BUSINESS EXPERT PRESS
EXPERT INSIGHTS

History and Applications of Blockchain Technology

Kate Baucherel

Abstract: Blockchain is a distributed ledger technology, which has its roots in the development of the Bitcoin cryptocurrency in 2009. The emergence of Ethereum, permissioned blockchains, distributed applications, and smart contracts has sparked rapid development. Blockchains are appropriate for any transaction or process that features a string of clear transactions and would benefit from distributed responsibility and disintermediated operation rather than centralized control. However, there are challenges and regulatory concerns to be addressed.

Keywords: Bitcoin, Blockchain, Cryptocurrency, Disintermediation, Distributed blockchain, Distributed Ledger Technology (DLT), Ethereum, Permissioned blockchain, Smart contracts

Kate Baucherel is an author, speaker, and digital business strategist. She first worked in the digital sector in 1988, sparking a lifelong interest in technology and innovation. A qualified accountant with more than 25 years' commercial experience, she helps businesses to solve business challenges using new and emerging technology.

Introduction

Blockchain technology has been hailed as the most important development since the internet itself. Originally underpinning cryptocurrencies, starting with Bitcoin, the concept of *Distributed Ledger Technology* (DLT) is well established in the world of finance (fintech). However, blockchain has the potential to transform both business practices and societal challenges, revolutionizing services in government and the private sector (UK Government Chief Scientific Adviser, 2016). This article examines the different types of distributed ledgers and their existing and potential applications in, among other things, digital identity, government, Internet of Things, accounting and finance, supply chains, and data security.

Development of Blockchain Technology and Bitcoin

Blockchain was originally introduced as the technology that underpins Bitcoin, the first working cryptocurrency. The idea of cryptocurrency has been in fictional and academic circulation for decades. In fiction, it is an appealing concept in the operation of futuristic societies. How else would any character described by authors from Douglas Adams to Isaac Asimov pay for rented

ground cars or cocktails on arrival at the spaceport of a new planet? In research, the concept and workings of digital cash were suggested by a leading cryptographer in the early 1980s, with multiple articles exploring the mathematical underpinning of virtual currency (Chaum, Fiat, & Naor, 1988). Two fundamental problems were clearly defined at the outset. First, double spending: there is a need to prevent someone spending the same digital money more than once. Second, a cryptocurrency must be created, supported, and secured without recourse to physical reserves or central banks. A decade after Chaum et al., a computer engineer (Wei Dai, 1998) suggested solutions for the transfer and the creation of digital money, and also a process for the effecting of contracts, all of which have now been realized.

In 2009, an article was published under the pseudonym Satoshi Nakamoto proposing a "peer-to-peer version of electronic cash" (Nakamoto, 2009). Nakamoto's proof of concept solved the challenge of double spending, and incentivized a huge network of users to create cash and maintain the system in perpetuity through the *mining* process. A working cryptocurrency, Bitcoin, was born.

Operation of the Bitcoin Blockchain

So how does the Bitcoin blockchain enable the currency to function? Double spending is a simple concept, and is solved by the structure of the blockchain itself. In real life, if one person has a dollar bill, and hands it to a retailer, the original holder can no longer spend that dollar. A physical transfer has taken place. If the holder makes a transfer or payment direct from their bank account, the records held in centralized databases at each of the participating banks show that the transaction has taken place and ownership of the money has moved. However, if the currency of this transaction is not part of a traditional banking system and has no physical form, how is it possible to confirm that the transaction has taken place? This is where the blockchain comes into play. A block is created, which contains the original holder's declaration that they have sent a sum of money, and the recipient's declaration that they have received it. The block also contains a reference—a *hash*—that carries the fingerprint of all the preceding blocks in the chain. Each of those blocks is itself an individual transaction. Once our transaction is complete, the block closes and cannot be changed. It is an *immutable* record at the end of a related chain.

Creation of currency is more complex, but vital to the resilience of the blockchain. To verify the transaction in the block we have just made, users who are *special nodes* in the system run a complex algorithm to ensure that the *hash* in the block is referring to the previous blocks in the chain. As a reward for processing that algorithm, these users receive Bitcoin: they have *mined* currency, creating cash, and they have collectively confirmed that the transaction is real. This is *distributed responsibility* for the accuracy of the records: no single entity either controls the records or unilaterally confirms the legitimacy of the recorded transactions.

Extending Blockchain Technology

A blockchain, therefore, is a series of individual transactions, each one referencing the previous related blocks in the chain. Why should a distributed ledger approach be restricted to financial transactions? There are parallels in many sectors, although of course it is important that a blockchain is not viewed as a fashionable replacement for a database. DLT will be most effective and disruptive in processes that feature strings of transactions where there are multiple interested parties, each with responsibility for elements of the chain. As an example, an asset does not have to be monetary to be involved in multiple transactions. The devices we use, the clothes we wear, and the food we eat are all subject to several stages. Organizations

in the chain and even end users have an interest in the origins of the components, the fabric, or the raw ingredients. Responsibility for quality and regulatory compliance is distributed. However, it's likely that the manufacturers want to keep this ledger out of the public domain to protect commercially sensitive information. Additionally, one of the features of the Bitcoin blockchain is the monetary incentive to maintain its integrity. How can the ledger be protected, and how could users be incentivized to carry out transaction verification, which is costly in terms of processing capacity and electricity, in a *distributed ledger* that is not related to a cryptocurrency?

Permissioned Blockchains

To solve the problems of privacy and verification, a more private variant of DLT (Jayachandran, 2017) has started to emerge: the *permissioned blockchain.* This takes all the benefits of blockchain as a transparent, immutable record, but eliminates the anonymity of the users, which is a feature of public blockchains. There is no need to create value, as no currency is involved, so there are no miners. The transaction verification comes through controlled inputs from a known group of distributed participants who have a vested interest in the accuracy of the records stored in the shared blockchain. The ability to include *smart contracts* in the chain incentivizes participation. Enterprise applications, which are built on a private (permissioned) blockchain, use technologies such as *Hyperledger* (Linux), *Fabric* (IBM), *Sawtooth* (Intel), and *Corda* (R3). Where there are clear sequences, such as a series of supply chain transactions, a permissioned blockchain combines the clarity and security of recording with the privacy required in a commercial organization.

Ethereum

In many business settings, a single chain sequence is not appropriate to all scenarios. What about the transfer of a large asset, such as a house? There is a hierarchy of multiple simultaneous transactions that feed into the ultimate transfer of ownership. Surveys and searches must be completed, remedies applied, and completion can be a complex affair with many transactions closing simultaneously, and settlement being made through a complex web of banks and legal representatives. The development of *Ethereum* addresses these complex scenarios.

"A next generation smart contract and decentralized application platform" was proposed by Vitalik Buterin in a white paper (Buterin, 2013), which traced the evolution of the Bitcoin blockchain, identified possible security concerns, and introduced the Ethereum blockchain. Ethereum allows for multi-block decentralized applications or *distributed apps* (dapps), and is already making DLT significantly more accessible as a base for new projects. It also changes behavior around the transaction, incorporating *smart contracts* and the use of *tokens* to provide evidence of the events that are recorded. The speed at which Ethereum dapps are being developed is a good indicator of the scale and rapidity of disruption that is expected from DLT.

Smart Contracts

Both permissioned blockchains and Ethereum include the use of *smart contracts*. Smart contracts were the third feature of the hypothetical cryptocurrency system suggested by Wei Dai (1998) in his article. A smart contract is not a legally binding contract as we would understand it. Instead, it describes a feature of blockchains where the completion of a transaction automatically triggers an action. This could be settlement of an invoice in the supply chain, or the creation of a new transaction that must be carried through. A real-world comparison might be a discharge from hospital treatment that triggers the creation of a follow-up appointment.

The significance of smart contracts is their ability to *disintermediate* any trans-

action. By removing the role of a central agency, parties can transact directly, even settling their commitments using the platform's or the dapp's native currency. However, there are good reasons to be cautious about disintermediation. In practical terms, making disintermediated transactions available to all not only removes the middleman but also obfuscates the legal and fiscal position of the parties. Although a smart contract is a transactional process and not designed to be contractually watertight, execution may result in the formation of a legally binding contract. Would the transaction itself be properly legal if carried out on a dapp, and what recourse do the parties have under law if there is a dispute? While the validity of an immutable, verified transaction cannot be disputed, and there is transparency by the very nature of the system, what jurisdiction applies to the contract that is created? In a wider context, under what tax system should earnings be declared? What privacy or other laws apply to interactions on the dapp? Regulatory bodies will be watching the development of dapps with great interest.

Challenges and Regulatory Concerns

Blockchain technology is still in its infancy, and there is something of a Gold Rush mentality around it. Ideally, developers should be identifying burning problems that need to be solved and deciding to build using an appropriate blockchain after a process of determining the best technology for the project. Commonly, though, cutting edge software development is technology driven, with developers defaulting to blockchain and manipulating the solution to fit, sometimes losing sight of the original problem in the process.

Inadvertent creation of a legally binding contract is the tip of the iceberg in managing the detail behind the application of distributed ledgers. Anonymity of public blockchains may conceal perpetrators of crimes. The irreversible nature of a blockchain transaction poses problems if an error is made in processing, which is common, or if a transaction is made under duress. Disintermediation may compromise checks and balances on the legal transfer of assets. There is also concern over the legal and fiscal jurisdiction under which a distributed ledger might operate. Recent articles on blockchain for the legal profession (Shooter & Nicholas Thompsell, 2017) and for the insurance industry (Lovells, 2017) address the challenges in more detail; other sectors will already be tackling similar questions.

Ethereum is a very flexible technology and is being widely explored; however, at the time of writing this article, very few dapps are fully launched, and there are a huge number in development (State of the Dapps). Projects proposed include voting platforms, multiplayer games, messaging, secure transportation of assets, social media, fine art sales, escrow services, music and media copyright management, and crowdfunding. To complicate matters further, Ethereum allows for the issue of monetary tokens within a dapp, and these are being used as a fast track to crowdfunding through *token sales,* also known as *Initial Coin Offerings*. Independent token sales are also gaining ground as a fundraising tool for businesses who are not using blockchain technology at all. Ethereum itself raised $18 million in the space of 42 days, and there are solid projects underway that have been funded by investors keen to see a return when the dapps are launched. The rapid development of these applications owes much to the easy availability of capital, and where the proposals are sound, this is advancing our understanding of the technology and its potential. However, if an idea is not sufficiently robust to attract the attention of traditional investors such as venture capitalists and banks, or to succeed in mainstream crowdfunding, a token sale can attract significant investment without the project having been rigorously or independently reviewed.

Authorities are rushing to impose regulation. In July 2017, the US Securities and Exchange Commission issued a report (2017) on a token sale by German organization "The DAO." Shortly following the sale, which reportedly raised $150 million, a flaw in the code allowed hackers to steal a third of The DAO's assets. Investments were somehow recovered and returned to participants, and the project abandoned. The report determined that the tokens offered for sale were securities under the Securities Act of 1933, and therefore should be regulated as such.

Applications of Blockchain Technology

Use cases of enterprise blockchains include not only supply chain management but also asset provenance, proof of ownership, secure storage of data, streamlined accounting processes, digital identity, government services, Internet of Things, and financial technology.

Digital Identity

Proving personal identity effectively has been a challenge for generations. Partial solutions for the physical confirmation of identity are applied piecemeal across the world. Crossing national borders generally requires an identity card or passport, some but not all of which may detail the holder's home address alongside their name, nationality, and birth details. Screening could also involve providing (in the author's recent personal experience) thumb prints, index finger prints, full sets of prints, retinal scans, facial recognition scans, contact details, and travel plans while in the country, or none of these. Within individual countries, identity cards may be either ubiquitous or absent, and the recording of births might be immediate and precise, or informal to the point that official documents routinely record birth dates as 1st January, in the absence of any detail other than the year of birth.

Digitally, there are multiple pseudo-identity systems allowing us to move seamlessly between software produced by individual providers, and often used to verify our identity with third party software. In 2016, Apple confirmed they had one billion active devices (The Verge, 2016), all attached to an Apple ID. Facebook's two billion users can "log in with Facebook" to multiple applications. Microsoft accounts control access to the whole suite of tools produced by the company. The landscape is messy and the accounts themselves are effectively anonymous, because users self-certify as real humans. Fake accounts proliferate. The technology to link accounts with services is good, but in situations where verification of account holder identity is genuinely required, for example in accessing taxation services or banking software, the process reverts to physical proofs.

It's a confusing picture, and one where control is centralized, and reams of personal data are vulnerable to hacking and theft.

Blockchain technology has the potential to deliver a single proof of identity with distributed verification. An individual's identity blockchain could begin with the registration of their birth, and incorporate life events such as vaccinations, qualifications, voter registration, and location changes as they occur. The records are immutable, data sources distributed, and there is no centralized control. In terms of security, although individual blocks may be accessed, the whole chain of information would not be visible. Currently, if an ID document is presented for proof of age, for example, it may also reveal place of birth and current address. Is that additional data required? Under principles of data protection and privacy, being able to reveal only the birth date block in a reliable record is preferable.

The United Nations ID2020 Project is developing a "personal, persistent, private and portable" distributed app (dapp) as part of its Sustainable Development Goals target to "provide legal identity to all . . . by 2030."

The first beneficiaries of this approach are likely to be the 20 million refugees among a billion people with no registered identity. This project is a perfect example of the type of large-scale international collaboration that will take advantage of the unique properties of a blockchain.

Government

Government and blockchain have been described as "a match made in heaven" (Donnelly, 2016). At the most public level, blockchain technology has the potential to eliminate electoral fraud and ensure that no citizen is disenfranchised. Work on digital identity aims to ensure that all those eligible to vote can do so, while maintaining anonymity in relation to the votes cast. In turn the votes can be recorded in an immutable form. A voting system that mimics this approach was implemented internally by a Danish political party in 2014, and there is a project in progress through the Bitcoin Foundation to develop a blockchain-based voting system (Pilkington, 2015). Within the government machine there is a need for increased accountability and transparency, which could be delivered by the same technology. Procurement systems, taxation, and other public services sitting in a permissioned blockchain would improve accessibility and transparency of process for participants: This is already being explored in the UK through both the Department of Work and Pensions and the G-Cloud procurement system (Merrett, 2016). Advances in blockchain technology rely upon support at the highest levels, and government interest in developing the use of DLT can only speed up adoption.

Internet of Things

The Internet of Things (IoT) introduces connectivity into everyday physical items, from smart kettles to intelligent buildings. There is a wealth of data being generated by these smart devices, which is analyzed in bulk, enabling informed decision-making and contributing to machine learning in the field of artificial intelligence. How could blockchain technology impact upon the IoT? The currently centralized ownership of data generated by smart devices is the main concern. There is a security risk with holding so much data, in terms of hacking, theft, and the resilience of the servers upon which the data resides. Distributed ledgers would reduce these risks considerably. Furthermore, the disintermediation of processes inherent in blockchain technology would streamline the collection of data, dropping transactional information directly to the ledger without need for a centralized authority. Several blockchain integrated IoT scenarios have been suggested by researchers (Huckle, Bhattacharya, White, & Beloff, 2016), bringing smart devices and smart contracts together to provide a seamless user experience. One of these scenarios follows a commuter journey, with a connected vehicle arranging the routing to refuel, while the blockchain confirms the identity and preferences of the driver and enables payment for the fuel as a smart contract without human intervention.

Accounting, Banking, and Finance

Accounting at its very heart is the recording of transactions with double entry verification, therefore blockchain is a very relevant technology. It mirrors the audit trail structure of accounting records, and the entries are immutable. The transparency of the records throws up a barrier to fraud, as auditors would be able to follow events clearly through all their related transactions. Furthermore, blockchains retain data transparency while preventing data theft in a form that is usable. Although the individual entries are visible and transparent, an outsider, or a hacker, would not be able to access other elements of the same chain without access to the algorithms that hash the data. Aside from recording transactions that occur in a business, the management of shareholders becomes more straightforward, clearly tracking who owns

what shares at any time, and allowing for responsibility to be distributed between the shareholder and enterprise to record share ownership in an accurate and timely manner.

The same applies to banking transactions. There is no reason why fiat currency could not be managed using a permissioned blockchain approach. There is no requirement to create cash, therefore no mining to be done, but the transfer of money and all related transactions can still be immutably recorded and confirmed by the distributed parties, i.e., the banks and the account holders.

Financial services provided by banks could also benefit from not only immutable records and distributed verification, but also smart contracts. One example is the existing system of documentary credit that reduces risk in import and export: Guarantees are issued by banks to ensure timely payment for goods that cross borders. The system is complex and costly. This could be replaced by a process whereby the transaction is electronically confirmed by distributed markers in a blockchain, and the system is set to release funds instantly at completion of the transaction. By streamlining export management and reducing risk, blockchains may smooth the path of business growth.

Supply Chain

The supply chain is a perfect example of a process waiting for a blockchain approach. Increased scrutiny of the origins of manufactured items, concerns for the environmental impact of the things that we use, and differing standards of health and safety, quality, or employment practices across the world, can be resolved by transparency and traceability. Potentially, every step of the way from raw material to finished product could be reflected in a blockchain. By tracking the provenance of components, ingredients, and materials, the purchaser can be sure that goods meet every relevant quality standard and that they are the genuine article. The potential to reduce counterfeiting and raise standards is significant. Combining a straightforward provenance chain with smart contracts smooths the cashflow of the participants, even across borders. The technology might even touch on the IoT, feeding data back to manufacturers for improvements to design and production. This application of blockchain technology is possibly the furthest advanced of all the use cases being explored, with multiple systems in active development and some at a stage of client readiness.

Data Security

A recurring theme in all of these applications has been data security. Data theft is a growing problem and is not likely to abate as the volume of stored data grows. What Bitcoin, blockchain, and discussions of security and regulation have brought to the fore is a reimagining of transparency and trust online. Prior to our submersion in the digital world, transactions relied upon personal trust and community transparency. With the spread of transaction participants across wider communities and even national borders, secrecy in the form of encryption replaced the natural order of trust. Unfortunately, the days of encryption are numbered. It is becoming increasingly easy to crack the layers of security around our data, and a combination of hacking, social engineering (phishing), and quantum decryption means we must explore new ways to keep personal data safe. The solution may exist somewhere between the two extremes of transparency and anonymity. Blockchains facilitate semi-transparency by protecting data in immutable records while allowing the tracking of transactions. A blockchain can be audited by third parties to ensure that everything is genuine, but the data cannot be tampered with. Even if data can be accessed and copied, the structure of the blockchain, unlike a normal database, means that only a fraction of the full picture is visible unless the algorithms behind the blockchain are known.

Practical Implications

Blockchain technology is a genuine game changer. The technology is powerful, but its true potential is far from being realized. It will, however, be massively disruptive. It is the gateway to changed behavior: disintermediated contracting, distributed responsibility, and common use of cryptocurrencies and tokens. There are more than 2,000 cryptocurrencies in circulation at the time of writing, with tokens taking on a value of their own as alternative currencies—some legitimate, others less so. Bitcoin, the leader of the pack, is rising in value as the concept of blockchain technology moves toward the mainstream. The eponymous native currency of Ethereum is tracking the movement of Bitcoin and is likely to gain ground as the dapps built on the Ethereum framework realize their potential.

Blockchain technology is not appropriate for re-factoring existing systems unless there is a genuine requirement for management of data, distribution of responsibility, immutability of records, or disintermediation of the transaction. Industry will not have time, at the current speed of development, to devote resources to the replication of current systems for the sake of it, in the way that word processors replaced typewriters but added very little functionality. Changes will be dramatic and disruptive. The disintermediation of processes will be a particular challenge for agencies, who will have to prove their worth as intermediaries in any situation. Agency business models will move away from brokerage and focus on delivering added value. Organizations holding large swathes of personal data will turn to the mathematical security of blockchain, both to adhere to increasingly strict data privacy requirements and to reduce the risk of damaging data theft. Collaboration and cooperation will increase as distributed responsibility for the validity of records becomes commonplace, and trusted relationships will be established thanks to the transparency of the technology.

Conclusions

Blockchain technology has enormous potential to disrupt business processes. In the same way that, when faced with the nascent internet in 1995, we were unable to conceive of something like social media, so we cannot predict the shape of the changes that will be wrought in our very near future. The accelerating pace of change means that over the next decade or so, blockchain technology is likely to evolve further than the internet did in the 20 years following the creation of the World Wide Web.

References

1. V. Buterin (2013) "A Next Generation Smart Contract & Decentralized Application Platform". http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf
2. D. Chaum, A. Fiat, & M. Naor (1988) "Untraceable Electronic Cash", *Advances in Cryptology CRYPTO '88*, S. Goldwasser (Ed.), Springer-Verlag, pp. 319-327.
3. J. Donnelly (2016) "Enterprise Blockchain Use Cases: eGovernment", Distributed magazine, p. 77. https://distributed.com/
4. S. Huckle, R. Bhattacharya, M. White, & N. Beloff (2016) "Internet of Things, Blockchain and Shared Economy Applications", *Procedia Computer Science*, Vol. 98, pp. 461-466. http://www.sciencedirect.com/science/article/pii/S1877050916322190
5. P. Jayachandran (2017) "The Difference between Public and Private Blockchain", *IBM*. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
6. HoganLovells (September 2017) "Blockchain/DLT in the Insurance Sector". https://www.hlengage.com/_uploads/downloads/5425Blockchainininsurance V7FORWEB.pdf
7. N. Merrett (July 2016) "Government Confirms Wider Blockchain Plans in the Pipeline", *Government Computing News*. http://central-government.governmentcomputing.com/news/government-confirms-wider-blockchain-plans-in-the-pipeline-4951569
8. S. Nakamoto (2009) "Bitcoin: A Peer-to-Peer Electronic Cash System". https://bitcoin.org/bitcoin.pdf
9. M. Pilkington (September 18, 2015) "Blockchain Technology: Principles and Applications", *Research Handbook on Digital Transformations*, edited by

F. Xavier Olleros and Majlinda Zhegu. Edward Elgar, 2016. https://ssrn.com/abstract=2662660
10. Securities and Exchange Commission Release no. 81207, July 25, 2017. https://www.sec.gov/litigation/investreport/34-81207.pdf
11. R. Shooter, & N. ThompsellFieldfisher (2017) "Blockchain". http://www.fieldfisher.com/media/5598374/blockchain-fieldfisher-insights-paper.pdf
12. The Verge (January 2016) "Apple Earnings Report". https://www.theverge.com/2016/1/26/10828134/apple-earnings-report-first-quarter-q1-2016-record-profit
13. "State of the Dapps" curated collection of Decentralized Apps for Ethereum. https://www.stateofthedapps.com/
14. UK Government Chief Scientific Adviser, 2016. "Distributed Ledger Technology: Beyond Block Chain". https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
15. United Nations "ID2020 Project". http://id2020.org/
16. Wei Dai (1998) "BMoney". http://www.weidai.com/bmoney.txt