cdbb
Centre for Digital Built Britain

Blockchain and Smart Contracts:
What the AEC sector needs to know

Kirsten Lamb, CDBB

July 2018
Series No. CDBB_REP_003
DOI: https://doi.org/10.17863/CAM.26272

UNIVERSITY OF CAMBRIDGE

Centre for Digital Built Britain

This is a working paper, published in the CDBB publication series.

Acknowledgements:

This research was funded by the Centre for Digital Built Britain (CDBB). www.cdbb.cam.ac.uk

Blockchain and Smart Contracts: What the AEC sector needs to know

Kirsten Lamb, CDBB

Blockchain has been heralded as a game-changing technology across multiple sectors. Indeed, its influence on the financial sector is already profound. (Tapscott & Tapscott, 2017) Its potential to streamline processes, manage identities and save money have given the technology a mystique that is perhaps enhanced by a lack of understanding about how it works by the general public. Many sectors are exploring whether it is worth pursuing, not least of which the Architecture, Engineering and Construction (AEC) sector.

This report covers the **BASICS OF BLOCKCHAIN** and how it can be deployed for **SMART CONTRACTS** and related project management processes. Then it looks at **BENEFITS** and **BARRIERS**, **MATURITY** of the technology, and early adopters. The report highlights some caveats about the technology as it pertains to the **AEC SECTOR**. The report is an overview of existing literature and presents the idea that blockchain technology is not yet mature enough to implement at a large scale, particularly when it has not been proven in any sectors that are similar to AEC. However, there are interesting small-scale trials to follow and the report highlights some suggestions for where **FURTHER RESEARCH** is needed. The report is followed by a **GLOSSARY** defining some of the key terms around blockchain technology.

Blockchain Basics

As with any new and potentially transformative technology, blockchain is little understood by many of the decision-makers considering whether to adopt it, exacerbated by the hive of related buzzwords swarming around it. Any explanation of blockchain must begin with unpacking some of the terms associated with it, so readers may benefit from consulting the glossary included at the end of this report. You will find any terms defined in the glossary written in **BOLD**.

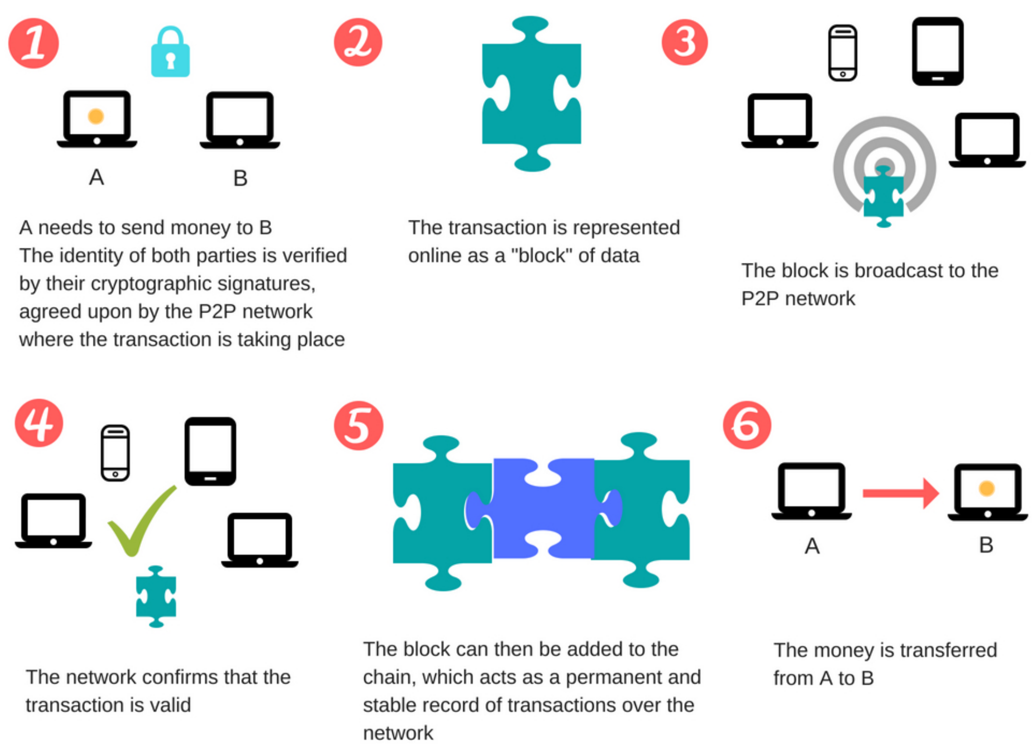
BLOCKCHAIN is the most prominent of several **DISTRIBUTED LEDGER TECHNOLOGIES (DLTS)**. It is closely associated with (and often confused with) the cryptocurrency **BITCOIN**. The process of Bitcoin production, known as "mining", is not considered relevant to this report, but to understand blockchain it will help to understand how it solves a key technical problem that enabled currencies such as Bitcoin to emerge.

Imagine you want to develop a currency that is not represented by any physical tokens, notes or coins but instead is digital-only (a **CRYPTOCURRENCY**). Since you want to control the amount in circulation, you might decide to use a unique encrypted file as the token that represents each unit of the currency. With physical currencies, each token, note or coin can only exist in one place at a time, so when someone spends a £20 note, that note is not duplicated but transfers to the recipient. With digital currencies, however, the token could be reproduced or falsified and committed to several recipients, a situation known as the double-spend problem. This duplication in turn would drive inflation and quickly diminish **TRUST** in the currency. Previous attempts and regulating this risk involved management by a single trusted third party, such as a bank, but this meant there was a single point of failure.

Blockchain was invented by a person or people under the pseudonym Satoshi Nakamoto in 2008 in order to solve the double-spend problem of cryptocurrencies without the need for a centralised server operated by a single party. By purportedly solving problems of identity, security and trust in digital transactions without the need to trust in a third-party, the developers were able to produce Bitcoin as the world's first decentralised currency and as a proof-of-concept. Blockchain has many other potential applications outside the world of digital currencies, including **SMART CONTRACTS** and supply chain management, financial asset management and data security. However, it is not a magic bullet and it is important to separate the hype from the application and performance of blockchain in order to understand whether it is a technology worth pursuing.

Blockchain and smart contracts

The term "smart contract" predates DLTs and refers to a contract that is fulfilled automatically. The originator of the term, Nick Szabo, likened a vending machine to a primitive form of smart contract; a customer requests a transaction by placing money into the machine and pressing the button corresponding to their choice. A simple if/then mechanism then fulfills the request by dropping the correct item into the tray for the customer to collect (Orcutt, 2018). In the era of blockchain, smart contracts are transactions that take place between verified parties, executed by computer code and vary widely in scale and complexity. The figure below outlines the process of executing a simple smart contract, the transfer of money from one party to another, using blockchain.



1. A transaction is requested and the request is sent to a Peer-to-Peer (P2P) network. These networks can be either public or private. The identities of the parties are verified. A transaction can involve contracts, records, building models, etc. However, currently only cryptocurrency is supported as a means of making payments over blockchain.
2. The data about this transaction is represented by a **BLOCK**.
3. The block is distributed to the P2P network.
4. The network validates the transaction via **CONSENSUS**-derived code.
5. The block can then be added to the blockchain, which acts as an unalterable record of transactions. Each node in the network (i.e. each individual server or computer) reflects the exact same version of this chain and if the data from a block is altered on one node, e.g. by someone attempting to commit fraud, this change is not propagated.
6. The transaction is completed and the contract fulfilled automatically.

With smart contracts, trust is distributed across a community on a P2P network rather than centralised. In other words, "No one can unilaterally take actions on behalf of the community" (Sun, Yan, & Zhang, 2016). Bulkin (2016) describes this idea of trustless trust in the context of an imagined cryptocurrency:

> *"In order for our digital monetary system to work, the recipient of a transaction must be able to confirm that:*

- *The originator of the transaction is in possession of the funds being transferred.*
- *The originator of the transaction has obtained the funds by one of the means commonly recognized as valid.*
- *As an outcome of the transaction the recipient will now be recognized by everyone as being in possession of the funds being transferred.*
- *As an outcome of the transaction the sender would not be able to present itself as being in possession of the funds anymore."*

These factors are programmed into the contract and agreed upon by the P2P network and describe a series of if/then dependencies: *if* the four conditions above are met, *then* the funds are transferred.

There are a number of configurations for blockchains depending on the access needs, according to Fitch Ratings (2018). A public blockchain would grant access to anyone upon what is known as **PROOF OF WORK** (PoW), conferring membership on anyone who contributes to the community. A private blockchain would roll back the decentralisation of blockchain and would confer authority over transactions and access on a single owner. A hybrid or consortium blockchain is any combination, often spanning organisations and entities that collaborate over the blockchain.

Benefits

The simplicity and immediacy of executing transactions across borders makes blockchain an appealing prospect to businesses. The technology reduces the need for intermediaries, manual identity checks, administration and waiting periods. Labour, duplication of effort, translation between different standards, data loss, and so on add up to make large, international or otherwise complex transactions expensive, so various organisations see blockchain as an opportunity to reduce costs. (Seetharaman, 2018) According to Cuccuru (2017), "At the end of the day, blockchains are nothing more than sophisticated accounting products, Bitcoin being just one—the first and the most popular—of the feasible applications. … Any digital asset, data or piece of information may be embedded in a blockchain and therein traded. Similarly, tangible properties may be digitally represented and securely registered into a decentralized ledger."

Blockchain has the potential to transform business information management, particularly around sharing information. Interoperability between business codes and information can be managed on the blockchain, allowing businesses to automate transactions without allowing competitors access to proprietary information (Nakasumi, 2017). Furthermore, by creating a stable, unalterable record of transactions, it has vast potential to make sectors with fraud and corruption problems more transparent and auditable.

In the case of supply chain management, using blockchain could allow businesses along the chain to establish quality of products using real-time data, leading to safer products, food and medicine making it to the market. "Quality data in production processes and inspection processes would be uploaded to and stored in blockchain. With the real-time quality data, process quality and product quality are evaluated in smart contracts and the results are sent back to suppliers, manufacturer and retailers." (Chen et al., 2017)

Finally, while it is potentially disruptive to existing business models it has the potential to "'automate away the center'", rather than putting blue collar workers out of their jobs. "'Instead of putting the taxi driver out of a job, blockchain puts Uber out of a job and lets the taxi drivers work with the customer directly.'" (Savelyev, 2017) It democratises transactions by enabling the community to agree on validation, identity checks and other parts of the process free from centralised authorities like banks, corporations and governments.

Barriers to smart contracts

A wide range of sectors have caught on to the transformative potential of blockchain. However, that potential is still unproven at scale and over time. There are many reasons to refrain from leaping too quickly onto the blockchain bandwagon without considering potential downsides and barriers to the adoption of the technology.

First, the cost reduction may be over-emphasised. According to Savelyev (2017), "It would not be correct to conclude that Smart contracts are cheaper than regular ones. Infrastructure necessary for implementation of Smart contracts and costs associated with the development ('drafting') of terms of Smart contracts are still rather high." The costs of paying people with the expertise to translate contractual language into code at both ends, working out interoperability standards and overhauling the energy and ICT infrastructure to the level needed for blockchain add up to a high price tag.

The cost of energy alone is a significant factor. Bitcoin has received attention lately for its staggering energy use, owing in large part to the computing power involved in "mining" the currency. However, energy, data storage and specialist support all contribute to high costs associated with blockchain as well, leading Bloomberg (2018) to argue that any cost savings in administration, legal and financial support are overhyped relative to reality. Blockchain itself could help make the energy grid more efficient in the future and offset some of this cost. (Chebbo, 2018) However, the demand for energy to support data storage, transfer and analytics is likely to grow in the face of IoT and connected devices. (Guardian, 2017) Therefore, the energy cost and environmental impact of blockchain relies heavily on the development of cleaner and more renewable energy sources.

Next, there is a significant skill gap in the workforce to overcome to make smart contracts a reality, and "competition for these skilled human resources will intensify as the technology takes hold" (Fitch Ratings, 2018). Knowledge about blockchain should not reside only with the specialists who write smart contracts but should exist among legal teams, IT and at the top levels of organisations as well. Leaders need to understand the actual potential, as well as the pitfalls, of the technology in order to exploit it appropriately.

There are technical issues that have not yet been resolved about this burgeoning technology. Despite its newness, blockchain seems to be falling victim to the same pitfalls of interoperability as many other technologies that promise interconnectedness and seamless data sharing. According to BisResearch (2017), "The fundamental flaw with the approach currently being applied to progress blockchain is that the organizations and companies are developing their individual blockchain networks. Multiple blockchain are being developed in the same industry in multiple standards, thereby fragmenting the members of the industry to different networks and stove-piping the information placed on the ledgers. This goes against the very purpose of distributed ledgers, fails to harness network effects." There are early signs of organisations recognising this problem and working to correct it, however. For example, "Certain consortiums and organizations such as R3, which consists of over 70 financial institutions, Financial Blockchain Shenzhen Consortium, and Blockchain Insurance consortium B3i are looking to circumvent this challenge by pushing industry stakeholders to work together."

Any data structure is only as good as the quality of the data it contains, however, and a 2016 study conducted on behalf of the State of Vermont concluded that data quality on the blockchain could not be guaranteed. They noted that despite its promise, at this point the economic value of the unproven technology was too speculative to be worth the cost of overhauling existing infrastructure when data quality could not be guaranteed. (Condos and Donegan, 2016)

Legal status of smart contracts

Currently smart contracts pose both a puzzle and a threat to experts in contract law. In theory, smart contracts remove the need for expensive legal and administrative staff in favour of encoding the parameters of a contract by a programmer. But when fulfilment of the contract is automated, is it still a contract in a legal sense? The strongest interpretation says that smart contracts are legally permissible "self-help" agreements outside of the "compulsion of law" or government intervention. After all, they are written in computer code, not legal language, and the language of contract law has not yet caught up with automated fulfillment by parties operating with distributed trust relationships. "Smart contracts are meant to be stand-alone agreements – not subject to interpretation by outside entities or jurisdictions." (Savelyev, 2017) Even so, there are a number of legal issues that arise from the existence of smart contracts that have not yet been tested against existing contract laws.

If/then logic seems to remove the fuzzy grey areas of natural language contracts, potentially reducing contractual conflicts. However, the programmer could misinterpret what the clients want, members of the P2P community could have unacknowledged disagreements over meanings, code can contain bugs and even the best encryption cannot prevent hacks. In a 2016 hack on one of Etherum's smart contracts, the hacker successfully acquired $47 million and later claimed in an open letter that he had simply exploited a bug, or, in his words, made use of an "'explicitly coded feature as per the smart contract terms.'" (Savelyev, 2017) The need of legislation to resolve these conflicts and protect the data and funds on blockchains is clear. But given the borderless and decentralised nature of smart contracts, the issue of jurisdiction is unclear. According to Savelyev, "Those jurisdictions which will have the most Blockchain-friendly regulations will have a competitive advantage in attracting new innovative business models and companies willing to exploit them in a legal way." That has to include data protection for blockchain.

A further hypothetical that has yet to be resolved goes as follows: if a transaction is completed on the blockchain, but then a dispute in court rules that one of the parties was threatened into paying, rendering the transaction null and void, the blockchain would reflect one version of the truth while the legal record would reflect another. Resolving this would mean putting in place some mechanism of altering the blockchain, such as the following:

> *"(1) To introduce the concept of a 'Superuser' for government authorities, which will have a right to modify the content of Blockchain databases in accordance with a specified procedure in order to reflect the decisions of state authority. (2) To enforce decisions of state authorities in 'offline' mode by pursuing the specific users and forcing them to include changes in Blockchain themselves as well as by using traditional tort claims, unjust enrichment claims, and specific performance claims."*

Option (1) is prone to abuse/manipulation if an individual can alter the record and (2) is inefficient and relies on offline modes of arbitration, jurisdiction and deanonymisation, both of which make blockchain less appealing. Users may develop their own consensus about how to resolve conflicts. (Savelyev, 2017)

Maturity

The maturity of blockchain technology varies from sector to sector. The financial sector is a global leader in adoption of blockchain technology for smart contracts. Its close association with cryptocurrencies such as Bitcoin notwithstanding, the financial industry is deriving value from blockchain as a machine-to-machine (M2M) technology that promises to reduce fraud and human error, reduce costs and reliably automate complex processes. The Bank of America holds the greatest number of blockchain related patents (Piplovic, 2018), demonstrating that it is not only for cutting-edge startups like Ethereum but can also benefit organisations with a longer history. The financial sector is the ideal testing ground for smart contracts according to Cuccuru (2017), because of the standardisation already present in the sector and the complex ledger and accounting system that is ripe for automation, meaning that inter-institutional and international interoperability is crucial.

Within the financial sector there are leaders and laggards. BisResearch (2017) predict the leaders in blockchain – those organisations who are expected to feel the impact of blockchain between 2017-2020 – to be P2P payments and loans, trade finance, digital identity management and private market trading.

The laggards – organisations that can expect impact from blockchain from 2025-onward – are likely to be insurance, cash equity trade settlement and repurchase agreements. It is not only private firms but also governments beginning to use blockchain to manage finances, identity, authentication and other forms of digital transactions. The table below outlines some of these early initiatives.

Adopters of distributed ledger technology

Category	Governments Using or Pursuing	Startups Offering
Antifraud	Singapore	
Authentication	Channel Islands	
Citizen payments	U.K.	
Contracts	Delaware (U.S.), Vermont (U.S.)	
Currency	The Philippines	
Energy and utilities		Bankymoon, EMS Invirotel Energy Management, Power Ledger
Identity	Estonia, U.S.	
Intellectual property rights		Open Music Initiative
Land titling	Honduras, Georgia (Republic)	
Notarization	Estonia	
Public safety	Australia	
Real estate	Sweden	
Records	Delaware (U.S.), Dubai, Vermont (U.S.), U.K.	
Registration	Isle of Man, Estonia	
Supply chain	Australia	
Voting	Denmark, Ukraine	Blockchain Technologies, e-Vox, Follow My Vote

Adapted from source: (Holgate, Furlonger, & Howard, 2018)

Because it enables a transparent chain of ownership, blockchain can also aid in accountability and quality management of real-world goods. Klappich et al. (2017) describe several nascent initiatives exploring the potential of blockchain for supply chain management. For example, the retail chain Walmart is trialing automated tracking of produce and pork from suppliers to stores, enabling faster recall of sub-standard products. Similarly, Toyota is considering a pilot to track parts between manufacturers and assembly points, again helping with recalls and with flexibility in the manufacturing process if particular plants are disrupted, e.g. by natural disasters. Luxury items could also benefit from blockchain-based management. IBM is working on a project called Everledger that is designed to track diamonds from mine to store. Encryption of luxury goods, e.g. art and fine wine, would reduce the possibility of counterfeits making it to market and if the information is made available to customers that could increase trust in their quality.

To predict how blockchain will evolve, it is essential to consider not only technological maturity but the maturity of standards, policy and legislation. While contract law has yet to catch up, a number of organisations are working on technical standards. W3C have developed working groups for blockchain, ISO have launched a committee on DLTs, "With liaisons with several other ISO committees and other relevant standards developing organizations", and the International Telecommunications Union (ITU-T), IEEE, Society for Worldwide Interbank Financial Telecommunication (SWIFZ) all have programmes looking at standards for blockchain. However, creation, development and curation is also driven from outside official standards channels by industry, trade and community organisations. Like the development of Bitcoin, "These are distinguished from the work of formal standards organizations by the fact that they are often accompanied by repositories of open source implementation code" (Anjum, Sporny, & Sill, 2017).

While numerous pilots exist in different sectors, ultimately blockchain is an unproven technology outside of the cryptocurrency context. Much of the hype about security has proven unfounded as cryptocurrency exchanges have been hacked multiple times, most recently to the value of £27.8m. (Kollewe, 2018) Indeed, despite blockchain’s reputation as the gold standard for security, a major breach with a huge financial cost is seen as inevitable in the next few years and the technology has only been deployed at a small scale. Horvath, Care, & Mahdi (2018) argue that standard cybersecurity advice still applies with blockchain: organisations should assess the risks of any project and have a plan in place for minor and major breaches.

Given the uncertainty, in is perhaps unsurprising that technology consultancy Garter "**believes that 90% of pilots will fail over the next 18 to 24 months.**" Until the technology can mature, conventional technology may be better, and some firms that are currently piloting blockchain technologies may be doing so out of misunderstanding their potential. (Klappich et al., 2017) Gartner believes that while blockchain has the potential to be disruptive or even transformative in the long term, it will not happen before 2023. "To fulfill its potential for disruption, blockchain needs further technology maturity and hardening, in addition to significant changes to business models, operating processes, societal constructs, and regulatory and governance mechanisms." (Smith & Plummer, 2018) There is the need for a holistic approach to smart contracts that includes business model transformation and adequate governance. As Pradhan, Stevens, & Johnson (2017) put it, "Full blockchain development could take five to seven years or longer, or may not occur at all. Early adopters who commit to testing blockchain across the supply chain must be prepared to accept significant levels of risk — and be prepared to fail fast and try again."

Smart contracts for the AEC sector

While opinion pieces abound telling how blockchain might transform construction, as yet there is relatively little academic literature on the intersection of BIM and smart contracts. Koutsogiannis & Berntsen (2017) highlight some advantages blockchain could present in the AEC sector. For example, automated if/then schemes could reduce the need for lawyers and administrators, saving time and cost. Blockchain encourages consensus, transparency, accountability and control, which could lead to better collaboration. Faster data sharing could mean quicker evidence-based decision making, especially across different stakeholders and workstreams, and information would be delivered to all parties real-time.

However, several barriers and drawbacks exist to smart contracts in AEC, not least because digitalisation in general is behind some other industries. "’We are talking about the least digitised industry where 95% of the produced data is thrown out of the window’, according to Klaus Nyengaard, chairman of GenieBelt. It is evident, then, that before we introduce smart contracts, for example, we have to build the right context that will accommodate them." Successful implementation in other sectors is not necessarily evidence that the technology will fit in the AEC sector and other technologies may be better suited to the culture. However, the potential of smart contracts is appealing; "They could be an amazingly useful element for construction if we get to a point where the generation of a building's real-time digital twin is an integral part of the construction process." (Koutsogiannis & Berntsen, 2017)

Because of this there are small-scale trials and projects already underway. Tozzi (2018) notes that blockchain is not infiltrating the AEC industry as quickly as others but that there are consortia and businesses devoted to applying the technology to construction. Bimchain.io, a French start-up, is among the first to develop a proof of concept for integrating BIM with blockchain through plug-ins with common BIM platforms and workflow tools. "The aim is to create a new collaborative process that bridges the gap between 3D digital modelling and the formal and legally binding paper-based processes related to project administration, building control, insurance and payment," in other words to manage BIM through smart contracts. The company's CEO observes, "One of current challenges with BIM is to achieve a high level of quality, which a fully contractual 3D model, filled with validated and certified data, can enable." (Cousins, 2018)

Thomson (2018) argues that portions of AEC sector contracts are well suited to blockchain and could be embedded within a BIM model that is managed and secured by blockchain. "The 'smart construction contract' would combine a traditional construction contract and reference the self-executing portions of itself that have been coded into the BIM model." In addition to facilitating access to the model by all project partners, blockchain could manage funds available, release payments on fulfillment of obligations and, "Automatically and securely transmit data regarding the project and its progress to relevant stakeholders and third parties, such as lenders, insurers and governmental authorities."

In the academic literature, Turk & Klinc (2017) note that the scale of information used in BIM for a single project is much smaller than Bitcoin and therefore the architecture used can vary depending on the need. They suggest four possible models:

1. Decentralised database: Building information is copied onto a standard blockchain.
2. Slightly decentralised: "It would appear to the client that a file is local while in fact it would be pulled from the blockchain and cached locally if and when needed. At least one project partner would need to host the blockchain and every project partner that would want to have it could have it" in order to deal with scalability.
3. Unchained: Metadata but not files themselves are stored in the blockchain. "All members of the project could have a copy of the blockchain – proof that a certain file existed at some point; they would also have a possibility to prove that the file is the one whose fingerprint is in the blockchain. However, it would be left to other software to guarantee that all the files mentioned in the blockchain would be preserved somewhere."
4. Integrated with a BIM server.

In their paper they outline a proposed architecture for number 4 as well as a flowchart for helping select which option is appropriate.

Despite its promise, the fact remains that none of these models have been tested at scales and in contexts that provide a good demonstrator for the AEC sector. Any early adopters in this sector should enter into blockchain experimentation with both eyes open and if blockchain is likely to form part of the information architecture underlying digital built Britain, the requisite investment in research, passing of regulations and transformation of business models should commence sooner rather than later.

Further research

If blockchain as a technology is unproven for the purposes of BIM smart contracts, what research is needed to prove it? Yli-Huumo et al. (2016) point out several capability gaps that, if explored, will help facilitate the scalability of blockchain, including: latency, throughput, bandwidth, versioning, multiple forks and usability. They found in a review of the literature that Bitcoin was over-represented relative to studies that apply blockchain to other problems. Security was another key issue they pointed out. Although there is already a strong body of literature on this topic, as blockchain matures so will the effectiveness of attackers, and so continuing research on security and resilience of blockchain systems will help overcome problems on the horizon.

Alharby & van Moorsel (2017) re-iterate the need for research to support scalability, as well as the need to explore other applications for smart contracts outside of financial sectors. There is a lack of research on blockchain platforms other than Ethereum, which is to better understand their pros and cons for different contexts. There is little research on social factors, such as criminal activities in smart contracts, and addressing this gap would be important to increasing trust in the technology and understanding the human impacts of implementation.

At present, all of the supporting infrastructure that would enable integration between blockchain and other current systems are underdeveloped. "Improvements addressing confidentiality, strong identity, and collaboration between the blockchain network participants will be required in near future... and associated standards and tools will be required for developing, debugging, monitoring, and managing smart contract systems." (Anjum et al., 2017) If blockchain is needed to help with smart monitoring of BIM databases, developing those capabilities may be essential prerequisites before using blockchain in the AEC sector. (Turk & Klinc, 2017)

Beyond any technical issues, it is essential that policies and standards are in place that protect individuals' rights and ensure legitimate transparency before moving forward. Decision makers need to understand the potential pros and cons of the technology and build policies with blockchain in mind. Failure to do so before implementing blockchain would result in a case of the cart leading the horse, with potentially disastrous.

Glossary

BLOCK A unit of data about a transaction.

BLOCKCHAIN A data structure formed of **BLOCKS** arranged in an ordered list.

CONSENSUS Changes to a **LEDGER** must be agreed by all parties on the network. This agreement can be reached by using "proof of computation to randomly select a node which single-handedly decides the next operation" as with Bitcoin mining, or by using "communication based protocols in which nodes have equal votes and go through multiple rounds of communication to reach consensus" (Dinh et al., 2018).

Cryptocurrency "A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank." (Oxford Dictionaries, 2018) Bitcoin is the most well-known example of a cryptocurrency.

Distributed Ledger Technology (DLT) - A class of data structures characterised by **ledgers** that are shared among a network where each node in that network reflects the same version of record.

Encryption Ensuring security of **DLTs** involves multiple types of encryption. First, the architecture of a **blockchain** itself is based on existing cryptographic information architectures. Second, the historical record of the blockchain is protected since the **blocks** that are added cannot be altered later. **Trust** in the **ledger**, which in turn drives the value of **cryptocurrencies**, for example, requires trust in the quality of encryption used and its ability to detect fraud.

Identity management Users of **blockchain** are identified by their own encrypted key or signature. This ensures that only verified parties are conducting transactions, ensuring **trust**. The techniques for generating and managing user keys varies between public and private **ledgers**.

Ledger "A ledger is a data structure that consists of an ordered list of transactions. For example, a ledger may record monetary transactions between multiple banks, or goods exchanged among known parties." (Dinh et al., 2018)

Proof of Work (PoW) In order to prevent denial of service attacks and other abuses, membership of a **blockchain** P2P network is regulated through Proof of Work or Proof of Stake, evidence that large amounts of computing power have been set aside to solve complex problems.

Smart contract "Computer protocols which formalize the elements of a relationship and automatically execute the terms therein encoded once pre-defined conditions are met." (Cuccuru, 2017)

Trust In the context of **blockchain** and **smart contracts**, trust is not placed in a centralised authority but is built by **consensus** through **encryption** and **identity management**. Therefore, smart contracts are built on what is referred to as "trustless trust", where automated systems replace the need for interpersonal trust.

Blockchain and Smart Contract Startups

- Bimchain.io: sign your contracts directly from the model, and go paperless. (France)
- Brickschain: Blockchain for Construction and Facilities Management. (USA)
- Data Gumbo Corporation: Data Gumbo provides blockchain based smart contracts to automate incentive contracts in the oil and gas industry (USA)
- DFINITY: Building an open, decentralized blockchain that runs smart contract software with vastly improved performance, capacity, and governance. (Switzerland)

- Ehab: A blockchain based platform which connects people, developers & the crowd to create sustainable homes & livable smart cities. (UK)
- ubirch GmbH: With the Blockchain for Things we are offering a stack to make IoT Things (actors, sensors) part of a blockchain. (Germany)
- YINC: Leverages Blockchain technology to transform the service-to-hire industry for consumers & real estate management companies. (USA)

Bibliography

- Alharby, M., & van Moorsel, A. (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study. *ArXiv:1710.06372 [Cs]*, 125–140. https://doi.org/10.5121/csit.2017.71011
- Anjum, A., Sporny, M., & Sill, A. (2017). Blockchain Standards for Compliance and Trust. *IEEE Cloud Computing*, *4*(4), 84–90. https://doi.org/10.1109/MCC.2017.3791019
- BisResearch. (2017). *Blockchain Technology in Financial Services Market - Analysis and Forecast: 2017 to 2026*.
- Bloomberg, J. (2018). Don't Let Blockchain Cost Savings Hype Fool You. Retrieved 26 June 2018, from https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/
- Bulkin, A. (2016, May 3). Explaining blockchain — how proof of work enables trustless consensus. Retrieved 26 June 2018, from https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845
- Chebbo, M. (2018). Powering a sustainable future: how blockchain can solve bitcoin's energy consumption crisis. Retrieved 26 June 2018, from https://www.itproportal.com/features/powering-a-sustainable-future-how-blockchain-can-solve-bitcoins-energy-consumption-crisis/
- Chen, S., Shi, R., Ren, Z., Yan, J., Shi, Y., & Zhang, J. (2017). A Blockchain-Based Supply Chain Quality Management Framework. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)* (pp. 172–176). https://doi.org/10.1109/ICEBE.2017.34
- Condos, J., Sorrell, W., & Donegan, Susan. (2016). *Blockchain technology: opportunities and risks* (Government report). State of Vermont. Retrieved from https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf
- Cousins, S. (2018). French start-up develops Blockchain solution for BIM | BIM+. Retrieved 26 June 2018, from http://www.bimplus.co.uk/news/french-start-develops-blockchain-solution-bim/
- Cuccuru, P. (2017). Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology*, *25*(3), 179–195. https://doi.org/10.1093/ijlit/eax003
- Fitch Ratings. (2018). *Blockchain and Insurance - The Trust Machine*. London: Fitch Group.
- Guardian Environment Network, & Network, part of the G. E. (2017, December 11). 'Tsunami of data' could consume one fifth of global electricity by 2025. *The Guardian*. Retrieved from http://www.theguardian.com/environment/2017/dec/11/tsunami-of-data-could-consume-fifth-global-electricity-by-2025
- Holgate, R., Furlonger, D., & Howard, R. (2018). Toolkit: Government Use Cases for Blockchain. Retrieved 22 June 2018, from https://www.gartner.com/document/3615119?ref=solrAll&refval=205068957&qid=c8b41438b531b274d39c3961548eab96
- Horvath, M., Care, J., & Mahdi, D. A. (2018). Evaluating the Security Risks to Blockchain Ecosystems. Retrieved 22 June 2018, from

https://www.gartner.com/document/3869088?ref=solrAll&refval=205068957&qid=c8b41438b531b274d39c3961548eab96

- Klappich, C. D., Tohamy, N., Johnson, J., & Stevens, A. (2017). Seven Things That Supply Chain Leaders Need to Know About Blockchain. Retrieved 22 June 2018, from https://www.gartner.com/document/3620517?ref=solrAll&refval=205068957&qid=c8b41438b531b274d39c3961548eab96
- Kollewe, J. (2018, June 11). Bitcoin price plunges after cryptocurrency exchange is hacked. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck
- Koutsogiannis, A., & Berntsen, N. (2017). Blockchain and construction: the how, why and when. Retrieved 26 June 2018, from http://www.bimplus.co.uk/people/blockchain-and-construction-how-why-and-when/
- Nakasumi, M. (2017). Information Sharing for Supply Chain Management Based on Block Chain Technology. In *2017 IEEE 19th Conference on Business Informatics (CBI)* (Vol. 01, pp. 140–149). https://doi.org/10.1109/CBI.2017.56
- Orcutt, M. (2018). Ethereum's smart contracts are full of holes. Retrieved 27 June 2018, from https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/
- Piplovic, N. (2018, January 16). The Leader in Blockchain Technology Patents Is Not Who You Think It Is. Retrieved 20 June 2018, from https://www.stockinvestor.com/32256/leader-in-blockchain-technology-patents/
- Pradhan, A., Stevens, A., & Johnson, J. (2017). Supply Chains Are Racing to Understand Blockchain — What Chief Supply Chain Officers Need to Know. Retrieved 22 June 2018, from https://www.gartner.com/document/3823374?ref=solrAll&refval=205068957&qid=c8b41438b531b274d39c3961548eab96
- Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036
- Seetharaman. (2018, March 14). The Cost-Cutting Potential of Blockchain. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/the-cost-cutting-potential-of-blockchain-1520993100
- Smith, D. M., & Plummer, D. C. (2018). Measuring the Impacts of Digital Disruption: Populating Gartner's Digital Disruption Scale. Retrieved 22 June 2018, from https://www.gartner.com/document/3871147?ref=solrAll&refval=205071451&qid=586dd0d792b53bb99d48d0ebc7328ab8
- Sun, J., Yan, J., & Zhang, K. Z. K. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financial Innovation*, *2*, 26. https://doi.org/10.1186/s40854-016-0040-y
- Tapscott, A., & Tapscott, D. (2017, March 1). How Blockchain Is Changing Finance. Retrieved 17 July 2018, from https://hbr.org/2017/03/how-blockchain-is-changing-finance
- Thomson, M. (2018). BIM, Blockchain and the Smart Construction Contract. Retrieved 26 June 2018, from https://www.lexology.com/library/detail.aspx?g=a94913aa-9135-4547-a5e4-5a114dc3d502
- Tozzi, C. (2018, May 1). How Blockchain Innovation Can Help Cost-Efficiency in the Construction Industry. Retrieved 26 June 2018, from https://www.nasdaq.com/article/how-blockchain-innovation-can-help-cost-efficiency-in-the-construction-industry-cm956525
- Turk, Ž., & Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management. *Procedia Engineering*, *196*, 638–645. https://doi.org/10.1016/j.proeng.2017.08.052

- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE*, *11*(10). https://doi.org/10.1371/journal.pone.0163477