 for a single coin) thereby creating a self-fulfilling prophecy. Further on in this article we'll explore the impact that bitcoin and other cryptocurrencies have on entire industries, as well as the challenges they must face.

What is blockchain?

Blockchain is the core technology upon which bitcoin and other applications have been built. Fundamentally, a blockchain is a distributed ledger of all transactions, which are recorded into discrete blocks and linked together, in a chain. Each block contains private data, (aka transactions), and a public header, which is used to link to the next block on the chain. The blocks are sequentially linked and cryptographically secured such that only the owner of data in a block can unlock it using their private key. However, anyone can see who owns each block, via its public header information, and can follow the links through the entire chain right back to the first block. The blockchain is stored in a peer network of nodes, where each node contains a copy of the entire blockchain and has the ability to add new blocks to it. Some key attributes of blockchain are:

- Decentralisation - blockchain works by linking all participants in a market place without intermediaries such that each transaction is transparent to all the participants in the network. It has been described as 'a value network, where parties can transfer custody of valued assets in an auditable manner without relying on intermediaries.'
- Trust and provenance - transactions on the blockchain do not require any authorisation, validation or verification by a trusted third party or intermediary. The blockchain provides irrefutable evidence that

the data (or transactions) in a block existed at a particular time, and because each block contains a hash of the header of the preceding block this creates automatic proof of the history, position and ownership (i.e. which node created) each block on the chain.

- Resilience and irreversibility - blockchains are designed for secure distributed operation in a peer network of (public/private) nodes, or computers, each of which hold a copy of the entire blockchain, thereby making it extremely resilient, much like the internet. Once data or transactions are appended and accepted/confirmed by the nodes on the blockchain, it is nigh impossible to change or alter it. The blockchain is essentially an append-only data store (no deletes or edits allowed), hence its capability/suitability as an unimpeachable record keeper.

In summary, the blockchain uses cryptography and the power of distributed computing to provide a digital trust mechanism over the internet. It does this in such a way that, as Marc Andreessen puts it, 'only the owner of an asset can send it, only the intended recipient can receive it; the asset can only exist in one place at a time, and everyone can validate transactions and ownership of all assets anytime they want.'

Key blockchain applications across industries

There are several types of blockchain applications and the following groups, (adapted from a *Radar* article by William Mougayar), are used to categorise them according to function and increasing levels of complexity, autonomy and impact.

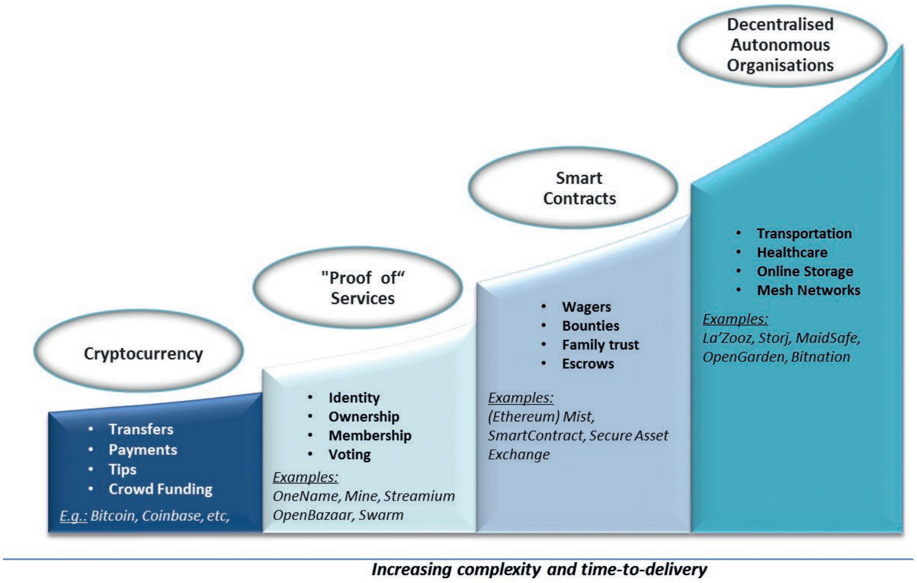
1. Cryptocurrency. This blockchain application is used for making transfers and payments, and it works by enabling trusted transactions between unknown parties, at negligible cost, and without any intermediary. Cryptocurrencies has effectively napsterised the payments industry, which typically relies on trusted third parties to work. The profound implication of blockchain is not lost on the financial services industry, many of whom are working frantically to understand and explore opportunities created by this technology. According to a McKinsey report on payments, 'if distributed ledgers become the basis for the booking and transfer of public securities, they will bring about significant changes in post trade activities such as clearing, custody and cash management.'

In addition to streamlining cumbersome, costly and risky correspondent networks, they could effectively replace the technological infrastructure for processing securities in real-time. Leading financial institutions such as Barclays, Citibank, UBS, Deutschebank and HSBC are experimenting with blockchain and the distributed consensus model, although many are using a 'safer' approach that limits the network only to recognised and trusted nodes in what is known as 'permissioned' or 'proof of stake' blockchains. Ripple, the second largest cryptocurrency after bitcoin, uses a permissioned blockchain and is squarely aimed at the financial services industry.

In the creative industries, blockchain applications like bitcoin make it economically feasible to execute true micro transactions, (i.e. to the nth degree of granularity in cost and content or sub component thereof). There are several initiatives using blockchain to improve transparency in music payments - e.g. artiste Imogen Heap's collaboration with UJO Music features a prototype of her song demonstrating how income from any aspect of the song and music is shared transparently between the contributors.

2. Proof services. This is based on a core capability of blockchain to 'store value' at an atomic level, (e.g. identity, ownership, membership etc.), as a horizontal service upon which useful vertical applications can be built. Such applications could be used by governments to provide services for their citizens, and various research outfits are actively looking into this area. For example, the MIT Digital Currency Initiative is collaborating with multiple stakeholders, including governments, to identify and develop practical pilots for suitable blockchain-enabled use cases. Their article in *Wired* highlighted some plausible scenarios, e.g. birth and death certificates, business licenses, property titles, as well as certain non-governmental records (e.g. educational qualifications). Real-life examples include the identity-based services offered by BitNation, (a project aimed at decentralising governance at a global scale), who have already created a World Citizenship ID based on blockchain. They also launched a Refugee Emergency Response project, which features: BitNation

Key Blockchain Application Groupings


Decentralised Autonomous Organisations
Smart Contracts
"Proof of" Services
Cryptocurrency
• Transfers
• Payments
• Tips
• Crowd Funding
E.g.: Bitcoin, Coinbase, etc,
• Identity
• Ownership
• Membership
• Voting
Examples: OneName, Mine, Streamium OpenBazaar, Swarm
• Wagers
• Bounties
• Family trust
• Escrows
Examples: (Ethereum) Mist, SmartContract, Secure Asset Exchange
• Transportation
• Healthcare
• Online Storage
• Mesh Networks
Examples: La'Zooz, Storj, MaidSafe, OpenGarden, Bitnation
Increasing complexity and time-to-delivery

Source - Adapted from **"Blockchain Apps: End user View"** by William Mougayar (2015) http://radar.oreilly.com/2015/01/understanding-the-blockchair

Emergency ID (BE-ID) and Bitcoin Visa Debit Card (BDVC), for displaced individuals in the ongoing refugee crises in Europe.

3. Smart contracts. Contracts that can self-execute transactions without intervention by a third party is the key idea behind smart contracts. Such automated transactions, (based on predetermined rules and specific events which are embedded in the contract), are executed between two or more parties well after the contract is created. The Ethereum Project is one of only a few public blockchains to offer full featured smart contract capability. Others are privately owned, 'permissioned' blockchains which connect only known and trusted nodes, for additional security. This makes some sense given the enormous power smart contracts possess to do more than merely transfer funds. In a blog post about internet of things (IoT) governance, I touched on how blockchain (aka smart contracts) could ultimately play the role originally intended for, but woefully executed by, DRM mechanisms. However, it is still early days, and there are still a few obstacles to overcome, e.g. it seems smart contracts can make for slower blockchains.

4. Decentralised autonomous systems/ services. This is perhaps the ultimate role for blockchain, i.e. providing the trust mechanism that underpins a key manifestation of the evolving interdependence, (dare I call it symbiosis), between man and machine. According to Ethereum Founder Vitalik Buterin, a decentralised autonomous organisation (DAO) 'is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.' It is based on a blockchain where the users become part of the chain, (i.e. in their roles as owners, users and nodes), by doing work which enhances the value of the self-organising and self-governing DAO.

An article by William Mougayar also provides useful insight on the operational framework for DAOs. Creating a DAO is no walk in the park, however, once fully implemented it'll likely have tremendous impact on various industries. Some early examples are starting to show up in

Further reading

1. 'What is Bitcoin?' https://bitcoin.org/

2. 'Will Provenance Be the Blockchain's Break Out Use Case in 2016?' Gideo Greenspan & Maya Zehavi (2016) www.coindesk.com/provenance-blockchain-tech-app/

3. 'Why Bitcoin Matters' Marc Andreessen (2014) http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

4. 'Understanding the blockchain' William Mougayar (2015) http://radar.oreilly.com/2015/01/understanding-the-blockchain.html

5. 'Napsterize' definition www.macmillandictionary.com/dictionary/british/napsterize

6. '16 in 2016: Trailblazing trends in global payments' in Mckinsey on Payments: Volume 18, Number 22 (2015) http://bit.ly/1SY7lwa

7. 'What is Ripple?' https://ripple.com/

8. 'Tiny Human by Imogen Heap' https://alpha.ujomusic.com/#/imogen_heap/tiny_human/tiny_human

9. 'MIT Digital Currency Initiative' https://www.media.mit.edu/research/highlights/media-lab-digital-currency-initiative

10. 'How blockchain will enable self service government' by Brian Forde and Michael Casey (2016) www.wired.co.uk/news/archive/2016-01/05/blockchain-is-the-new-signature

11. 'Governance 2.0: Borderless / Decentralized / Voluntary' https://bitnation.co/main/

12. 'BITNATION WORLD CITIZENSHIP ID V. 0.2' https://bitnation.co/world-citizenship-id/

13. 'BITNATION REFUGEE EMERGENCY RESPONSE (BRER)' https://refugees.bitnation.co/

14. 'What is Ethereum?' www.ethereum.org/

15. 'DRM for things - managing the rights and permissions for IoT' Jude Umeh (2015) www.bcs.org/content/conBlogPost/2519

16. 'Why smart contracts make slow blockchains' Gideon Greenspan (2015) www.linkedin.com/pulse/why-smart-contracts-make-slow-blockchains-gideon-greenspan

17. 'DAOs, DACs, DAs and More: An Incomplete Terminology Guide' Vitalik Buterin (2014) https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

18. 'An Operational Framework for Decentralized Autonomous Organizations' William Mougayar (2015) http://startupmanagement.org/2015/02/04/an-operational-framework-for-decentralized-autonomous-organizations/

19. 'IBM Buys The Weather Company, Advancing Its Insight Economy Strategy' R 'Ray' Wang (2015) www.constellationr.com/research/ibm-buys-weather-company-advancing-its-insight-economy-strategy

20. Silk Road (marketplace) https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

21. 'Mt Gox: The History of a Failed Bitcoin Exchange' Yessi Bello (2015) www.coindesk.com/mt-gox-the-history-of-a-failed-bitcoin-exchange/

22. 'Bitcoin: A Peer-to-Peer Electronic Cash System' Satoshi Nakamoto (2008) - https://bitcoin.org/bitcoin.pdf

23. 'What is the impact of blockchains on privacy?' Jenni Tennison (2015) http://theodi.org/blog/impact-of-blockchains-on-privacy

24. 'Everyone's talking about blockchain' Anat Elhalal (2015) www.digitalcatapultcentre.org.uk/everyones-talking-about-blockchain/

25. 'Blockchain: smart contracts for creative collaborations' Sam Davies (2015) www.digitalcatapultcentre.org.uk/blockchain-smart-contracts-for-creative-collaborations/

26. 'RoboCop' David Z Morris (2015) https://aeon.co/essays/are-we-ready-for-companies-that-run-themselves

areas such as: transportation, healthcare and online storage. In each case, users are recruited to do some work that will enhance the value of the entity. Given that DAOs are non-profit making by definition, various players may seek to monetise this opportunity by acquiring strategic resources needed by DAOs - e.g. high quality information and insight services. IBM's recent acquisition of the Weather Channel may be a clear signal of this shift.

The weakest link

The overall strength of any chain resides in its weakest link, and in the case of blockchain that weak link may be found in end-users of blockchains such as bitcoin. For instance, Silk Road generated over $200 million in sales of drugs and other illicit goods using bitcoins. Also, as a currency, Bitcoin has suffered severe volatility in its lifetime, e.g. falling from over £1,200 to £250 in the course of a year.

Furthermore, Bitcoin has a history of security breaches and hacks, e.g. Bitstamp (a Slovenian exchange) was hacked to the tune of $5m following the even more headline-grabbing $350m hack of Mt Gox (a Tokyo Bitcoin exchange). These unfortunate events were not due to flaws in Bitcoin's blockchain technology, rather they're linked directly to its use and abuse by people. However, there are still a few concerns and issues with blockchain that need addressing.

Block hacking/tampering

What if someone hacks the nodes and changes or deletes transactions? In order to alter a transaction in the blockchain, an attacker will need to modify data within the transaction block, which will change the cryptographic hash (or signature) of that block, thus requiring regeneration and re-linkage of every subsequent block on the chain. It'll need over 50 per cent of the network nodes to agree to in order to make this work.

According to the original paper by bitcoin designer, Sataoshi Nakamoto, 'As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.' Although not totally impossible, such a hack is a non-trivial, computationally prohibitive activity to execute over a large distributed peer network.

What about the real cost of a 'free' service (e.g. power consumption, performance and scalability)? Blockchain processing (e.g. mining for bitcoins) requires computational resources to perform hefty calculations, as 'proof of work', in order to obtain itcoins. This requires electricity and, although the exact carbon footprint of the bitcoin system is unknown, various estimates claim anything between the amount of energy needed to run a small country, (I've heard Ireland mentioned in this context), to that required for over 150M average American households.

Regardless of the actual number, there is some real cost associated with mining, especially in the face of climate change and other related concerns. Also there may be built-in performance limitations, such as with bitcoin, which takes up to 10 minutes to add a new block.

Finally, there are scalability concerns with larger blockchains, which need more storage, bandwidth and computing power to process.

This could lead to centralisation behaviours, since only the most powerful nodes are able to handle the task of mining, thereby making it easier to collude together. Finally, good configuration management is essential to ensure all nodes are running the same version software in order to maintain distributed consensus hygiene.

Blockchain vs. privacy

According to the Technology Director of the Open Data Institute, 'the irreversibility and transparency of blockchains make them unsuitable for personal data.'

For one thing, it makes it extremely difficult to exercise people's 'right to be forgotten' since that would require modification or deletion of transactions on the blockchain.

www.bcs.org

Summary, conclusions

In light of the above, the following are some key conclusions to be drawn from the current situation with blockchain technology and applications:

1. Blockchain is certainly high up on the curve of inflated expectations, but that is perhaps only to be expected given the attention already showered upon Bitcoin. The inevitable slump will follow when people start to understand that blockchain is not an all-singing all-dancing solution to every problem in the digital space.

2. Blockchain still has many teething problems to overcome before it can be considered ready for prime time use by a global digital population. Also, it seems not enough people understand and fully appreciate the implications of this technology (both good and bad), therefore it'll need a lot more thinking and tinkering before we can make that call.

3. However, there are profound benefits to be derived from blockchain if/when it can overcome its growing pains. As a matter of fact, it successfully scratches a few digital itches in many areas, including: digital identity, secure distributed trust mechanisms, decentralised digital architectures and business models, as well as forcing the evolution strategy consideration for many types of businesses in the age of digital.

4. Finally, it is tempting to point out the overwhelming parallels between blockchain/bitcoin and other previous disruptive digital phenomena, (e.g. peer-to-peer, Napster, BitTorrent, and PirateBay), but blockchain and its various applications appear to be in a league far removed from those examples. This may be because blockchain has real potential to deliver some of their benefits without all the side-effects, but only time will tell.

Overall, the prognosis for blockchain remains very good, in my opinion, but a fair bit of caution is advised in order to avoid over-inflated bubbles and other potholes on the journey to its realisation.