Blockchain Technology

How the Inventions Behind Bitcoin are Enabling a Network of Trust for the Built Environment

ARUP

About Arup

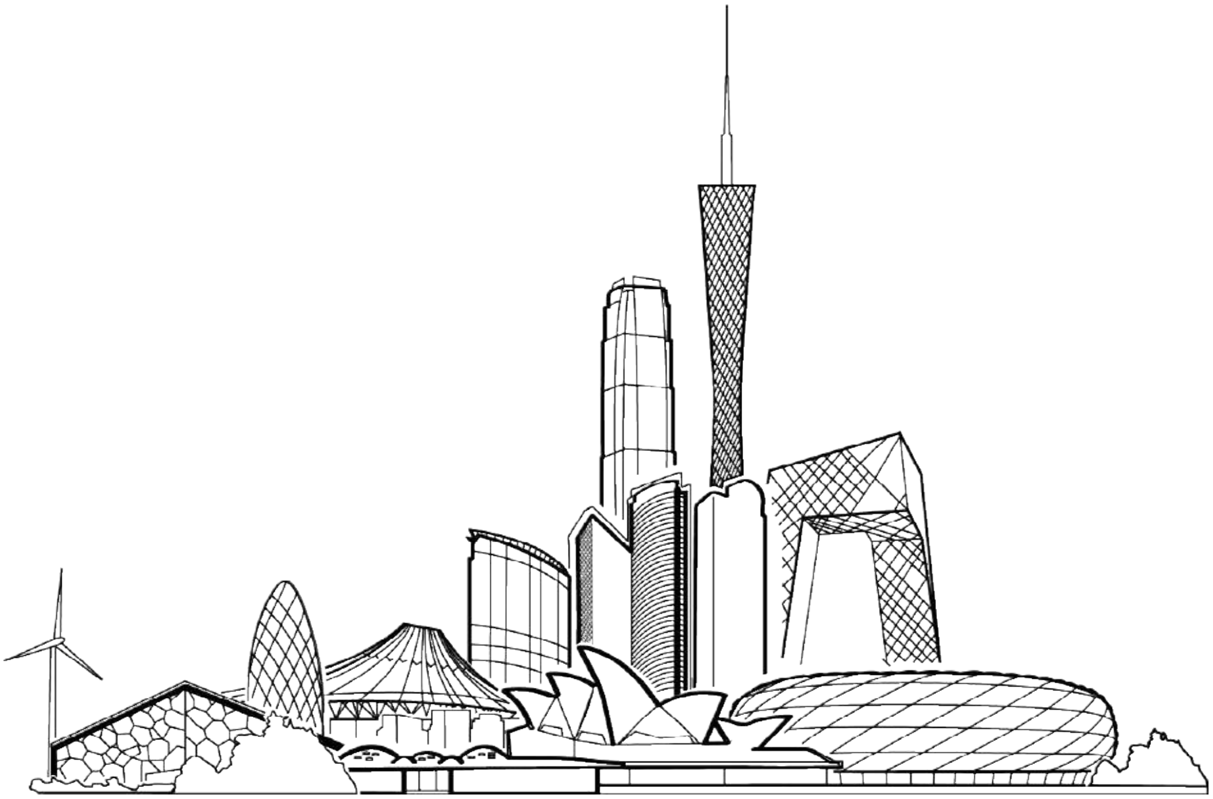
Arup is a global design and consulting firm offering a broad range of professional services for the Built Environment: from technical design in individual specialist disciplines to complex multidisciplinary projects.

Founded in 1946 by Sir Ove Arup, the company gained international recognition with its creative contributions to landmarks such as the Opera House in Sydney and the Centre Pompidou in Paris. Today 13,000+ employees in 90 offices in over 40 countries work for Arup. Designers, engineers, architects and consultants — united under one roof — develop concepts which stand for quality, innovation, creativity and sustainability. Arup's unique trust ownership structure means our people are free to pursue the firm's vision rather than chase short-term shareholder returns.

About Foresight

Foresight is Arup's internal think-tank and consultancy which focuses on the future of the Built Environment and society at large. We help organisations understand trends, explore new ideas, and radically rethink the future of their businesses. We developed the concept of 'foresight by design', which uses innovative design tools and techniques in order to bring new ideas to life, and to engage all stakeholders in meaningful conversations about change.

We shape a better world.



ARUP

13 Fitzroy Street
London WIT 4BQ
arup.com

Contents

About the Authors

Christopher Kinnaird

Buildings Scotland
B.Sc. Computer Aided Design
Certified Bitcoin Professional
Certified Blockchain Expert

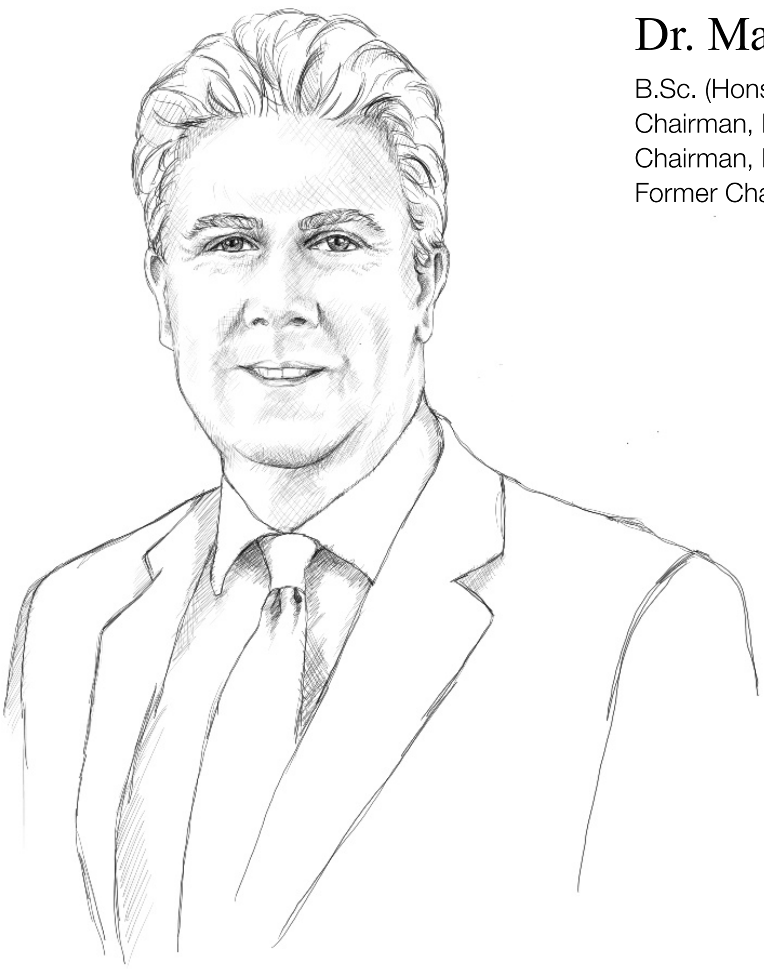
Chris has been with Arup's Buildings team in Scotland for over a decade. His long-time interest in politics and economics eventually led him to Bitcoin in 2013. He has since invested great effort into understanding and following the silent socioeconomic revolution being brought about by the Bitcoin blockchain. Chris is convinced that the blockchain is not only here to stay, but that it can radically transform the Built Environment for the better, by becoming the platform that allows the Internet of Things to become a reality, which paves the way for a Circular Economy.

Matthias Geipel

Advisory Services, Berlin
B.Sc. Applied Computer Science / Facilities Management
Project Management Associate
Certified Bitcoin Professional
Certified Blockchain Expert

Matthias started working for Arup's Advisory Services Team in 2010. Two years later he learned about Bitcoin and was immediately overwhelmed by the concept and what it implies. Since then he has been a strong advocate of the technology and still sees Bitcoin's blockchain technology as a game changer for the Built Environment, businesses and society.

Foreword



Dr. Mark Bew MBE

B.Sc. (Hons) Computer Science
Chairman, Digital Built Britain
Chairman, PCSG
Former Chairman, BuildingSmart UK

Mark has a track record of delivering successful process and technology driven business change programs from within the Engineering and Construction industry. He trained in the defence industry and has worked at Laing, Costain and Scott Wilson where he served as CIO and is currently Chairman at PCS Group.

He chaired the development of the UK Government BIM Strategy which was published in July 2011 as part of the Government Construction Strategy. He is Chair of Digital Built Britain which is the organisation tasked with the delivery of the Government's industry digitisation programme.

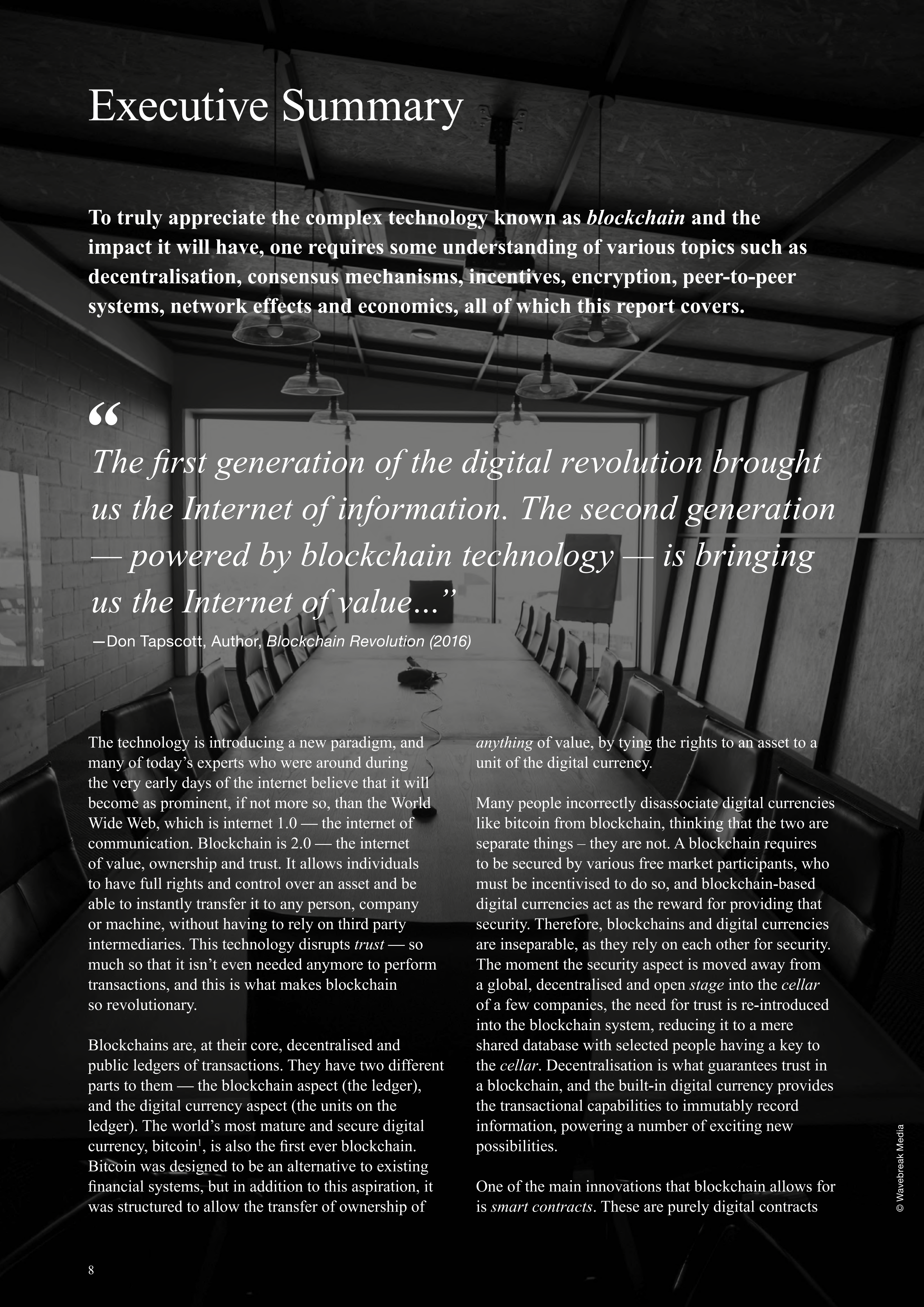
Mark is a Chartered Engineer with strong technical and commercial skills; he has a BSc (Hons) in Computer Science and a PhD in the fusion of Digital Engineering (BIM) data and Social Science. He is a Fellow of the Institution of Civil Engineers and Royal Institute of Chartered Surveyors as well as a member of the British Computer Society. Mark was awarded the MBE for services to construction in 2012.

The Built Environment delivery, operation and service provision sectors are the last bastion of old analogue methods and traditions. The sector is characterised by fragmentation, low margins and unpredictable performance. Over the last five years interventions by a number of Governments led by the UK have seen the first tentative steps in digitisation through the use of Building Information Modelling (BIM) technologies.

BIM has shown us that it is possible to create useful structured data which describes brief, design, manufacturing and operational scenarios. However, the sector is limited by the existing data processing and exchange methods which remain characterised by analogue methods that support old adversarial behaviours. For the last two decades, the sector has tried to apply the collaboration mantra. But at the end of the day, when the chips are down, it is the contract that shapes behaviours and outcomes. So, how do we go forward? What is the solution to complex data transactions where openness, transparency, honesty and immutability are the basic foundations?

Enter Distributed Ledger and blockchain, with the promise of permanent, secure and valuable transaction methodologies. For the first time a technology has the potential to provide an effective solution, but how do we apply them? What are the challenges and where do we start? The workshop hosted by Arup described in this document has provided a useful start to what is likely to be a long journey to begin to understand how these technologies may be applied to the challenges posed by the Built Environment. I encourage you to use this as a first step to what could be a very exciting journey.

Executive Summary


© Wavebreak Media

To truly appreciate the complex technology known as *blockchain* and the impact it will have, one requires some understanding of various topics such as decentralisation, consensus mechanisms, incentives, encryption, peer-to-peer systems, network effects and economics, all of which this report covers.

> “
> *The first generation of the digital revolution brought us the Internet of information. The second generation — powered by blockchain technology — is bringing us the Internet of value...”*
>
> —Don Tapscott, Author, *Blockchain Revolution (2016)*

The technology is introducing a new paradigm, and many of today’s experts who were around during the very early days of the internet believe that it will become as prominent, if not more so, than the World Wide Web, which is internet 1.0 — the internet of communication. Blockchain is 2.0 — the internet of value, ownership and trust. It allows individuals to have full rights and control over an asset and be able to instantly transfer it to any person, company or machine, without having to rely on third party intermediaries. This technology disrupts *trust* — so much so that it isn’t even needed anymore to perform transactions, and this is what makes blockchain so revolutionary.

Blockchains are, at their core, decentralised and public ledgers of transactions. They have two different parts to them — the blockchain aspect (the ledger), and the digital currency aspect (the units on the ledger). The world’s most mature and secure digital currency, bitcoin[1], is also the first ever blockchain. Bitcoin was designed to be an alternative to existing financial systems, but in addition to this aspiration, it was structured to allow the transfer of ownership of *anything* of value, by tying the rights to an asset to a unit of the digital currency.

Many people incorrectly disassociate digital currencies like bitcoin from blockchain, thinking that the two are separate things – they are not. A blockchain requires to be secured by various free market participants, who must be incentivised to do so, and blockchain-based digital currencies act as the reward for providing that security. Therefore, blockchains and digital currencies are inseparable, as they rely on each other for security. The moment the security aspect is moved away from a global, decentralised and open *stage* into the *cellar* of a few companies, the need for trust is re-introduced into the blockchain system, reducing it to a mere shared database with selected people having a key to the *cellar*. Decentralisation is what guarantees trust in a blockchain, and the built-in digital currency provides the transactional capabilities to immutably record information, powering a number of exciting new possibilities.

One of the main innovations that blockchain allows for is *smart contracts*. These are purely digital contracts

> *“Imagine a world in which all people can trust each other.”*
>
> —Nicolas Cary, President & Co-founder, Blockchain

that can mimic the terms of traditional contracts, but are enforced by computer code. They could provide many benefits to businesses in the Built Environment sector, such as contract dispute reduction through automation, decentralised cloud computing for vastly improved data security, and automated administrative tasks and audits to reduce business operating costs.

Even more disruptive use cases for smart contracts include providing the micro-transaction and security requirements to enable the Internet of Things and the machine economy to become a reality, enabling live BIM models; solving intellectual property issues; and forming the foundation of disruptive new types of companies called Decentralised Autonomous Organisations (DAOs). These are corporations that exist solely as computer code in the cloud, and are impervious to conventional regulation as they are stateless. They could have massive implications for the future of corporate structures, and even how society operates and organises itself.

The blockchain industry, mainly via Bitcoin, has been disrupting the financial sector for a few years now, and a number of companies and groups are creating their own versions, many with the goal of replicating Bitcoin’s success. Most of them since 2015 have begun with *Initial Coin Offerings* (ICOs), which allow their creators to sell tokens to fund the development of their products. Most ICOs today exist on the Ethereum blockchain, and some accommodate their core business functionality in around 40 lines of code.[2] This has led to a frenzy of activity, with new tokens flooding the market by the day, possibly resulting in this industry’s version of the dotcom bubble. This has not gone unnoticed, and every major bank in the world is now studying blockchain technology to ascertain the potential impact for them, and the Built Environment sector is just beginning to follow suit.

Successful blockchains, ICOs and smart contracts are reliant on the quality and robustness of the underlying code, which if poorly executed, runs the risk of being exploited by hackers. For example, Ethereum’s DAO[3] lost millions in user funds following an attack. The best blockchains are those that are built and maintained by global teams with developer numbers in the hundreds, who are experienced in creating secure, peer-reviewed computer code.

The industry is growing at a rapid pace, and has garnered serious attention and participation from leaders in key sectors such as business, venture capital, and regulation. The latter has been creating legislation in a number of jurisdictions around the globe, hoping to ensure safeguards for users whilst not stifling innovation. This has increased confidence for the future of the blockchain space.

It has become clear that this technology is here to stay. Therefore, it’s fair to say that blockchain will come to have a major impact on the Built Environment, as well as many other industries, in the same kind of way the World Wide Web did. It will have a profound effect on society, as it creates a global *network of trust*, allowing individuals, organisations and even machines to transact with each other, *but — for the first time in history — without having to trust each other*. Those who harness the power of a blockchain’s decentralised, secure, immutable and transparent properties, can really help to *shape a better world* for everyone.

This report was informed by a two-day Arup Explores workshop hosted by the authors in Arup’s Berlin office in early 2017. Participants included leading experts from Deloitte, PwC, Volkswagen Financial Services, the Ellen MacArthur Foundation, Arup experts from the Legal and Consulting fields, and Dr. Mark Bew MBE, Chairman of the UK Government’s Digital Built Britain strategy.

© Rafael Matsunaga

Introduction

At the start of 2009, when the world was in the middle of a major financial crisis, a paradigm shift in technology quietly made its debut. That technology is called Bitcoin, and it's the biggest innovation in finance in 500 years, and certainly the greatest invention of the 21st century so far.

> *"Basically, Bitcoin is among the greatest inventions in history, and the rest of us need to mainly focus on trying to understand what that could mean for different fields rather than complaining about this or that mostly imagined problem."*
>
> —Konrad S. Graf, Bitcoin Theorist

Bitcoin can be defined as having three main attributes: a *digital currency*, a *digital asset*, and a *trust network*. It's been in the media a fair amount over the years mainly because of those first two properties. The digital currency aspect allows anyone, anywhere, to digitally send money to anyone else in the world almost instantly, and this has captured the attention of the financial industry. As a digital asset, Bitcoin has a limited supply and is therefore a store for value, which has made it popular with investors and led to it being dubbed 'digital gold'.

However, it is the notion of Bitcoin as a trust network (or blockchain technology) — that is of particular interest to the Built Environment sector. It allows for many incredible technological use cases that simply were not possible before, and they have the potential to transform the industry in many different ways.

Blockchain technology could disrupt supply chains, with live tracking of goods and materials, simple authentication, and paperless records being just a few examples of the benefits. Major container shipping companies are now testing the technology to identify potential improvements to their administrative operations and costs.[4]

This report outlines the implications of the potential future convergence of blockchain, the Circular Economy, BIM and the Internet of Things, with an idea the authors have dubbed 'The Blockchain of Circular BIM Things'. This explains how blockchain technology can provide the bulletproof security and transaction capabilities required to ensure that the Internet of Things can take off in a meaningful way, which in turn would allow a Circular Economy to flourish. The benefits for BIM could be incredible, including the potential to digitally link model components to their physical counterparts. This could allow for *live* BIM models, whose components could continuously be fed usage data from the real buildings throughout their operation.

© Jason Benjamin

This can shift BIM models from being ‘As Built’ to ‘As Is’, meaning that instead of embedded information ceasing to update at the end of the construction stage, it would evolve during in-use and re-use stages. This could make BIM models the main source of Circular Economy related information in terms of buildings, which could transform the way they are managed and operated.

Another major use case for blockchain in an engineering context would be the adoption of a digital currency designed specifically for the sector. The first example of such a currency, known as *Quant*, allows engineers to connect on a global level, and provide assistance to one another when required. Any information that engineers produce for projects, such as specification documents or case studies, can be added to Quant’s blockchain using smart contracts, which automatically creates new Quant currency units. **The currency’s value would therefore be backed by the knowledge, skills and experience of engineers**. Individual pieces of engineering information would become commoditised, allowing external collaborators on a project, such as clients, to quickly and easily pay for specific information. This can open up a plethora of possibilities in terms of fee structures and the potential for engineers to gain additional rewards for their important contribution to projects and society.

This report also explores major aspects of blockchain technology such as smart contracts and the legal benefits and implications, as well as use cases outside of the Built Environment sector that demonstrate its potential across multiple industries.

The authors of the report have hidden a small blockchain bounty on one of the pages. Anyone can claim this free money and move it to an address that you own. First come, first served. Good luck!

© Rick Turoczy

What is Blockchain Technology?

Almost unknown[5] before the year 2015, 'blockchain technology' is now far more mainstream, and widely used[6] by businesses and governments around the world. Many are still in an exploratory or learning phase, some are working on solutions to real-world problems, others are even creating solutions to problems that don't exist.

To understand what blockchain technology is, it is first necessary to know where it comes from, what *blocks* and *chains* are, and what properties a *viable* blockchain consists of.

A Simple Explanation

A blockchain is a ledger of digital transactions, but instead of being centrally located and controlled, as most databases are today, it is decentralised and not under the control of any single individual, group or company. The technology is structured in this way to make it extremely difficult to change the rules that define the structure of a database or its content without consensus amongst the people who use it.

A blockchain processes transactions on its database in a similar way to entries in a physical ledger, around every ten minutes transactions are assembled into small groups, called *blocks,* like new pages in a physical ledger. Newer blocks are linked to older ones, forming a *chain*, hence the term *blockchain*. This structure ensures that the database can only have entries added, data can never be changed or removed because changing a single entry in an older block would mean rewriting the entire history of transactions subsequent to that block.

This *immutability* is critical to the functioning of any blockchain and is what differentiates them from traditional databases.

Tampering with the blockchain is almost impossible as any change is immediately recognized by all other participants, followed by a rejection by the network. The only way to manipulate existing entries in the ledger, for example to spend an asset twice, would be to manipulate the ledger across the entire network, almost simultaneously. There are various ways that blockchain technology prevents this from happening, the most common and widely used technique is to require some form of computational work before data can be added to the ledger.

The Origins

Blockchain technology, although not named as such at the time, was presented to the world in a whitepaper, in 2008, which outlined its use in the digital peer-to-peer currency system, Bitcoin. Bitcoin is a form of network protocol, like HTTP or TCP layers that underpin global internet infrastructure and used every time we browse the World Wide Web.

Intriguingly, the white paper was published by Satoshi Nakamoto, a pseudonym for a person, or a group of people, who remain unknown. The code running the Bitcoin protocol is open source, meaning that anyone who understands the code can see what it does and how it does it, so there is no need to identify or trust the inventor.

The first application of the Bitcoin protocol was the digital currency called bitcoin (lower case 'b'). This invention finally solved a problem[7] computer scientists had been trying to solve for years — how to create a digital asset that cannot be copied. This is crucial for creating any (digital) currency because it too should not be allowed to be copied or produced "out of thin air".

For the first time in history, it was possible to create a truly global economy, based on a decentralised, immutable and permissionless ledger, simply accessed via either a connected computer or an SMS-enabled mobile phone.

> *“…anything of value — money, but also titles, deeds, identities, even votes — can be moved, stored and managed securely and privately. Trust is established through mass collaboration and clever code rather than by powerful intermediaries…”*
>
> —*Blockchain Revolution*, Don and Alex Tapscott, 2016

The Consequences

Blockchain has attracted broad interest from various groups, businesses, industries and governments. The idea of an open, distributed ledger of transactions is highly apolitical and transparent. However, it is also highly controversial and threatens to wrest control over bookkeeping and record keeping from individual institutions, which explains why the financial industry initially dismissed the technology, then moved to try and better understand its implications. Other industries, including the Built Environment, are now coming to understand how the technology might impact on them and making inroads to explore it.

How Blockchain Technology Works

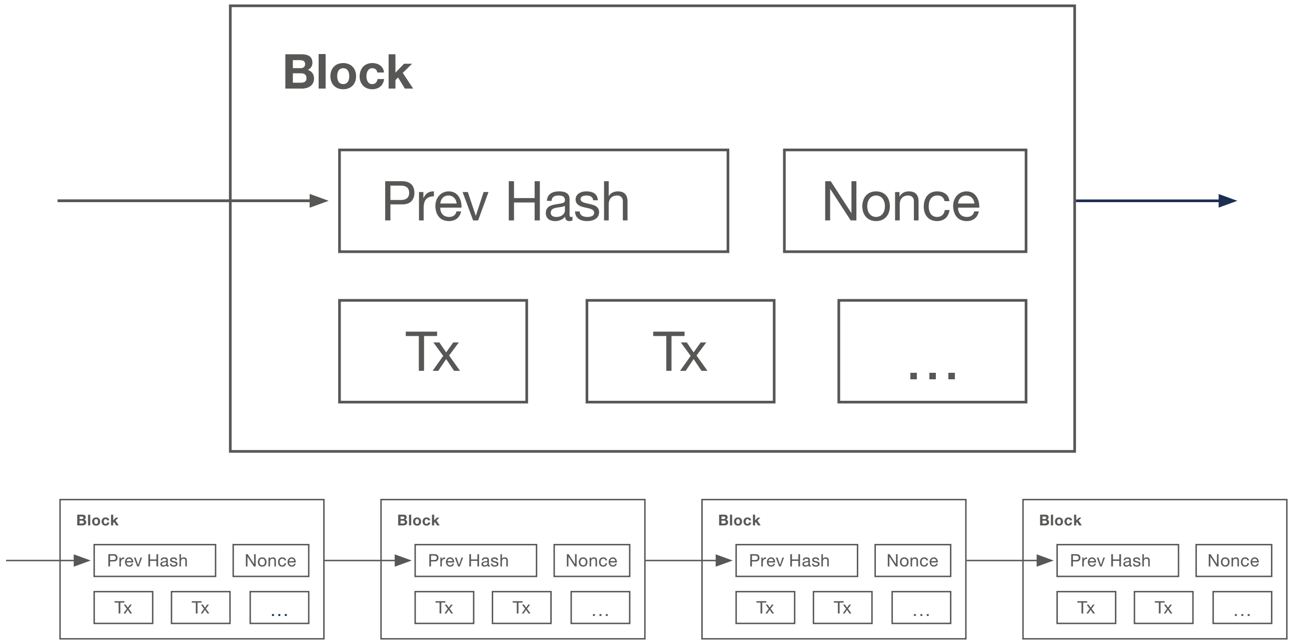
Since there are a broad variety of blockchain implementations, it is impossible to provide *one* explanation for how *all* of them work. This section aims to explain the core principles of many blockchains, including the most well-established example, Bitcoin.

Blocks and Chains

Several key properties must be present for a blockchain-based system to function, if one of them is missing, the system may not reach its full potential or even fail. The main 'ingredients' for a blockchain include:

- A technique to reach a consensus in the decentralised network
- A peer-to-peer software client that builds and connects to a decentralised network of nodes
- A data structure to store network information, such as Merkle hash trees, pointers, or a blockchain (the data structure blockchain technology got its name from)
- A mechanism that secures data on the network, such as mining, minting, proof of work, proof of stake etc.
- A validation method that clearly defines which transactions are valid and which are not
- Secure cryptography
- An incentive, or reward, for participants who contribute to the health of the network

© Kuzmick



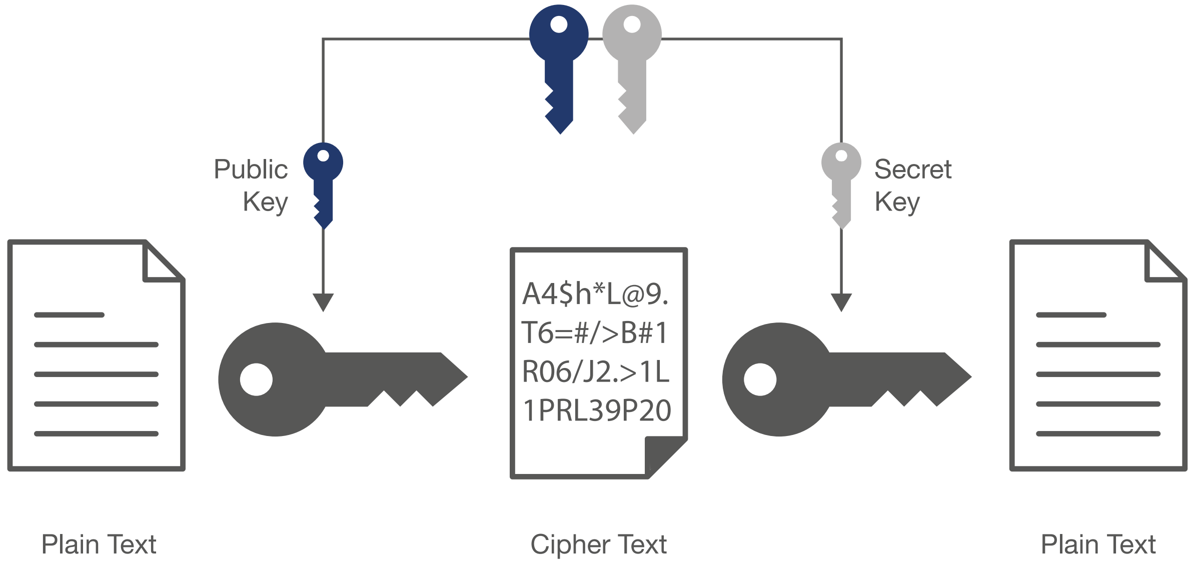
Depiction of a chain of blocks

In addition to these properties, a successful blockchain requires a methodology for dealing with changes to the network, such as updates and security patches. This includes a group of code maintainers, peer reviews and audits of the code.

Some of these individual properties existed years before the launch of the first blockchain, for example as requirements for basic software programs, **but their clever combination is what makes a blockchain feasible.**

In an open blockchain network, nodes (i.e. small or large computers) permanently listen for new transactions (Tx) and relay those they deem valid. A transaction is valid if it follows the rules of the protocol (e.g. in structure and size) and if it is not a double spend transaction. In addition to relaying these valid transactions, some nodes also provide computational power to the network by putting all valid transactions they received into a block. The special thing with blocks in an open blockchain ledger is that a new block always references its predecessor thus creating a linear chain of blocks outlined in the original Bitcoin whitepaper.

> “
>
> *Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value.”*
>
> —Eric Schmidt, Former CEO, Google



Asymmetric encryption

The Key to Success

This section covers various technical details of the technology. If you are not interested, skip to the Summary or the next chapter.

To better understand the inner workings of blockchain systems, two core concepts need to be understood:

1. Asymmetric Encryption

One of the most important inventions used in blockchain technology is asymmetric or public key cryptography.

This is a mechanism widely used in IT-systems, the World Wide Web and email, which allows people to encrypt data without the need to share a secret, such as a password that could get compromised the moment it is shared. Instead, a pair of keys are provided, one private and one public. The **public key** can be used by any person, or machine, to encrypt data and the owner of the corresponding **private key** is able to decrypt that data.

In a blockchain, the public key is represented by a public address, which can be shared with anyone. Regardless of the asset being sent to that public address, only the owner of the corresponding private key can access the asset in order to transfer it elsewhere. To compare this with today's existing banking infrastructure the public address can be likened to a bank account number that anybody is free to send money to. The private key resembles the PIN (or passphrase) that is needed to access the funds and should not be shared. To achieve this, the owner would sign a transaction with their private key (this happens locally without disclosing the key) and broadcast that signed transaction to the blockchain network.

2. Hashing

Blockchain systems make heavy use of mathematical 'one-way' functions that map data of arbitrary size to data of fixed size, so called 'hash functions'. These are designed to make it very difficult to reconstruct input data based on hashed output data.

To give an example, the sentence above run through the MD5 hash-function results in the code:

Global distribution of nodes, Bitnodes (2017)

`Blockchain systems make heavy use of mathematical 'one-way' functions that map data of fixed size, so called 'hash functions'`

↓MD5
`3848978891d73a3fed015861d904d47f`

Running the word 'Arup' through the same hash function results in the code:
`Arup`

↓MD5
`f5f6f830a7eee400cc4ff0b7e94c74dd`

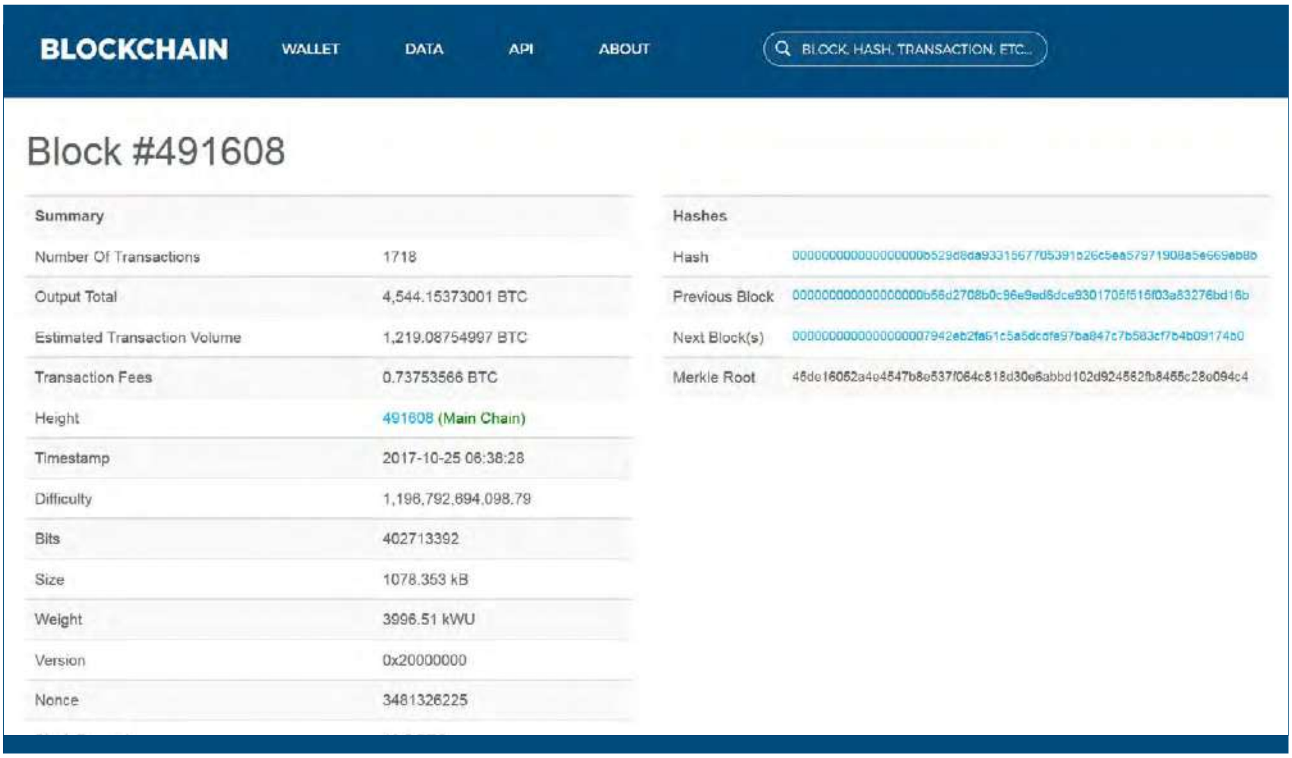
This shows how, no matter the size of the input data, the output data (for an MD5 hash function in these examples) is always a seemingly random 32 character text string.

Outside of blockchain technology, this principle is widely used, with one example being to store user passwords on servers. But instead of storing the actual passwords, a hash is generated and stored. This allows users to keep their passwords and not have to send them through the web, and thus exposing them to possible attackers. The user generates a hash of their password in their web browser, then the hash is sent to the web service, which compares it with their copy. If they match, the service knows the user must have known the correct password.

It is important to note that two different inputs should ideally never generate the same hash. If such a collision is likely to happen, another hash function should be considered. The likelihood of a collision depends on the amount of possible individual input data sets the hash function needs to face.

The Bitcoin network uses the SHA-256 hash function for many operations. A collision in this case would mean that while generating a random pair of new keys, someone would accidentally generate a private key belonging to an existing public address, enabling them to access the funds behind that address. The likelihood of such a collision is unfathomably small.

Another property of hash functions is that one cannot reconstruct the input data by looking at the hashed output data. The amount of effort it would take to reverse the mathematical function depends on the hash function that is used and the amount of computational power available to an attacker. The hash functions used in the Bitcoin protocol make it essentially impossible to reverse such a hash. There is not enough energy in the solar system to power a computer large enough to do so.[8]



Block #491608

Summary	
Number Of Transactions	1718
Output Total	4,544.15373001 BTC
Estimated Transaction Volume	1,219.08754997 BTC
Transaction Fees	0.73753566 BTC
Height	491608 (Main Chain)
Timestamp	2017-10-25 06:38:28
Difficulty	1,196,792,694,098.79
Bits	402713392
Size	1078.353 kB
Weight	3996.51 kWU
Version	0x20000000
Nonce	3481326225

Hashes	
Hash	000000000000000000b529d8da9331567705391b26c5ea57971908a5e669eb8b
Previous Block	000000000000000000b56d2708b0c96e9ed6dce9301705f515f03a83276bd16b
Next Block(s)	0000000000000000007942eb2fa61c5a5dcdfe97ba847c7b583cf7b4b09174b0
Merkle Root	46de16052a4e4547b8e537f064c818d30e6abbd102d924562fb8455c28e094c4

This screenshot from the blockchain.info website shows a block's hash starting with 18 zeros

A Network Reaches Consensus

There are a number of ways a blockchain network could reach consensus on the validity of transactions in the digital ledger. The process of *mining* is central to how the Bitcoin network and other blockchains reach a consensus and it carries out two functions:

1. It validates and adds transactions to the blockchain securely.

2. It generates and issues the network's native token, *bitcoin*, which also functions as a reward for securing the network. The next section of the report, 'Why the Bitcoin Blockchain Works', focuses on this aspect in more detail.

Nodes

The participants of the global Bitcoin network who run a full node on a computer, form the nodes of the mesh network that is Bitcoin. This could be a single-board computer like a Raspberry Pi, a laptop or a desktop PC (smartphone apps usually are not considered full nodes, instead they connect to full nodes to interact with the network).

All the nodes 'listen' for transactions on the network, and when they find them, they validate them by checking the current state of the blockchain ledger against the local copy on their hard drive. If a transaction is deemed valid (i.e. funds have not been spent yet and the transaction follows all formal rules of the protocol), the nodes broadcast, or 'relay', the transaction to the network. This is why Bitcoin is often referred to as a 'gossip' protocol. If a participant on the network receives an invalid transaction from a node, it will not listen to the node for 24 hours, this ensures that 'bad' nodes are unable to spread invalid transactions on the network.

Some nodes on the network are 'miners' and not only validate transactions and relay them to the network, but also assemble valid transactions into blocks, comparable to a physical page in a ledger book, then permanently write them into the constantly growing Bitcoin ledger — the blockchain.

There is a random element to this process, and it is never clear if or when a miner node will be allowed to attach a block full of valid transactions to the blockchain.

Miners must expend computing power to perform a hash function (see the previous chapter for details on hashing) and generate a unique code for each block with a number of zeros at the start. This is a very complex task. The Bitcoin protocol requires each hash to start with several zeros, the more zeros there are, the more complex this task gets, and lowers the possibility that the hash can be randomly generated by a computer. The difficulty increases quadratically the more leading zeros are required.

The idea behind this complex task is that it's not only a time consuming and costly endeavour for honest participants, but also for anyone who wants to attack the network and maliciously alter the ledger. The difference is that honest miners are incentivised by the mining reward, something dishonest miners will not be able to claim because the network would reject their blocks, thus rendering the reward useless for them.

When a miner produces a hash with the required amount of leading zeros, its block is 'mined', added to the blockchain and shared with the entire network. All nodes then add the block to their local copy of the blockchain, bringing it up-to-date, then return to the process of validating new transactions.

This process is called **Proof of Work** (PoW) because computational power is required to find a hash with the number of zeros required by the network, and the miner that finds it thus *proves* that they did a certain amount of *work*.

The Bitcoin network is designed to mine a new block on an average of every ten minutes. If more node operators start mining and more computing power is added to the network, the protocol will automatically ensure that the difficulty (how many zeros at the start of the miner's hash) is increased to maintain the ~10 minute new block rate. Since the process is based on probability, sometimes new blocks are found in quick succession, sometimes it can take as long as an hour.

The introduction of Proof of Work to the concept of Bitcoin was key to the solution of the Byzantine Generals Problem[9] affecting fault-tolerant computer systems, in particular distributed computing systems that others couldn't solve before Satoshi Nakamoto.

There exists other consensus algorithms, with another main one being *Proof of Stake* (PoS). In PoS blockchain systems, the node which is allowed to add the next block to the blockchain is chosen randomly. The chance of one account being chosen depends on the stake (i.e. amount of blockchain tokens) the account has. Blocks in PoS blockchains are *forged* or *minted*, not *mined*, to illustrate that there is much less work involved when compared to PoW.

Summary

- A blockchain is a method of storing data.
- Additional processes are required to ensure that data stored on a blockchain is secure, valid and tamper-proof.
- Without a way to incentivise honest behaviour on a blockchain, there is no punishment for wrong behaviour. This leads to a system that relies on trust similar to centrally administered database systems.
- The inclusion of an open and permissionless system in which everybody can participate, a consensus algorithm backed by incentives, and an overarching decentralised approach, makes blockchain technology a genuine game changer.

Why the Bitcoin Blockchain Works

© Steve Jurvetson

Overview

To fully understand blockchain technology, it is important to learn why Bitcoin, the world's largest scale and most widely-used blockchain, is so effective. Incentives are vital for Bitcoin's continued operation, and this section of the report focuses on the three main categories of them.

> *"I really like Bitcoin. I own Bitcoins. It's a store of value, a distributed ledger. It's a great place to put assets..."*
>
> —David Marcus, Former CEO, PayPal

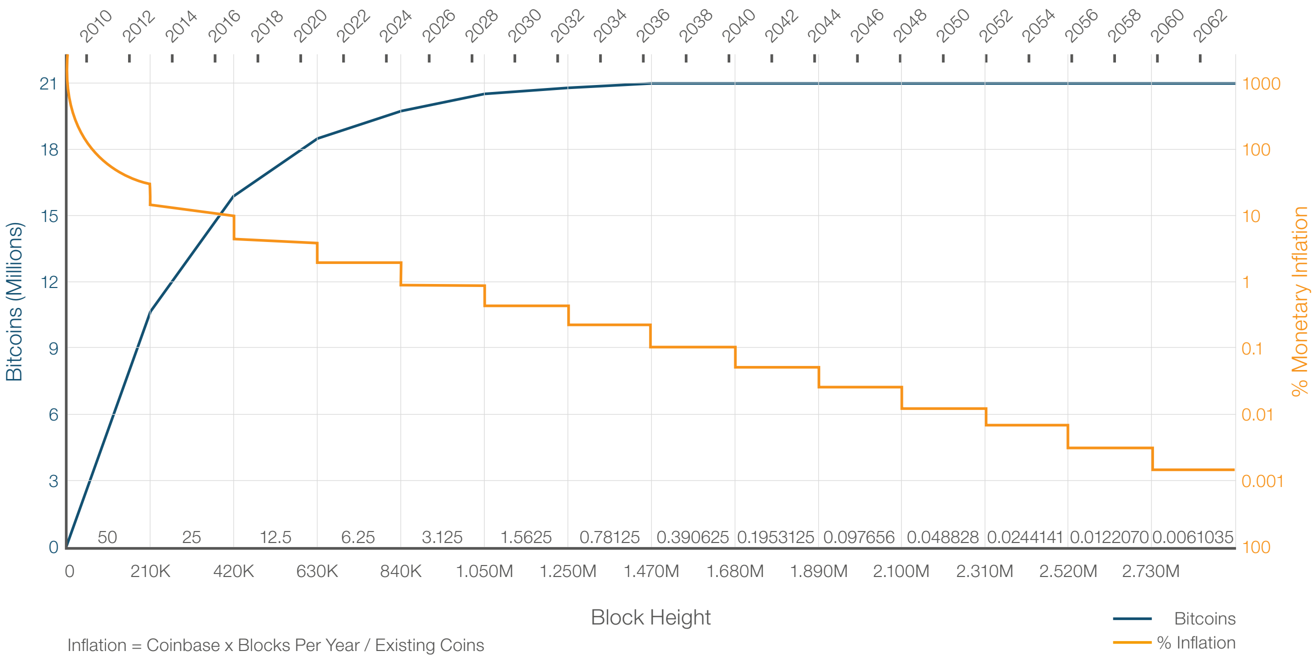
The Bitcoin protocol is a state of the art, complex digital system. It was designed to be the most useful and resilient form of money possible, which requires it to be completely decentralised, to avoid trust issues inherent in centralised systems. Some of the incentive examples in this section focus on the financial side of Bitcoin. The reason for this is that open blockchains like Bitcoin have two aspects to them — the ledger (blockchain), and also a digital token (the money aspect). Every open blockchain has a digital token, because they are what is required to provide security.

A blockchain is an open, decentralised database with no single person or company in charge. The cost of hosting, maintaining and securing a centralised database is paid for by the cost a company charges for the product or service it offers. But there is no company in charge of securing a blockchain. Therefore, the security needs to be outsourced to the free market.

In order to incentivise free market participants to provide the security for an open blockchain, they are regularly rewarded with a share of a predefined number of the blockchain's native tokens if they provide the computing power required to validate transactions and include them in blocks. This is called the block reward, and it diminishes slowly over time for most blockchains, eventually being replaced by transaction fees. The fact that most blockchains will not achieve a reasonable level of adoption in the longer term, due to the sheer number of them in existence, makes it fair to assume that they will need to have large transaction fees in order to maintain their level of security, and would therefore struggle to survive. The most likely exception to this scenario is currently the Bitcoin blockchain.

Economic Incentives

Perhaps the most important type of incentive for people adopting bitcoin, is the economic aspect. The Bitcoin blockchain typically increases in value over time, due to the combination of its hard limit on the currency supply (making it a store of value), and the massive potential for growth in its user base. As more people seek a share of the



Bitcoin Monetary Inflation, Cointelegraph (2017)

fixed number of bitcoin available, the price of one unit escalates and market volatility rates reduce, as has proved to be the case throughout 2016 and into 2017. Lower market volatility encourages more people to use the Bitcoin blockchain, which results in an even higher valuation of the system. Unlike snowball or ‘Ponzi’ marketing schemes where a lack of new users causes the system to collapse, Bitcoin would continue to function as normal, even if the influx of new users suddenly stopped. This is because Bitcoin is not controlled by any one person, and therefore the free market forces the system to find an equilibrium between the number of active users and the cost to operate and maintain the blockchain.

Currency Limit

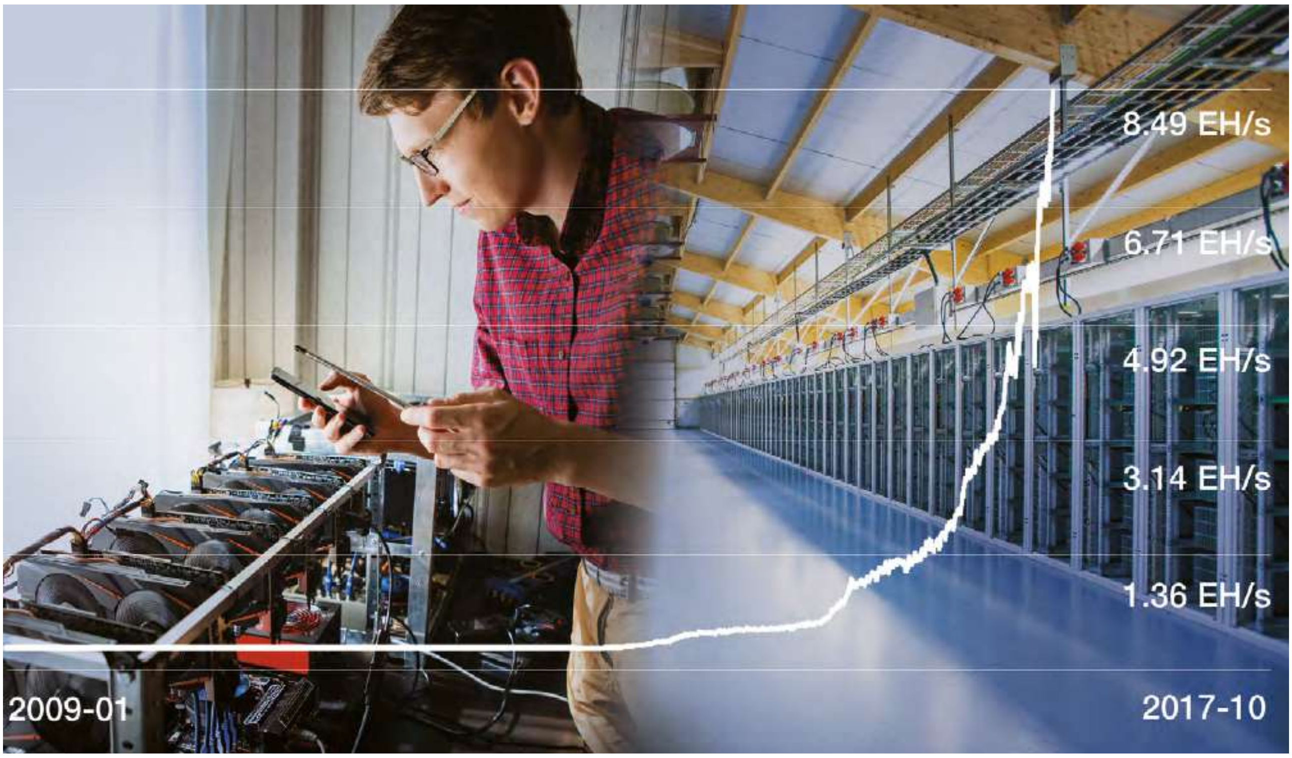
Bitcoin has a hard-coded rule that limits the total number of currency units that will ever exist to 21 million (or 20,999,999.9769 to be precise)[10] and this number will be reached approximately in the year 2140. This rule cannot be changed without consensus amongst all participants in the system, and because bitcoin is designed to be a rare digital asset, it is unlikely that users would vote to increase the total number of currency units. Anyone can copy Bitcoin’s code, create a different version of it and increase the currency supply, but it would have very little value compared to the more scarce original version. The reason Bitcoin’s inventor, Satoshi Nakamoto, chose to set a hard cap on the currency was to remove the possibility of endless inflation which would decrease the currency’s value over time. Bitcoin’s scarcity makes it very likely that it will be a store of value in the longer term.

Decreasing Inflation and Increasing Growth

Until the year 2140, bitcoin will be an inflationary currency by design, in order to bring the supply into the market. Nakamoto hard-coded the inflation rules into Bitcoin at the start. The protocol was programmed to release half of the total supply of currency in the first four years, and then it halves the inflation rate every four years until 2140, when all bitcoin has been mined. Bitcoin’s constantly decreasing inflation rate, its cap on currency supply and continuously growing usage, more or less guarantees that value increases rapidly over time.

Uncorrelated Asset Class

Bitcoin is an entirely separate financial system from traditional assets and currencies, with its own unique properties, and as such, its value does not correlate with them. The fact that it also operates outside of the politics of single nations makes it an attractive medium for investors, as a hedge against other assets in their portfolio.



Development of Bitcoin computing power over time

Security Incentives

Bitcoin employs some clever and important incentives to keep miners in particular very honest. This ensures the current and future stability of the network.

Proof of Work

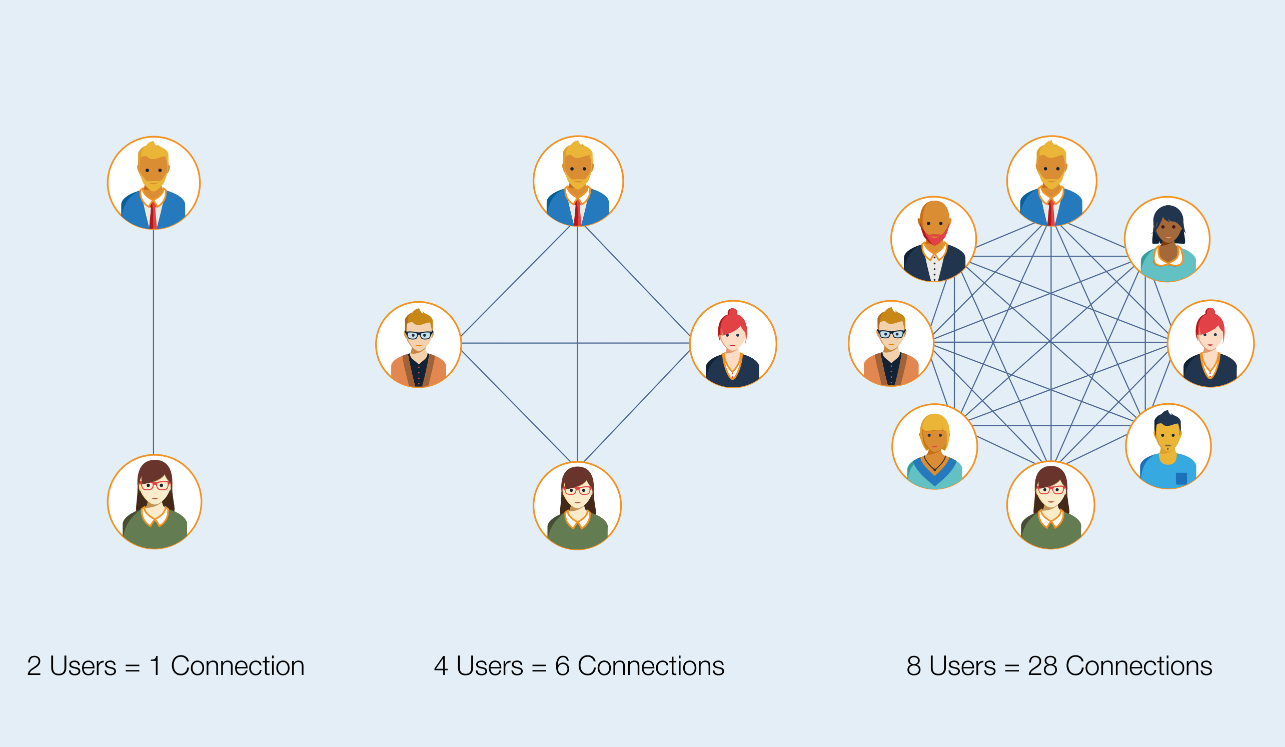
Bitcoin currency units are created based on Proof of Work, which requires the expenditure of time and energy by miners who must acquire, set up and run mining machines. The machines are a specialist form of hardware called Application Specific Integrated Circuits (ASICs), and are specifically designed to efficiently mine bitcoins by generating SHA-256 hashes. ASICs are relatively expensive to purchase and require a constant electricity supply, so Proof of Work costs money, therefore people who want to become miners have to take a financial risk to be a part of the system. They literally hold a stake in the Bitcoin ecosystem, and once they are part of it, they must regularly spend money to update their mining machines to stay competitive with the other miners to make a profit. If their machines are not competitive, the cost-to-reward ratio becomes unsustainable. Upgrading the machines makes them more efficient, and as a result, the hash rate of the network rises constantly, increasing the security of the network.

At the time of this report's publication, Bitcoin's mining hash power stands at over five Exa-Hashes per second, which means that together, miners are able to run more than five million, million, million SHA-256 hash operations every second. This makes it *by far* the most powerful, and therefore secure, blockchain network in the world, which consumes more energy[11] annually than Slovenia. Anyone wishing to try to attack the network to control the majority of hash power would need to spend hundreds of millions of dollars on mining equipment.

It has been calculated that the Bitcoin network could, provided certain technical barriers are overcome, scale to securely process all transactions in the world. The amount of power required to secure the network does not need to increase beyond what it consumes today, as the security is already world-class. This makes it a far more sustainable option compared to the energy required to operate and secure legacy payment and banking networks, including servers, ATMs, physical cash, vaults, armoured trucks and office space for related staff. In addition, renewable energy is already being used to mine and secure bitcoin at a large scale, particularly in countries like China.

Unrivalled Network Effect

Bitcoin had very humble beginnings, being announced on a cryptography mailing list. Nakamoto did this to attract the interest of the type of people who were trying to create something like Bitcoin back in the 1990's. A few individuals were involved when Bitcoin launched, to help with coding and other tasks, and



Network effect

> *“Bitcoin has a tremendous ‘network effect’, in my opinion, which may give it an insurmountable early-mover advantage.”*
>
> —Andreas M. Antonopoulos, Technologist

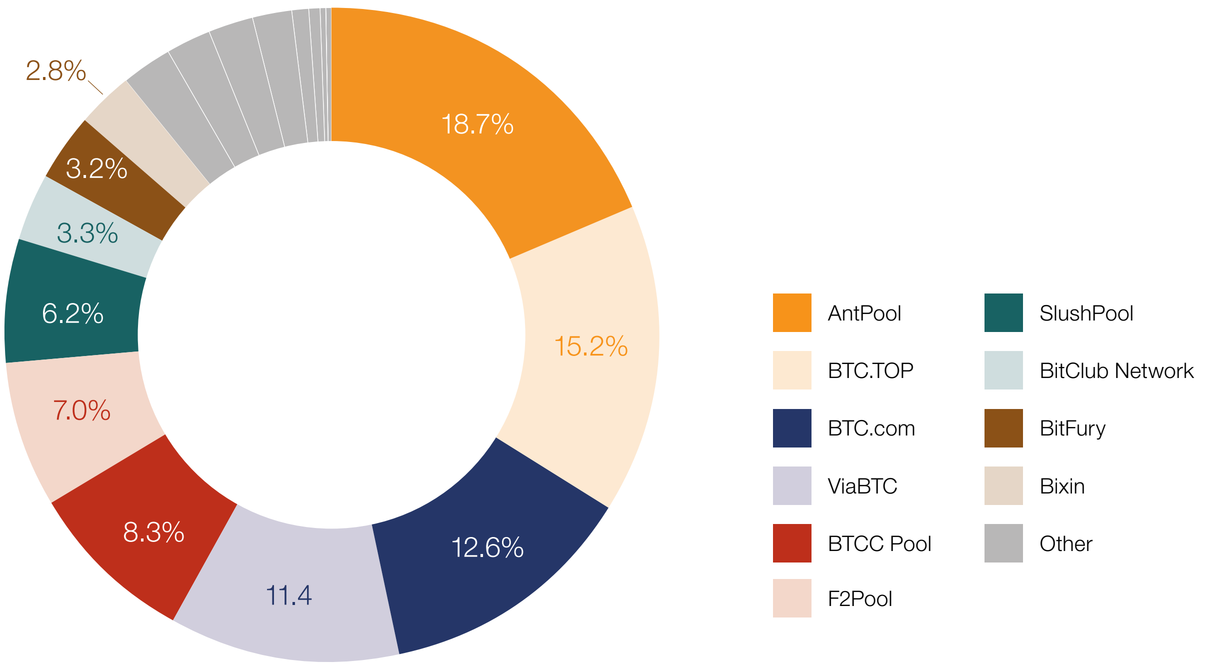
the first two years were important for laying the groundwork for its future. Bitcoin quietly gained momentum, attracting an increasing number of developers and users over the years until it reached a tipping point in 2013, experiencing a massive increase in adoption and value. This so-called network effect continues to fuel adoption and participation, particularly when it comes to mining and nodes, increasing the security of the system.

You Cheat, You Lose

Some miners in the past have attempted to try to ‘game’ the system to earn more money from blocks than Bitcoin’s rules dictate. Attempts to cheat the system are punished and miners lose the block reward value, and the related money spent on powering their mining machines to find blocks. This mechanism provides an economic incentive to play by the rules.

Miners Must Act Rationally

Pools allow miners to combine their hashing power in order to have a better chance of finding blocks more consistently. The pools then split the block reward between the miners, based on hashing contribution. Mining pools that allow themselves to gain too big a percentage of the network will suffer the consequences from the miners. This happened with the Ghash mining pool in mid-2014, when it very briefly gained 51% of the network hash rate. That percentage dropped rapidly immediately afterwards, and continued to drop until the pool became almost irrelevant. This can unsettle the market, which can



Bitcoin hashpower distribution (2017)

cause the bitcoin price to drop, thereby reducing miners' revenue. Miners are incentivised to maintain a healthy balance with regards to the percentage of the hash rate that mining pools have.

Addresses Cannot Be Hacked

Addresses are basically 'accounts' where bitcoins are held. As they are publicly known, an address[12] with a large number of bitcoin may become a target for hackers. However, it is almost impossible to hack a bitcoin address. To put this into perspective, there are more possible bitcoin addresses than there are grains of sand on Earth. But if each of those grains of sand represented another planet Earth, there are billions more possible bitcoin addresses than there are grains of sand on all of those Earths *combined*.

As there are so many possible private keys, but only one that can be associated with a bitcoin address, a miner would have to use their hash power to go through all possible private keys until they find the correct one, which would allow them to retrieve the bitcoin from that address. Therefore, as long as a person knows how to securely store the associated private key, a bitcoin address is *by far* the world's most secure location to store wealth.

Ideological and Usage Incentives

The ideological benefits of Bitcoin were an early trigger for adoption, and as it evolves, they are powering a shift in our understanding of what money is and should be.

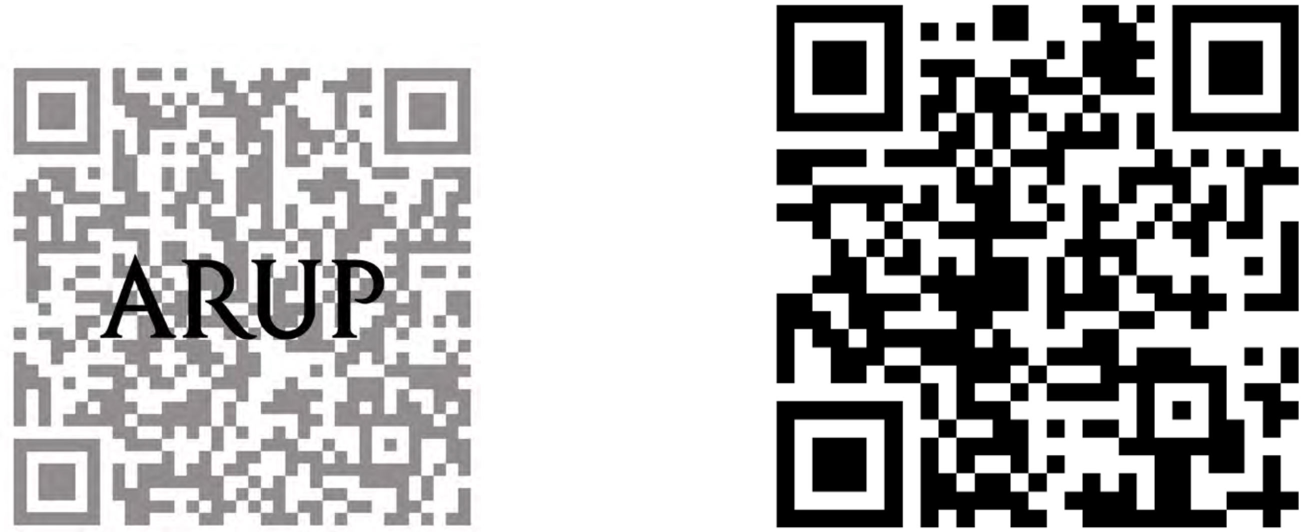
Fun fact: '*Ideological*' is the only word Bitcoin's inventor Satoshi Nakamoto spelled incorrectly in the hundreds of forum posts and emails sent over a two year period.

Allows People to Control Their Own Money

Financial organisations like banks, credit card companies and PayPal, are trusted with customer funds and permit or prevent them from spending those funds, based on what they are being used for. This is called a 'pull system', as companies can *pull* funds out of the user's account if they are given permission to do so. In a *push* system like Bitcoin, only the owner of the funds can authorise their release. This provides the user with total control of their money, and they can spend it whenever and on whatever they want. The downside of this system is the lack of insurance; if a user loses their bitcoin, they can never get them back.

Properties Cannot Be Changed Without Consensus

The traditional financial system of central and commercial banks delegates responsibility for changes to important economic policy decisions to a small group of people. In contrast, any changes to



QR codes for a bitcoin public address and private key pair

the Bitcoin protocol typically require 95% consensus from the user base. Since early 2015, the Bitcoin community has discussed solutions to increase the transaction capacity of the network, which has edged closer to its limit. Most of the community has given support for a combination of so-called “on-chain” and “off-chain” solutions, but others have not and this lack of consensus prevented a solution from being reached for a long time. However, on August 24th 2017, the largest ever upgrade to Bitcoin’s codebase, Segregated Witness, was activated, meaning that a partial scaling solution was reached, and opened the door for further positive developments in the future.

The difficulty of upgrading Bitcoin’s code could be considered one of its few weaknesses, but is also one of its greatest strengths because the protocol cannot be hijacked by a small minority. Developers working on the Bitcoin codebase compare it to the maintenance of a race car — with the engine turned on — while racing. There is just no way to shut it down for a weekend of maintenance.

Self-Regulating System

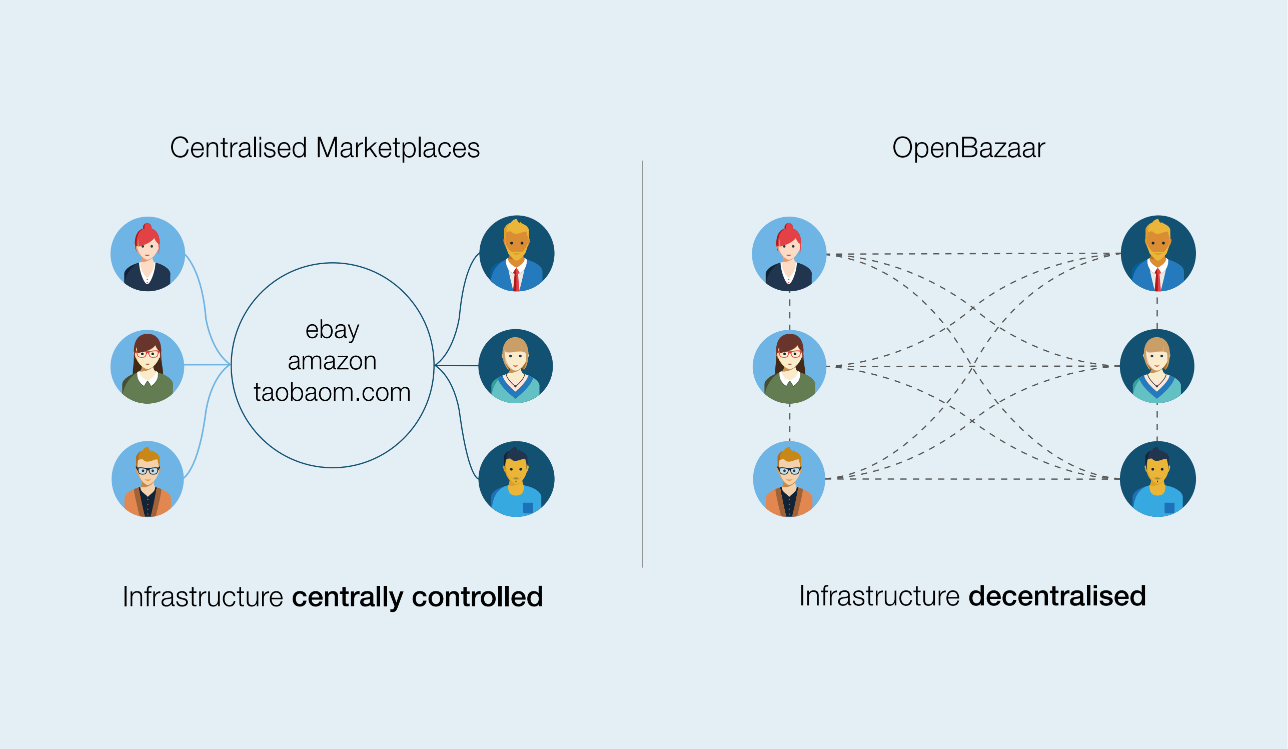
The traditional financial system is regulated by designated legislative bodies in various national jurisdictions, a form of ‘add on’ to the financial system. Bitcoin, on the other hand, is a global network that’s self-regulated by the hard-coded rules of the protocol, and conventional laws cannot apply. Bitcoin can exist within all jurisdictions simultaneously, and has no headquarters, and no CEO or leader who is accountable under law.

Allows For Decentralised Trade

Bitcoin made it possible to launch the first ever decentralised online marketplace, OpenBazaar, in 2016. The program runs on PC (for now) and, similar to Amazon, enables users to buy products and services from individuals or companies. But while Amazon acts as an intermediary, taking a cut of transaction prices and monetising user data, OpenBazaar operates only as a platform for free trade, by exploiting the decentralised and programmable nature of Bitcoin.

Businesses Save Money

Bitcoin payment processors such as Coinbase provide payment interfaces for regular websites that enable companies and organisations to accept bitcoin payments from customers. The payment processors sell those bitcoins on the open market for fiat currencies (such as dollars, euros, etc), which are sent to the company’s bank account. This process costs companies up to 1% for each transaction, compared with the 2-3% charged by credit card providers, meaning a significant reduction in transaction fees and a substantial increase in profits if they only accept bitcoin for payment.


Centralised Marketplaces
ebay
amazon
taobaom.com
Infrastructure **centrally controlled**
OpenBazaar
Infrastructure **decentralised**

Architecture of centralised vs. intermediary-free marketplaces, openbazaar.org (2017)

No Chargebacks or Fraud

Bitcoin transactions are irreversible and under the sole control of the owner, so fraud is eliminated. So-called chargebacks (a demand by a credit card provider for a retailer to make good the loss on a fraudulent or disputed transaction) are frequent and costly for merchants, and therefore built into the price of goods and services. Chargebacks are not possible under Bitcoin, so any dispute, such as returning an item, must be settled by other means, perhaps via direct communication, or a smart contract. Seeing the economic benefits, well over 100,000 merchants worldwide now accept bitcoin for payment, and this number continues to grow rapidly.

24-Hour Trading

Bitcoin is a protocol like the internet, therefore it is always available to use. Transactions can be made at any time of any day, and liquidity to the market is in constant supply, which helps facilitate global trading. By contrast, trading on Wall Street, at the London Stock Exchange etc. happens only during opening hours.

Huge Opportunity for Developing Countries

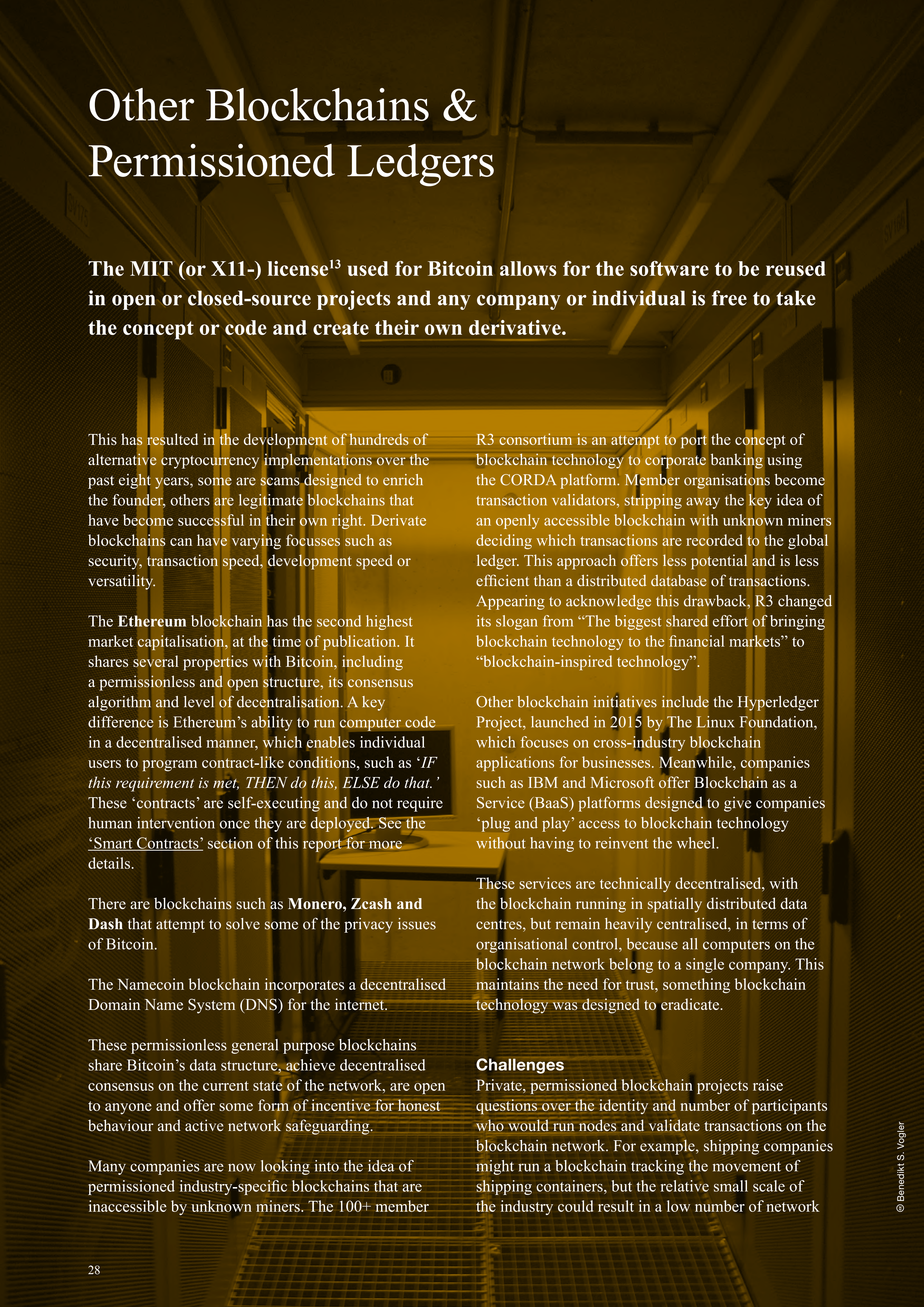
Minimal banking services in developing countries makes it difficult and expensive for their citizens to transact, especially internationally.

However, the relative widespread availability of mobile phones and internet access in these regions opens up the opportunity for people to become their own bank and transact with anyone worldwide using the Bitcoin protocol, averting the need for traditional brick and mortar banks.

Physical bitcoins

Summary

- The economic and security incentives built into the Bitcoin protocol are some of the most important innovations in the history of computer science.
- The economic incentives allow for the growth of a more fair, inclusive and stable form of money. They also allow individuals and companies to use Bitcoin as a store of value in the longer term.
- The security incentives of Bitcoin, coupled with the economic incentives, ensure that information added to the blockchain, which is designed to be immutable, is protected.
- Bitcoin has many usage incentives that can appeal to anyone, even those not interested in its economic properties.



© Benedikt S. Vogler

Other Blockchains & Permissioned Ledgers

The MIT (or X11-) license[13] used for Bitcoin allows for the software to be reused in open or closed-source projects and any company or individual is free to take the concept or code and create their own derivative.

This has resulted in the development of hundreds of alternative cryptocurrency implementations over the past eight years, some are scams designed to enrich the founder, others are legitimate blockchains that have become successful in their own right. Derivate blockchains can have varying focusses such as security, transaction speed, development speed or versatility.

The **Ethereum** blockchain has the second highest market capitalisation, at the time of publication. It shares several properties with Bitcoin, including a permissionless and open structure, its consensus algorithm and level of decentralisation. A key difference is Ethereum's ability to run computer code in a decentralised manner, which enables individual users to program contract-like conditions, such as '*IF this requirement is met, THEN do this, ELSE do that.'* These 'contracts' are self-executing and do not require human intervention once they are deployed. See the 'Smart Contracts' section of this report for more details.

There are blockchains such as **Monero, Zcash and Dash** that attempt to solve some of the privacy issues of Bitcoin.

The Namecoin blockchain incorporates a decentralised Domain Name System (DNS) for the internet.

These permissionless general purpose blockchains share Bitcoin's data structure, achieve decentralised consensus on the current state of the network, are open to anyone and offer some form of incentive for honest behaviour and active network safeguarding.

Many companies are now looking into the idea of permissioned industry-specific blockchains that are inaccessible by unknown miners. The 100+ member R3 consortium is an attempt to port the concept of blockchain technology to corporate banking using the CORDA platform. Member organisations become transaction validators, stripping away the key idea of an openly accessible blockchain with unknown miners deciding which transactions are recorded to the global ledger. This approach offers less potential and is less efficient than a distributed database of transactions. Appearing to acknowledge this drawback, R3 changed its slogan from "The biggest shared effort of bringing blockchain technology to the financial markets" to "blockchain-inspired technology".

Other blockchain initiatives include the Hyperledger Project, launched in 2015 by The Linux Foundation, which focuses on cross-industry blockchain applications for businesses. Meanwhile, companies such as IBM and Microsoft offer Blockchain as a Service (BaaS) platforms designed to give companies 'plug and play' access to blockchain technology without having to reinvent the wheel.

These services are technically decentralised, with the blockchain running in spatially distributed data centres, but remain heavily centralised, in terms of organisational control, because all computers on the blockchain network belong to a single company. This maintains the need for trust, something blockchain technology was designed to eradicate.

Challenges

Private, permissioned blockchain projects raise questions over the identity and number of participants who would run nodes and validate transactions on the blockchain network. For example, shipping companies might run a blockchain tracking the movement of shipping containers, but the relative small scale of the industry could result in a low number of network nodes. This low level of decentralisation would make the blockchain more prone to attacks compared to large, established open blockchains like Bitcoin or Ethereum.

If only a few approved participants are allowed to validate transactions on the blockchain, the system becomes reliant on the concept of trust and the idea that a transaction history is only valuable if the validators are trusted parties.

The Sewer Rat

Blockchains that operate in the open with a large user base are vulnerable to attacks and hacking but more likely to have security flaws discovered early, before an exploit turns into a large scale problem. If the software is open-source, a fix to a vulnerability can usually be provided very shortly after it is discovered.

Closed ecosystem blockchains are theoretically resilient to security threats because the possibility of flaws being discovered by those outside the system is low. However, when an attack is successful it can be much harder to identify an appropriate response and if that vulnerability becomes publicly known it can severely damage the company's reputation.

Andreas M. Antonopoulos, a renowned security expert and Bitcoin speaker, has compared open blockchains to a sewer rat[14] that is permanently exposed to all kinds of viruses, which builds up its immune system and makes it extremely resilient. He compared closed blockchains to a 'bubble boy', whose bubble protects him from threats most of the time, but when it is pierced and he gets a 'virus' he becomes bedridden for days. In other words, no matter how corporations try to protect their closed systems, they will never have the same level of security as open systems that are constantly exposed to threats.

Summary

- Blockchain systems can be classified in terms of how permissioned they are.
- Blockchains can serve various purposes and focus on different aspects, such as security, speed and versatility.
- Making a blockchain accessible to only a few selected stakeholders to validate transactions conflicts with a fundamental principle of blockchain — to eliminate the need for trust.
- Security flaws in open blockchains are detected early and do not follow the 'security through obscurity' principle whereby reliance on the secrecy of the network design or implementation is the main method of providing security.

Smart Contracts

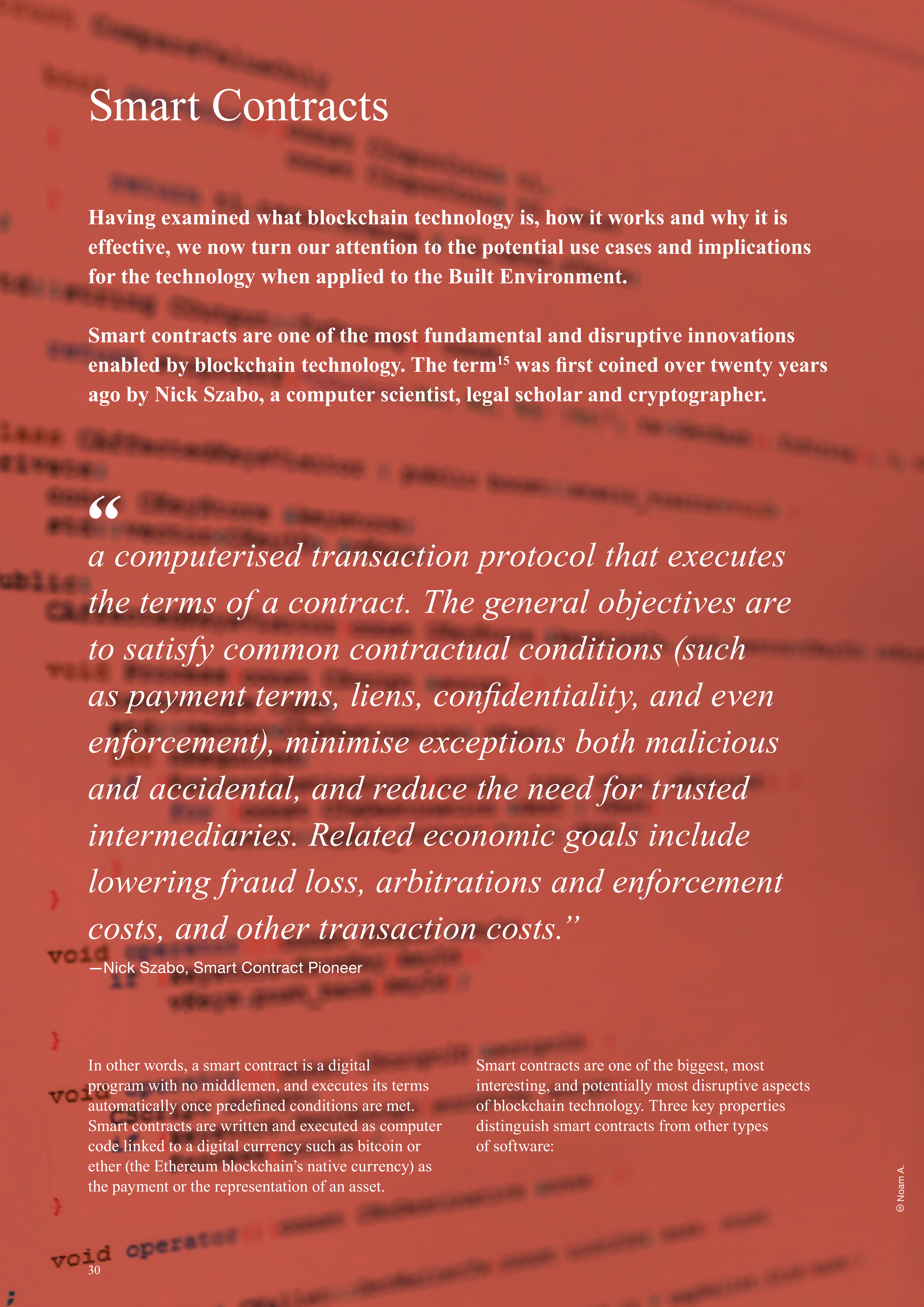
Having examined what blockchain technology is, how it works and why it is effective, we now turn our attention to the potential use cases and implications for the technology when applied to the Built Environment.

Smart contracts are one of the most fundamental and disruptive innovations enabled by blockchain technology. The term[15] was first coined over twenty years ago by Nick Szabo, a computer scientist, legal scholar and cryptographer.

> “
> *a computerised transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and reduce the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.”*
>
> —Nick Szabo, Smart Contract Pioneer

In other words, a smart contract is a digital program with no middlemen, and executes its terms automatically once predefined conditions are met. Smart contracts are written and executed as computer code linked to a digital currency such as bitcoin or ether (the Ethereum blockchain’s native currency) as the payment or the representation of an asset.

Smart contracts are one of the biggest, most interesting, and potentially most disruptive aspects of blockchain technology. Three key properties distinguish smart contracts from other types of software:



© Noam A.

© Steve Snodgrass

1. They can only be recorded on a blockchain, which gives them some of the same properties as a blockchain, such as high security, immutability and censorship resistance.

2. A smart contract itself controls the recording and transfer of assets on a blockchain.

3. A blockchain executes the smart contract, which cannot be changed unless users agree to it in consensus.

Benefits for the Built Environment Sector

Smart contracts offer many advantages[16] for organisations within the Built Environment sector, including:

Fast Settlement

The fact that smart contracts are automated by computer code and connected to a global blockchain means digital tasks can be performed much faster and more frequently. For example, if a smart contract is used to pay a contractor for work, the payment could be executed almost immediately once the work is complete.

High Accuracy

Provided that smart contracts are written properly, actions performed using them will be very accurate because they adhere strictly to a computer code, which almost entirely eliminates the possibility of mistakes.

Less Risk

Using a blockchain to execute smart contracts makes them more secure than regular contracts that require centralised counterparties. In addition, they would be virtually unhackable, immutable and not prone to manipulation.

Trustless

There are no intermediaries involved in smart contract settlements, which removes the need for trust in any individual or company.

Lower Costs

Since smart contracts do not rely on third party intermediaries, the associated costs are reduced or even removed. Legal costs, especially related to dispute resolution, frequently impact on traditional contracts but these can be significantly reduced if different scenarios or contingencies are written into smart contracts as code. This process could mean introducing legal participation before a project begins to ultimately save money on legal costs post-handover. This process is similar to how BIM requires more design input up front to reduce the overall cost of construction.

Brooklyn Microgrid

Also, as repetitive tasks could be automated, this means that the main costs associated with using smart contracts for this purpose would just be the actual creation of the contracts themselves.

Use Cases

There are a number of potential uses[17] for smart contracts within the Built Environment sector. These include:

Digital Identity

Smart contracts could allow individuals to define and control their own personal information and choose what and how much of it to disclose to counterparties. The financial aspect of blockchain, particularly Bitcoin, allows for 'push' rather than 'pull' transactions, which means that users decide to give their asset to others, rather than have it taken from them, with their permission. Digital identity could operate in the same manner, enabling individuals to define what information is provided to counterparties, rather than have large amounts demanded from them, with the danger that some of it could be sold to advertisers. In addition, personal data is only ever contained within the smart contract itself, eliminating the cost and risk of the counterparty having to store personal information.

Intellectual Property Rights

Ownership rights for an asset, especially a digital asset, can be proven and tracked. Blockchains such as Bitcoin and Ethereum, enable assets to be tracked publicly and the related ownership rights transferred, almost instantly, with negligible cost. In the context of BIM, proving the rights of Revit families has been problematic because files can be easily copied and modified. Digital currencies could securely and publicly record the ownership of Revit families, and with the aid of smart contracts, transfer ownership in exchange for payment.

Property and Land Titles

Smart contracts could be used to transfer the ownership of deeds to property or land, reducing or eliminating the associated legal costs and need for paper contracts.

Energy Transfer / Microgrids

Smart contracts could be used by energy companies to transfer the ownership of energy and keep track of energy used or owned by customers. Most people get their energy from large providers, but the rise of decentralised forms of energy production, such as solar, enables more homes to generate their own energy, and even have a surplus. A smart meter could assign ownership of excess energy to the homeowner and transfer it to others via a smart contract. The

Blockchain in Voting

actual energy transfer would be carried out by the energy company.

Supply Chain
Smart contracts can be used to purchase, track, and verify items in a supply chain, in real-time. This would reduce risk and therefore lower the costs of associated insurance. Live product tracking could begin at the factory and continue during transit and to the shelves at a distributor or store. On a building project, each item could be tracked to the site and linked, on a blockchain, to the digital version of the same item in a BIM model. See the 'Blockchain for the Supply Chain' and 'BIM with Blockchain' sections for more details.

DAOs
'Decentralised Autonomous Organisations'[18] (DAO) are smart contracts that essentially take the form of organisations, or corporations, that operate on a blockchain. They have no CEO, board of directors or headquarters, and exist solely in the cloud as computer code.

The first example of this type of organisation was called simply 'The DAO' and was launched on 30th April 2016 with a website and a 28 day crowdsale to fund it. The DAO was a smart contract built on the Ethereum blockchain, and it raised around $150m worth of ether, making it the highest funded crowdsale in history at that time. The DAO's purpose was to act as a venture capital fund used to invest in various businesses and pay out profits to the stakeholders who provided the capital.

However, less than three weeks after the crowdsale ended, a hacker managed to take control of around a third of the funds, so the Ethereum community decided to perform a contentious 'hard fork' of the blockchain to refund the stolen funds to investors. This essentially destroyed the promise that the Ethereum blockchain would be immutable, as all blockchains are supposed to be. Not everyone agreed with this course of action and some miners chose to remain on the original chain, called Ethereum Classic.

This split of The DAO into two different blockchains damaged its reputation, temporarily lowered its value due to the market sell-off of its native currency, and confused potential investors and users. The cause of all of this was the poorly written and insecure code, which is the biggest danger with any form of blockchain. The legal implications of DAOs are enormous, and are explored further in the 'Legal Implications of Blockchain Technology' section of this report.

DACs For Shaping a Better World
A smart contract-based Decentralised Autonomous Charity could be created by a company or individual in the Built Environment sector to automatically

© Volkswagen Group

transfer digital currency to charities or individuals at a time of crisis, such as following a natural disaster. This would enable the direct and immediate transfer of funds, without middlemen, also maximising the amount received. The DAC could be coded to search social media platforms for charities and individuals in urgent need and automatically send currency to their public address.

Benefits for Society

Smart contracts could transform the way election voting is performed, by combining digital identity (mentioned previously in this section), with voting via smart contracts. This would allow individuals to vote without having to reveal whom they have voted for. Election fraud could be eliminated as every vote would be listed on the blockchain, which is publicly verifiable, therefore reducing corruption and strengthening democracy.

Smart contracts could automate various mundane tasks to help simplify peoples' lives. In the smart home of the future, many household devices will have an internet connection and speak to each other. It is not difficult to imagine a situation where a refrigerator is able to weigh the amount of milk inside and, when supplies get too low, purchase more milk via a programmed smart contract. The smart contract could state that when the weight of milk reaches a certain level, for a certain period of time, more milk should automatically be purchased from a website (or maybe a decentralised marketplace like OpenBazaar) for delivery to the customer's home, possibly via a drone. The technology to make this happen already exists and could apply to an array of other appliances and products in homes, including bread bins, washing machines, light bulbs, or any product that can be measured in some way or require regular purchases of food or cleaning materials.

Self-driving vehicles will become common in the smart city of the future. They could utilise a digital wallet and use a smart contract to perform transactions with other vehicles in their vicinity. For example, if a car in front is being driven too slowly, a smart contract could be used to send a small amount of bitcoin to the car to pay for it to move to another lane or turn onto a side street. This would be particularly useful for emergency vehicles, helping reduce the time to reach the scene of an emergency.

Oracle Contracts

Pure smart contracts, which this section of the report has focused on so far, require no intermediaries and are useful for internal corporate use, however they may be unrealistic in contractual situations involving certain external collaborators. *Oracle*[19] smart contracts allow a number of intermediaries

(called *oracles*) to settle contracts in a decentralised manner. They provide the essential link between real-world contracts, which involve an element of human interaction but have the potential to be corrupted by individuals, and blockchain-based contracts, which are immutable and secure, but may be too extreme for some business situations.

Data held in oracle contracts is at greater risk of being inaccurate, but this is minimised by the fact that data included is the *median* value from all oracles. For example, if an oracle contract wanted to include current temperature data for a location, instead of trusting one source (such as a website), it could seek the data from several sources and calculate the average value. Using this method, the data would be mostly accurate (although not 100%) and also more readily available, since the removal of one source would not mean that the data would not be retrievable.

Summary

Aside from digital currency, smart contracts will become one of the defining aspects of blockchain technology in the future. They can automate many types of tasks traditionally performed by people, thereby reducing the time, costs and risks associated with them. Not only can the Built Environment sector benefit from them, but society as a whole can also. Homes, transport, companies and many other aspects that are key to an individual’s daily life stand to be enhanced in many ways. There will be a huge number of incredible uses for smart contracts in the future that people can’t even imagine today, and these will be realised once blockchain technology matures and scales to a level to serve everyone in the world.

Blockchain for the Supply Chain

© Christian Lambert

An immutable digital ledger could radically improve supply chain management (as a holistic approach to improving resource efficiency) by improving co-ordination, integration and logistics. It could provide a secure record of transactions for accounting, production and even research and development, potentially reducing the need for intermediaries and lowering costs.

The Journey of Conflict Stones

Blockchain technologies could enable construction to verify the chain of custody of a product, proving when and where it was handled by individual companies and when it entered and left their facilities, with corresponding benefits for transparency and efficiency.

In one frequently-cited project, London based start-up Everledger exploited the fingerprint-like properties of polished diamonds to record over a million of them onto a blockchain. Paper-based documents can be faked and therefore diminish transparency and authenticity of diamond trading. Everledger's blockchain-based digital system is immutable and fast, enabling retailers to ensure the diamonds they handle and trade are 'non-conflict stones' simply traced throughout their lifetime journey.[20] It is also able to check they were sourced by ethical means.

Construction Supply Chains

Construction supply chains are typically temporary and come together to deliver one-off projects. This results in an unstable and fragmented approach with design, and the construction disciplines kept largely separate.[21] This has led to problems with transparency and efficiency, and stagnating levels of productivity over the past 20+ years, as set out in the McKinsey&Co article *The construction productivity imperative.*[22]

Blockchain technology could solve these issues in a number of ways:

1. **Increasing the speed and scale of decision making and procurement processes.**

Many companies normally rely on handwritten signatures and scanned documents before starting any work. Digital contracts, hashed, signed and time-stamped on a secure blockchain, can provide customers and contractors with certainty without the need to wait for delivery of a contract or an email attachment.

2. **Providing consistent reporting for subcontractors, contractors, and owners.**

Project teams do not currently have a common understanding of how the project is faring at any given time.

For example, BIM is unable to reliably verify if certain information has been authorised by the issuing party. Blockchain could allow all project stakeholders to verifiably issue project related information in real-time by digitally signing and publishing it. Only relevant project participants will be able to see if a digital signature belongs to a specific company or person.

When smart sensors become more common in construction, they will report on aspects such as the curing rate of concrete elements, or the completed installation of components. A foreman could digitally sign off each dataset and a hash for it would be time-stamped and published on the blockchain. The dataset would be uploaded to the project's Common Data Environment to enable all team members to independently validate the hash.

3. **Providing objective data on the best people for a job.**

Contractors often act on human instinct when recruiting for projects and stick with familiar individuals and teams, rather than searching the marketplace for the best qualified. Decentralised marketplaces, based on blockchain, could provide objective data, to help identify reputable contractors and employees, without the need to disclose sensitive personal data to a centralised third party platform, as with existing services.

Limitations of Digital Signatures

A digital signature on a blockchain can be validated by participants that know the public key, or the 'address', of the issuing party. However, the signature does not verify the correctness of the data itself, whether it pertains to a measurement from a humidity sensor, or the content of a signed report. For this reason, moderators may need to by employed and incentivised to resolve disputes.

For example, if a project party signs and publishes a document on an agreed deliverable to the blockchain, all parties, including the Project Manager, can verify that the document has been signed and that the timestamp proves the document was submitted in time. However, this does not guarantee that the content of the document meets the agreed terms.

If someone disputes the correctness of the document's content, there are three possible outcomes:

- All parties talk to each other and attempt to resolve the problem by giving the issuer time to rework and re-issue the document.
- All parties open a case with the moderator, paid a defined percentage of the fee in question, to resolve the issue by checking the agreed terms and the issued document. The moderator can then decide whether or not locked funds should be released to pay the issuing party.
- As a last resort, the case can be handed to lawyers to resolve the dispute, as with non blockchain-based contracts.

Summary

Blockchain technology could play a key role in how supply chains are managed, providing a transparent ledger of transactions to give all participants real-time information about an asset's location, ownership and audit history. The fact supply chains behave more like supply networks than linear 'chains', between resource production and consumers, increases the potential impact of blockchain technology.

© Ethan Rohloff

Implications for the Circular Economy, Internet of Things & Smart Cities

The Circular Economy

The Built Environment is a major consumer of natural resources. As the world's population grows and resources become more difficult and expensive to access, it will become increasingly critical to find alternative methods of sourcing and utilising materials.[23]

Technology will play a significant role in moving the Built Environment towards a Circular Economy, with the potential to allow greater control of resource streams throughout the value chain and enhanced collaboration within the supply chain.[24] If the internet is considered the primary technology layer for the exchange of knowledge and information, blockchain technology can be considered a secondary layer that extends the first by enabling the secure exchange of value, and the ability to permanently and verifiably store information about an asset. Both layers could help realise a truly Circular Economy.

Product Passports

Proposed by the *Buildings As Material Banks Project,*[25] Product Passports hold information about the materials that building products contain, and define their characteristics, thus giving them a value for recovery and re-use. However, at the time of publication, the project provides no methodology for how passport information should be attached to a specific product.

Such information could be stored on a conventional readable label, an RFID tag, in a QR code, or using artificial - or selecta- DNA, but all of these methods are prone to destruction, vandalism or accidental deletion. A copy of all of a country's human passport information is stored on central databases run by the issuing authority, but as described previously in this report, central databases are prone to security issues and attacks.

If Product Passports were stored on a public blockchain, the information would be immutable to change and transparently available, with data on the identity of the issuer and the date simple to verify.

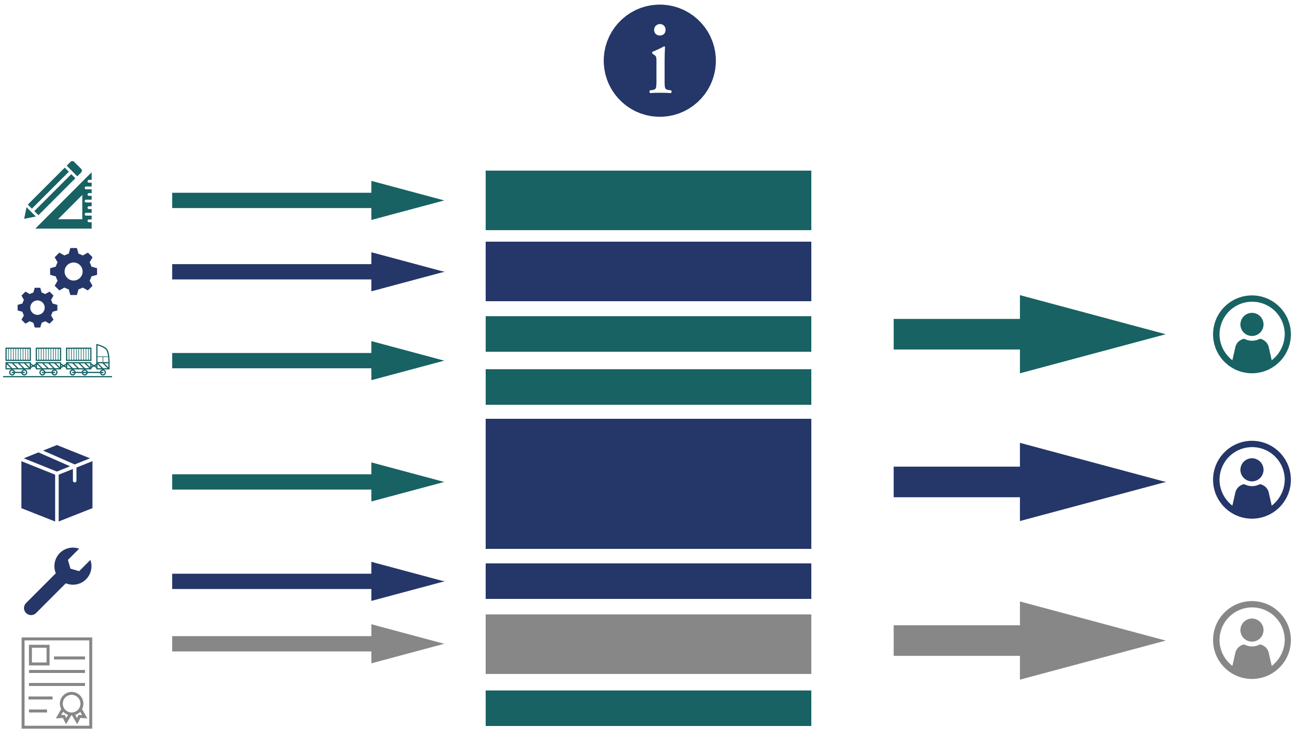
Once blockchain interoperability is in common use, elements within a building's BIM model could be linked to entries in the Product Passport blockchain, making it easy to retrieve information about the materials contained in various components and products (assets) when they reach end of life. This would make it possible to systematically extract and re-use materials, provided BIM data is maintained throughout the building life cycle.

The Internet of Things

The Internet of Things needs a ledger of things.[26] As a huge number of devices, in transportation, infrastructure, energy, waste or water, become connected, there will emerge a requirement for a blockchain-enabled Ledger of Things, a trusted system able to process transactions between autonomously provided IoT services and information sources.

Devices are increasingly being fitted with sensors that record data about their current state, temperature, location, usage history etc. and require an internet connection to make the data accessible to building owners and operators. This is the point where security becomes vital and blockchain could have a role to play in making it work.

However, delivering scalable IoT raises several issues. Smart devices are currently only able to transmit information, and not value, as required in blockchain systems. In addition, IoT networks and devices currently run on a variety of proprietary interfaces and



Materials Passport Platform, EPEA (2017)

> *“On the blockchain, nobody knows you’re a fridge.”*
>
> —Richard Gendal Brown, Chief Technology Officer, R3

protocols, developed by different organisations and manufacturers, which has resulted in fragmentation and a lack of interoperability.

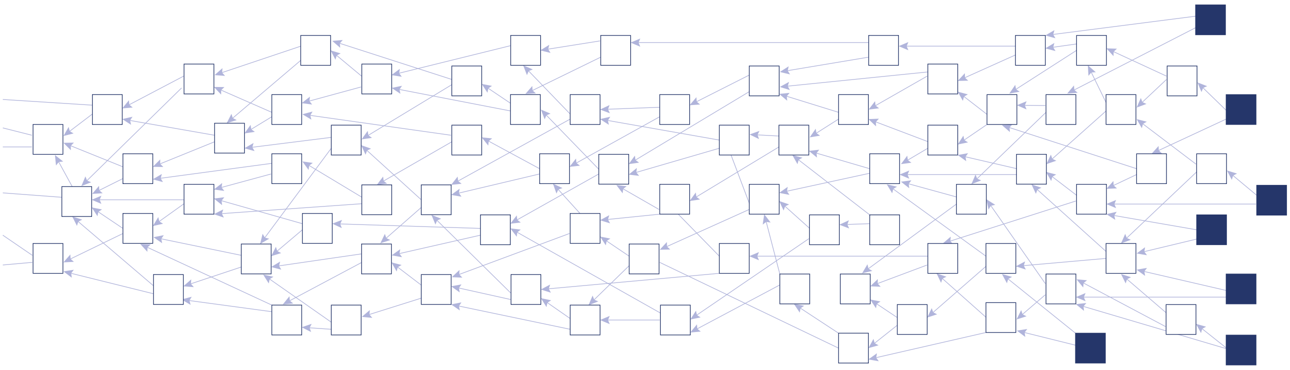
If smart devices are one day able to transmit value on an IoT network based on non-proprietary open standards, then blockchain could become the ideal solution to store IoT information in an immutable, global and decentralised manner. It could function as a value transfer system between machines (Machine to Machine) and individual users, opening up countless opportunities for people in all areas of society. Some specific examples include:

- Smart locks that allow a wider range of users to pay to access a vacant conference room at night
- Delivery vehicles could pay cars in front to switch lanes, to shorten delivery times
- A hospital could track how frequently and where disinfectant dispensers are used, and so identify where more refills are required to increase levels of hygiene.

In the long-term, blockchain technology is essential to unlock the potential of the Internet of Things.[27]

Directed Acyclic Graphs

Instead of building a network that records its current state in a linear blockchain, the IOTA project provides a different approach that is made specifically for the Internet of Things and the billions of devices it might consist of in the future.



Directed Acyclic Graph structure

On the IOTA network, every participant that sends a transaction has to validate two random past transactions.

This results in a mesh of interlinked transactions, and in IOTA, is called a *tangle*. Compared to blockchain systems, this network further decentralises the transaction validation and Proof of Work computation away from highly specialised miners to literally every participant. Another key result of this is that every attempt to harm the network by spamming it actually helps to make it more secure.

With this, the IOTA project provides a very promising approach to large scale smart device interaction, but at the time of writing this report, is still at a very early stage of development and currently lacks real decentralisation. The developer community is still very small[28] compared to its blockchain counterparts,[29] and the network will need Internet of Things hardware to include a dedicated chip specifically made for the hashing function that is used in IOTA to really make it decentralised and secure. Since this is not the case yet, IOTA decided to use a special node called the 'Co-ordinator',[30] run by the IOTA Foundation, that acts as a centrally controlled authority, and basically ensures that no double spends can happen on the network.

The role of the co-ordinator is said to be a temporary measure to help the network securely grow and leave its stage of infancy, but information on when and how the central co-ordinator will be phased out or shut down is not available yet. Currently, participating and having a stake in the project solely relies on the trust in the promise for the closed-source co-ordinator to be shut down.

Smart Cities

The development of Smart Cities is closely linked to the evolution of IoT hardware and software, as increasingly small, cheap and robust sensors, improved firmware and more energy efficient processors, make smart devices more useful and practical to roll out across urban areas.

When IoT networks are linked to an open, immutable ledger of transactions, there is great scope to transform energy efficiency and manage infrastructure more efficiently. The following specific examples give an idea of the broad impact the technology might have:

- The ability to perform transactions on local energy micro grids without requiring operators to authorise a bank transfer for every kW/h fed into, or consumed, on the network.[31]

- Companies that maintain city infrastructure can use a public blockchain to prove when maintenance occurred, making the information transparent and easily verifiable for taxpayers.

- Vehicles, both human-driven and autonomous, could pay for parking securely and by the minute from their own wallet, without the need to search for a parking meter or purchase a defined amount of parking time in advance.

- Citizens of a smart city could vote on the blockchain on district or neighbourhood-wide decisions that impact their daily lives.

Summary

Blockchain technology has the potential, not just to align with current developments in Smart Cities, IoT and the Circular Economy, but in conjunction with the internet, to form the base layer and springboard to enable those technologies to reach their full potential.

BIM with Blockchain

© Arup

Overview

Autodesk describes[32] Building Information Modelling (BIM) as "an intelligent 3D model-based process that equips architecture, engineering, and construction professionals with the insight and tools to more efficiently plan, design, construct, and manage buildings and infrastructure."

BIM is evolving at a rapid rate. Much of the developed world is currently at or working towards the implementation of Level 2 BIM, a level of BIM maturity defined by the use of a collaborative 3D environment with attached data, but created in separate models by different disciplines. Level 3[33] BIM has yet to be deployed, but proposes that all parties work together on a single, shared model, to create much deeper collaboration.

Blockchain technology offers to enhance BIM even further, in the fields of security, liability, transferability, and live data collection. Here we explore the possibilities.

Immutable Record of Changes

As all blockchains are designed to be immutable, transactions on them can be used to permanently record changes to BIM models. Companies in the Built Environment can use existing methods to record changes to a BIM model internally, but when sharing those changes with external collaborators, a blockchain can provide the platform to do this in such a way that the data is time-stamped and cannot be changed or tampered with.

Clients could demand that this method of sharing information be used in their projects when companies issue models to each other, and also when they issue them to the client. Using blockchain-based transactions for BIM processes would significantly increase the level of transparency of the data shared, and therefore increase trust amongst project collaborators, which would go a long way towards reducing corruption and inefficiencies caused by contractual disputes.

Proving Ownership of a Model

Blockchain-based BIM solutions are unlikely to achieve widespread use for several years, by which time the industry will have moved towards a Level 3 BIM implementation. Level 3 BIM proposes that all parties in a project work in a single model, held at a central location, possibly under the ownership of the Client. The central model could simply be a surrogate, combining Revit models from different disciplines, such as the architect, structural engineer, and services engineer, but ensuring that each still has control over their own model. Blockchain technology could allow companies to prove ownership of their model, or individual components within it.

Proving Ownership of a Digital Component

Using blockchain technology, it could be possible to prove ownership of digital BIM components (such as Revit families), and therefore solve intellectual property issues. Revit families for various objects in a BIM model could be linked to a bitcoin address and tracked on the blockchain.

For example, during the design stages, an MEP consultant could create an Air Handling Unit (AHU) family in the BIM model and associate it with an address on the blockchain. Other parties working on the BIM model would be able to see the AHU but would not be able to modify or claim ownership of it. As the project progresses, ownership of the AHU family could be transferred to the contractor by sending a tiny amount of bitcoin on the blockchain to the contractor's address for that component, giving it sole ownership of the family.

Linking the Digital to the Physical

Blockchain technology could help link BIM components to their real-life equivalents on site. When a project moves to the construction phase, real-life components could have an internet-connected microchip added during production to allow them to be tracked on the blockchain, from the manufacturer to the site. The system would ensure that the number of real-life components installed on site matches the number of objects in the BIM model, in the process reducing waste and carbon emissions associated with the over-production of parts and materials, and preventing the loss of time and money waiting for additional components.

RFID tracking could already make this possible, but the associated data could be controlled by one company, whereas with a blockchain-based approach, the data is publicly available and distributed. This allows for vastly improved trust in the system, as well as much greater security of the data.

Decentralised Common Data Environments

A Common Data Environment (CDE) is a central cloud-based repository where construction project information is uploaded and stored, including BIM models, drawings and documents, and accessible by other authorised project parties. The fact that CDEs are centralised introduces security issues and vulnerability to hacking, which is especially problematic when dealing with sensitive or secret projects related to the military, prisons, or government buildings etc.

A decentralised form of CDE is possible if we combine blockchain technology with cloud storage. The US-based company Storj[34] provides a state-of-the-art platform for decentralised, end-to-end encrypted cloud storage, which shreds data into small pieces called 'shards' and stores them in a global, decentralised network of computers. The technology makes the platform faster, cheaper, more secure, and more readily available than centralised counterparts.

The only potential downside of this type of platform is the interface, as CDE's are currently more user friendly. However, Storj and similar platforms, are likely to become easier to use in the future, particularly for business users.

Summary

The 'killer app' for Blockchain-enabled BIM is the ability to link digital components to their physical counterparts, which has the potential to create an entire new paradigm for building data collection and enable truly *live* BIM models, filled with data from individual internet-connected devices. A complete and up-to-date dataset for entire buildings would be extremely valuable for facilities managers when buildings are in operation. These ideas are explored further in the next section of this report called 'The Blockchain of Circular BIM Things'.

The Blockchain of Circular BIM Things

© Transport Scotland

Overview

Four key technologies and methodologies - Blockchain, the Circular Economy, BIM and the Internet of Things - are currently at early stages of deployment and mainstream use. Experts from these fields attended Arup's first Blockchain Technology workshop, held in Berlin in February 2017.

After reviewing the ideas discussed at the workshop, the authors of this report came to the conclusion that all four of these technologies will, to some degree, rely on and complement one another in the future, becoming a critical part of the Fourth Industrial Revolution, which could provide dramatic benefits for the Built Environment.

The use of blockchain is not currently widespread, but most people have heard of Bitcoin, by far the most successful and mature example of the technology, which has been running since the beginning of 2009 and advanced significantly since 2016. Most of the building engineering industry is using BIM at some level and likely to continue to do so, thanks to increased backing by international governments and a clearer understanding by firms of the cost and efficiency benefits. Principles of the Circular Economy (a system that aims to create a more efficient and environmentally-friendly economy through the re-use and recycling of materials) are considered best practice and have been put into use on some construction projects. Meanwhile, the Internet of Things, though facing obstacles related to different proprietary technologies and a lack of standardisation, promises to more fully automate building operation and underpin the realisation of smart cities.

The Circular Economy, if it is to function optimally, will need to operate in tandem with the Internet of Things. BIM models are the ideal 'interface' for accessing Circular Economy related data about buildings, but how can this Internet of Things-powered data be linked to BIM models?

That's where the blockchain comes in – it can act as the link between the other three technologies. This section of the report focuses on the implications of utilising the blockchain to bring about the convergence of these technologies into one big idea we call the *Blockchain of Circular BIM Things*.

Levels of Convergence

BIM Level 4,[35] though still a number of years from deployment, will deal with the social cost of buildings. It could adopt principles of the Circular Economy, helping to better integrate buildings into their environments, as well as the design and construction of them with long-term lifecycle costs in mind, and not just built for the lowest cost. To paraphrase Mark Bew, Chairman of Digital Built Britain, and a participant in the Arup workshop: "these are the costs you don't see on the balance sheet".

BIM models could be updated with real-time data transmitted from disparate IoT devices across a building to provide a powerful overall picture of operation, with great potential to drive efficiency and carry out predictive maintenance. However, this form of integration faces challenges in terms of how to securely connect thousands of devices in a building from different manufacturers in a single ecosystem. The consequences of an attack could be serious, for example a hacker could bypass security and take control of lighting or fire extinguisher systems, or change the settings of ventilation to cause damage.

"The Internet of Things needs a Ledger of Things"[36] in the form of a blockchain to provide the level of security required. Bitcoin has proved its worth, securing actual money, and has never been hacked, making it the obvious choice to secure IoT devices and networks. Advancements in scalability, such as the Lightning Network,[37] will allow for thousands of transactions per second, with tiny fees, and is the ideal solution for Bitcoin to become the Ledger of Things. IoT devices and materials could have a unique identity,

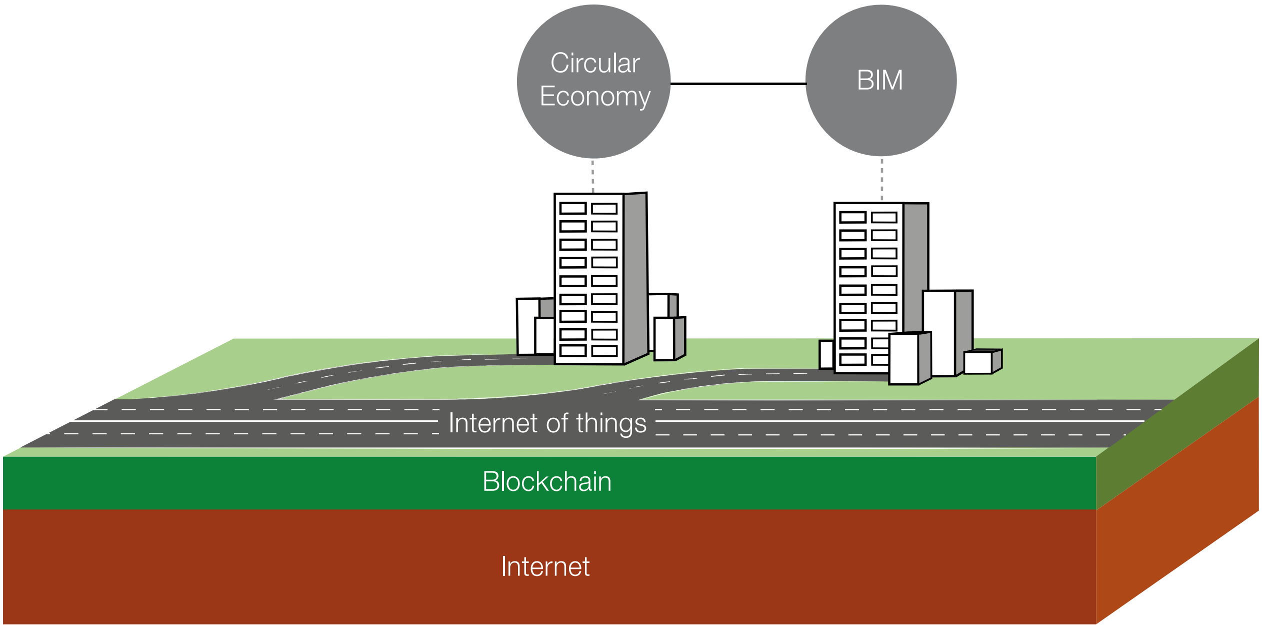
University of Chicago Centre Hong Kong

> *"There is a growing agreement among technology companies that the blockchain is essential to unlocking the potential of the Internet of Things."*
>
> — Don and Alex Tapscott, *Blockchain Revolution* (2016)

allowing their whereabouts to always be known, not just in transit, but in a building. Smart contracts could give IoT devices transactional capabilities, allowing for smart building components and materials that can have their ownership and usage details recorded onto the blockchain, giving companies and individuals an immutable dataset to examine the live usage and history of IoT-connected devices. This would provide huge benefits for the supply chain in terms of live tracking, ownership exchange, and the removal of paper records.

Data captured from a building could be used to accurately predict the remaining lifespan of a device and its suitability for re-use in other buildings or applications, reducing the likelihood of waste and over-supply, therefore cutting down material use and carbon emissions, and underpinning the principles of the Circular Economy.

BIM-inspired standardisation for these technologies will greatly help to advance their use and adoption. The International Organisation for Standardization (ISO) is currently working[38] to create standards for blockchain technology, so things are moving in the right direction.



The layers of the Blockchain of Circular BIM Things

From BIM to Circular BIM

A major limitation with BIM models is that they are only able to provide pre-set information on building components and devices, not *live* information. This restricts them to 'as built' models that generally stop being updated after buildings are constructed.

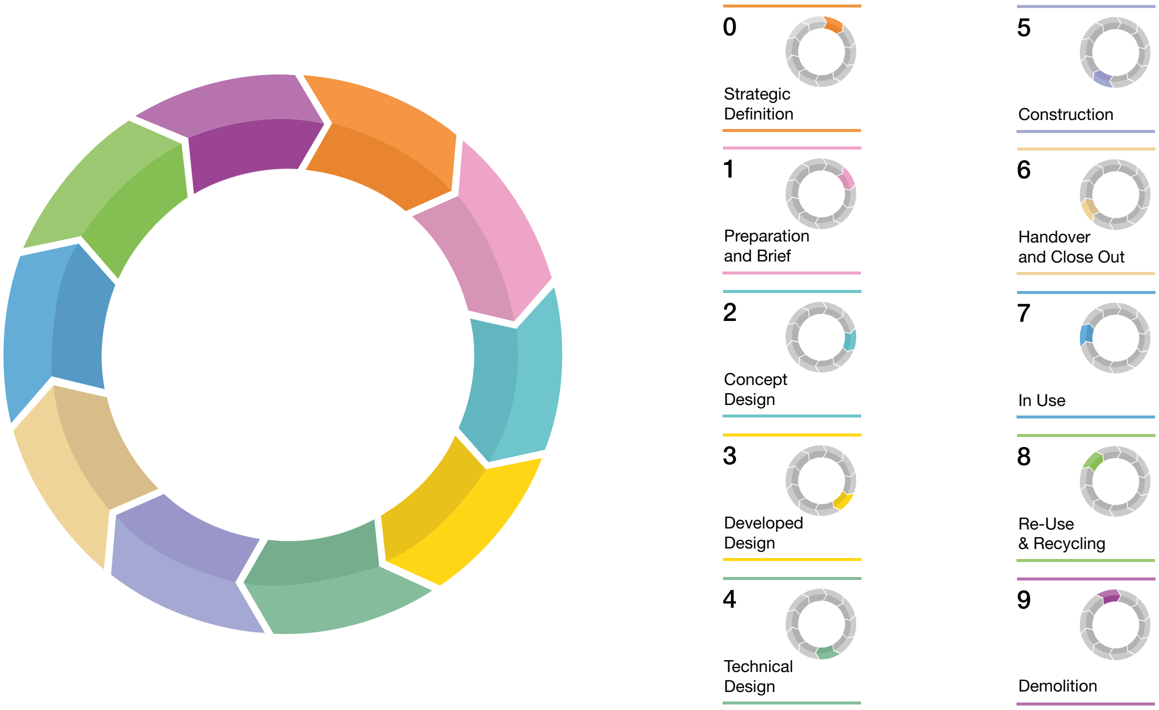
The Blockchain of Circular BIM Things concept offers the solution to this problem by using the internet as the foundation (layer one), with the blockchain and the Internet of Things built on top of it as layers two and three respectively. This would allow machines (or *things*) to transfer, in a live manner, their operational information to BIM models. Therefore, BIM models would become 'as is' models that contain live (or near-live) information about building components, and this data would be extremely valuable for facilities managers, during the 'in use' stage of a building's life cycle. Knowing exactly how every component within a building is operating would be hugely beneficial in terms of performance optimisation, helping to extend their life.

There are three main disciplines of BIM models – architectural, structural and MEP. The latter is the main beneficiary of the operational benefits that the combination of the blockchain and the Internet of Things can provide. However, the other two disciplines can also benefit. Building materials such as walls, structural beams and columns could be tagged and recorded onto the blockchain during construction and then linked to the building's BIM model. When a building is being demolished, this data would be useful for knowing exactly what materials can and cannot be recycled, as well as their whereabouts. In addition, the data would of course be digital and immutable, doing away with paper records that could be lost or destroyed, and eliminating the possibility for the data to be manipulated.

The operational, maintenance and record keeping benefits that the blockchain can provide for BIM models would allow them to become the main digital source of information for the Circular Economy with regards to buildings, thereby creating *Circular BIM models.* This term not only refers to the fact that the information collected would be relevant to the principles of a Circular Economy, but also that the BIM models could be used and updated throughout a building's life *cycle*, from design and construction, through to operation, recycling and demolition.

Post-Handover BIM

7D BIM outlines uses for facilities management applications, which would be implemented during design and construction of a building, and used during its operation. Currently recognized properties of 7D BIM would be utilised before the building is handed over to the client. The Blockchain of Circular BIM



The building lifecycle

Things concept can allow for the first post-handover dimension to be created called ‘Optimisation’. This *eighth* dimension would include powerful new uses for facilities management and the Circular Economy by utilising live BIM models, providing benefits for the operation, re-use and recycling stages of a building. Some potential new properties are:

BIM ‘As Is’ Models (Live Models)
BIM models don’t have to be limited to being ‘As Built’, they can be *‘As Is’*. Model components wouldn’t just have pre-set data, they would collect it from the physical equivalents in the building as they are operating.

Live COBie Data Population and Extraction
COBie parameters could be updated live with performance and energy usage data from the building.

Live and Immutable Operational Data Recording
Information collected from the building would be recorded onto the blockchain, and therefore become a permanent and immutable dataset.

Live Performance Optimisation
It could be possible for BIM components to have performance data updated in the model and synchronised with the actual components in the building.

Live Energy Usage Optimisation
Energy usage of a whole building or even individual devices can be monitored and recorded. Devices could even be switched off via a BIM model to optimise energy usage and reduce costs.

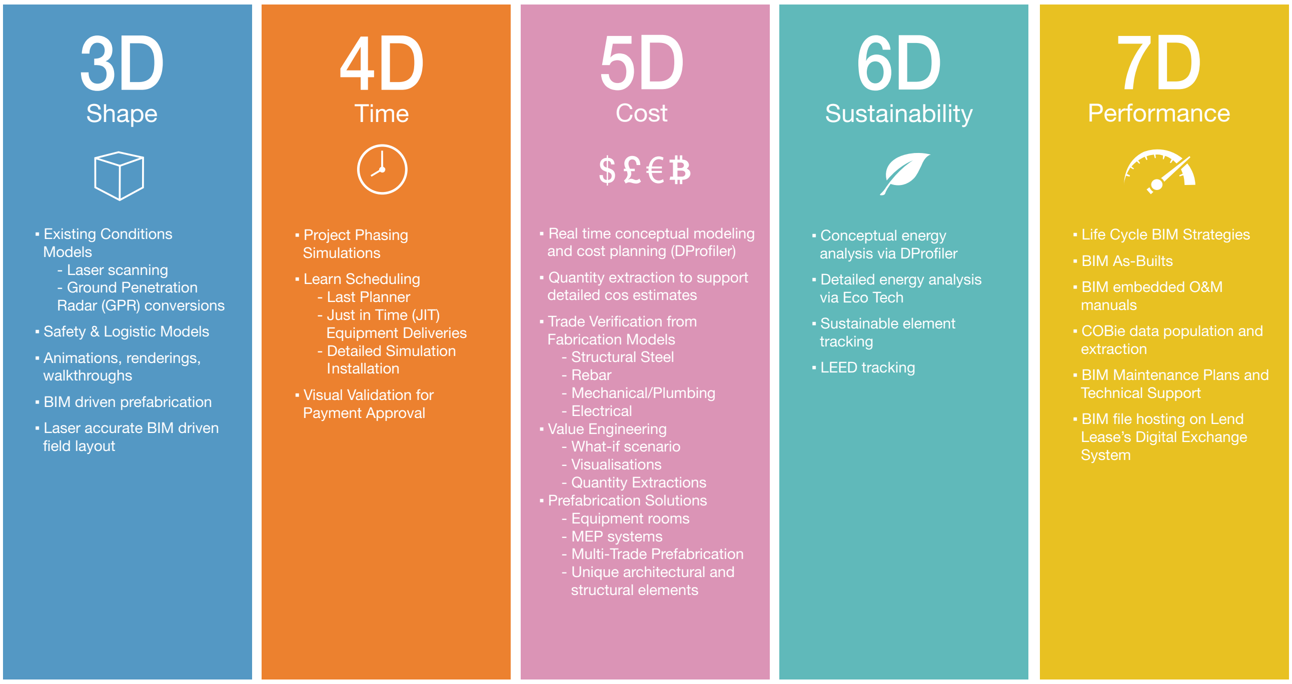
Predictive Maintenance
As energy and performance data can be accurately recorded, this allows for predictive maintenance, reducing the possibility for components to fail, thereby extending their life.

BIM Embedded Live Component Failure Warning System
Since the operation of components can be monitored live, so too could the failure of them. Knowing failures immediately can allow for reduced downtime and disruption to building operations.

Automated Replacement Part Purchasing
As building devices would be part of the Internet of Things, transactional capabilities can be added via Bitcoin. Devices could attach failure codes to transactions and send them to the manufacturer, along with payment for replacement parts.

BIM File Hosting on Blockchain-Based Decentralised Cloud
Rather than using centralised Common Data Environments (CDEs) which could be a security

Pre-Handover BIM Dimensions



3D Shape

- Existing Conditions Models
  - Laser scanning
  - Ground Penetration Radar (GPR) conversions
- Safety & Logistic Models
- Animations, renderings, walkthroughs
- BIM driven prefabrication
- Laser accurate BIM driven field layout

4D Time

- Project Phasing Simulations
- Learn Scheduling
  - Last Planner
  - Just in Time (JIT) Equipment Deliveries
  - Detailed Simulation Installation
- Visual Validation for Payment Approval

5D Cost

$ £ € ฿

- Real time conceptual modeling and cost planning (DProfiler)
- Quantity extraction to support detailed cos estimates
- Trade Verification from Fabrication Models
  - Structural Steel
  - Rebar
  - Mechanical/Plumbing
  - Electrical
- Value Engineering
  - What-if scenario
  - Visualisations
  - Quantity Extractions
- Prefabrication Solutions
  - Equipment rooms
  - MEP systems
  - Multi-Trade Prefabrication
  - Unique architectural and structural elements

6D Sustainability

- Conceptual energy analysis via DProfiler
- Detailed energy analysis via Eco Tech
- Sustainable element tracking
- LEED tracking

7D Performance

- Life Cycle BIM Strategies
- BIM As-Builts
- BIM embedded O&M manuals
- COBie data population and extraction
- BIM Maintenance Plans and Technical Support
- BIM file hosting on Lend Lease's Digital Exchange System

concern, blockchain technology can allow BIM models to be stored on a decentralised and heavily encrypted cloud.

Immutable Life Cycle Energy Usage and Efficiency Record
The accumulated data that could be gathered by the blockchain can allow anyone to view an immutable and complete record of the energy used by a building over its life. The data could be used to compare how efficiently a building has used energy relative to similar modern buildings, and those built in the past.

Immutable Life Cycle Performance Efficiency Record
The performance efficiency of individual components can be recorded, meaning a total figure for an entire building can be calculated. As with energy efficiency, this could be compared to the performance of previous buildings, to measure progress over time.

Immutable Life Cycle Carbon Footprint Record
The carbon footprint of individual devices and even materials could be calculated, giving an overall total. This data would be extremely valuable for helping to identify if a building is meeting carbon emissions targets.

Immutable Recyclable Material and Component Record
The quantity of materials such as plasterboard and steel, as well as IoT devices, that are able to be recycled to some degree, or even reused, could be easily recorded on the blockchain.

Immutable Recyclable Material and Component Location Record
Tying in with the previous use case, this one would help to quickly identity where recyclable components are located exactly, in turn reducing the time to remove them from a building.

P2P Surplus Energy Transfer
In the future, buildings could become net producers of energy. Any surplus energy generated could have its ownership transferred in a peer-to-peer manner to other buildings that require it, enabling buildings to generate their own profit.

Live COBie Parameters

COBie (Construction Operations Building Information Exchange) is a standard[39] for collecting data about a building, during design and construction, for use during operation and maintenance. It is becoming more commonly used, especially in Autodesk Revit MEP, which is the leading software package used to create the BIM models for the mechanical,

Post-Handover BIM Dimension

8D Optimisation

- BIM ‘As Is’ Models (Live Models)
- Live COBie Data Population and Extraction
- Live and Immutable Operational Data Recording
- Live Performance Optimisation
- Live Energy Usage Optimisation
- Predictive Maintenance
- BIM Embedded Live Component Failure Warning System
- Automated Replacement Part Purchasing
- BIM File Hosting on Blockchain-Based Decentralised Cloud
- Immutable Life Cycle Energy Usage and Efficiency Record
- Immutable Life Cycle Performance Efficiency Record
- Immutable Life Cycle Carbon Footprint Record
- Immutable Recyclable Material and Component Record
- Immutable Recyclable Material and Component Location Record
- P2P Surplus Energy Transfer

electrical and public health systems in buildings. The components in buildings that compose these systems will very likely be a pivotal part of the Internet of Things in the future.

If these components are connected to the blockchain, the live data that would be extracted from them could be used to update building operation-focused COBie parameters. Materials could have their information and location data attached to a bitcoin address, which could in turn be used in existing COBie parameters, hence providing a greater link between BIM and data relevant to the Circular Economy.

The definition of COBie could then potentially be changed to ‘a standard for collecting data about a building, during design, construction and operation, for use in performance and energy efficiency, predictive maintenance and material recycling applications’.

Potential parameters include:

HoursInOperation
This parameter would simply show the number of hours the device has been in operation since it was installed. This is useful to record exactly how long a device has actually been used for, rather than just how long it has been in a building, and ties in with some of the other parameters here.

HourlyPowerUsage
This parameter would display how much electricity a component uses per hour.

HourlyElectricityCostOfOperating
This would show the electricity cost of operating the device per hour.

NumberOfTransactionsPerformed
This parameter would show the total number of transactions the device has performed on the blockchain. This is useful for finding out which devices are more active in the Internet of Things, and therefore which ones are possibly more important.

HoursUntilWarrantyExpiration
This shows the number of hours left for the component to operate until its warranty expires. This would be linked to a rating provided by the manufacturer. A live warning inside the BIM model could appear when components are near the end of their warranty period.

HoursUntilRefurbishment
This parameter would display the number of hours left until the device is due for refurbishment or repair, based on the rating provided by the manufacturer. This would utilise the HoursInOperation parameter, and is useful for alerting facilities managers that a component needs servicing, before it fails and causes

Air handling unit

disruption with regards to a building's operation. The early replacement of components due to improper maintenance would increase material and energy usage, which is incompatible with the principles of a Circular Economy.

HoursUntilRetirement
The number of operational hours left until the device is due to be disposed of or recycled.

ExactLocation
This parameter would show the exact real-world co-ordinates of a component. The fact that they would be connected to the internet makes locating them trivial, especially in larger buildings.

CarbonFootprint
This parameter would show the carbon footprint of a single component. It could make use of the HourlyElectricityCostOfOperating and HourlyPowerUsage parameters, as well as the cost to purchase the component to help to calculate a figure.

RecyclabilityGrade
This parameter could record the potential for materials and components to be recycled at the end of their life, based on manufacturer data. Those components with a low grade may not be able to be recycled, and those with a high grade could mostly be.

These parameters would be valuable, as much of the data for equipment related to its operation, maintenance and replacement, which is contained within vast amounts of paper records, could be digitised into a spreadsheet which could be updated constantly, without the need for human input.

The blockchain allows the data that these parameters utilise to be sent to BIM models via transactions. These transactions could be performed every second for some components, and every minute or hour for others, depending on how regularly the information is required. Blockchain transaction costs for collecting a component's data more regularly, such as every second, would be significantly higher, however. The facilities manager would allocate some funds every year for these transaction costs, but would reap the benefits later through performance and energy efficiency gains. This could greatly help to move the Built Environment sector towards adoption of Circular Economy principles.

The Machine Economy

Since no personal details are required to transact with bitcoin, unlike with banks and payment companies, this allows machines (or *things*) to be part of the global economy. They could transact with each other, or with corporate interfaces specially designed for the Internet of Things.

The Circular House

> “
>
> *You cannot have an Internet of Things if you do not have the ability for machines to trade with machines.”*
>
> —Chris Skinner, Writer & Commentator

Any blockchain-connected building components would have a built-in digital wallet, allowing them to store a small amount of bitcoin to be used for performing transactions on the blockchain.

If a device malfunctions, and a new part (or possibly a full replacement) is needed, a larger amount of bitcoin could automatically be sent to it from the facilities manager’s digital wallet so that the device could order the necessary part on its own. The device could transfer details about failed parts to the manufacturer, making part identification easy, and they would send a replacement to the building, which could help to further automate maintenance processes.

Why the Blockchain?

The Bitcoin blockchain is the perfect network for turning the Blockchain of Circular BIM Things concept into reality, as it is ultra-secure, decentralised, immutable, transparent, neutral, traceable and open source. The Internet of Things should be considered a public utility, just like Bitcoin (and the internet itself). As such, it should have similar properties, particularly in relation to security. It would be unacceptable to connect a building to the internet if it meant that there is the possibility that it could be hacked and taken control of.

The decentralised nature of Bitcoin is what provides an exceptionally high level of security, as well as exciting use cases not possible in centralised databases.

Arup Materials Library

A number of large corporations today are joining consortiums that are working to create distributed ledgers (or permissioned 'blockchains'). These types of ledgers are akin to AOL or Compuserve during the early days of the internet, which failed as they were trying to build a wall around a technology which was designed to be open.

The open nature of the internet spawned a wave of incredible new communication platforms shortly after the turn of the century, long after it was invented. The endless possibilities that could be brought about by the Internet of Things, particularly with regards to a machine economy, can only happen in conjunction with an open network like the blockchain. Many of the internet-based applications that people use today were never imagined when it was invented, so there will certainly be innovations built on top of the blockchain in the future that only decentralisation and openness can provide.

From Concept to Reality

How would this concept be realised in the construction industry?

In 2011, the UK government mandated the use of Level 2 BIM on all major public buildings projects from 2016 onwards, as they clearly saw the efficiency and cost benefits of doing so. This made engineering companies take notice, and they quickly began to learn about using BIM processes. They started training employees to use BIM related software, particularly Autodesk Revit, the advanced modelling package for architectural, structural, and mechanical, electrical and public health engineering disciplines.

As of 2017, BIM is hugely more used in the UK than it was at the time of the mandate. This has resulted in a far more collaborative design process which, coupled with newer modelling software packages like Revit, has vastly increased the quality of data made available for buildings during their construction phase. The BIM mandate jump-started an industry which was stagnating in terms of innovation, and breathed new life into the entire building engineering sector. Many other countries have made a similar approach, and are also reaping the benefits.

In a similar manner to BIM, legislation could be implemented by governments to provide the same jump-start needed to get the Internet of Things off the ground, as it is essential to the Blockchain of Circular BIM Things concept. The key to making this concept a reality is getting internet connectivity built into most building components that use electricity. Connecting them to the blockchain would then be trivial.

If legislation required manufacturers to provide internet connectivity in all components used in publicly-funded building projects, as well as a programmable interface, this would enable facilities managers to connect them to the blockchain. Transactional settings determining the frequency of data transfer could then be customised for device categories or even individual devices.

Summary

The Blockchain of Circular BIM Things is an idea to combine the Bitcoin blockchain and the Internet of Things to create the technical solution for integrating the principles of the Circular Economy into BIM models. These *Circular BIM models* would become the dataset not just for the design, construction and operation of buildings, but for their entire usage history. Utilising the transactional capabilities of the blockchain and connecting equipment and devices to the Internet of Things can enable *live* BIM models that are able to monitor performance and energy usage of a building in real-time. This solution can provide enormous benefits for facilities management, as well as the operation, re-use and recycling stages of a building's life.

BIM has so far been a one-way street – data is added to models and used for the construction and operation of buildings. The Bitcoin blockchain can record the operational data from buildings permanently and securely, which can be fed into BIM models. Operational parameters for digital components could therefore be updated in a model and synchronised with the real-life equivalent in the building, allowing for live performance optimisation, and even predictive maintenance. This can happen without the need for trusted intermediaries.

Building materials and components can have information embedded within them that pertains to their recyclability potential, thereby allowing BIM models to contain more Circular Economy-related data. The Blockchain of Circular BIM Things idea offers a new BIM dimension – 'Optimisation' – which could be the first post-handover dimension, and includes benefits for Circular Economy principles brought about by the blockchain.

With the blockchain set to become the 'Ledger of Things' for the Internet of Things, this enables the exciting possibility of a machine economy, where *things* transact with each other. This could automate building maintenance procedures by allowing building components to alert their manufacturer when they break down, and then even pay for their own replacement parts.

With BIM becoming the norm in the engineering sector around the globe, and with sustainability being an ever more prevalent issue, the ideas of the Circular Economy will become more entrenched in the industry. With the inevitable rise of the Internet of Things, and its likely integration with the Circular Economy, it becomes clear that the blockchain could, in the future, serve as the fuel that *powers* them, as well as being that which propels BIM to the next level. All three can benefit enormously from the security and transactional capabilities of the blockchain.

© Tim Evanson

The Legal Implications of Blockchain Technology

Overview

Blockchain technology will have a profound effect on the legal sector and legislation in general, not least because open blockchains are decentralised and global in nature and therefore they exist outside the boundaries of conventional laws defined by jurisdiction. The law, institutions, and society in general will have to adapt to the blockchain revolution.

Implications for Businesses

Reduction of Contract Disputes

Clients may one day require the use of smart contracts on building projects to reduce disputes, especially during construction. In a similar way to how BIM involves parties collaborating more at the earlier stages of a project to save time and money, smart contracts could be defined and utilised early on[41] to facilitate legal collaboration.

Essentially, smart contracts could transfer the legal costs associated with dispute resolution from the middle and end of a project to the start, greatly reducing them in the process.

Organisations could work with the client's lawyers from the outset, to define rules and a detailed set of contingencies to apply throughout design and build to handover. Any party that fails to meet the terms laid out in the smart contract, would be automatically penalised, possibly with a fine, or alternatively the client could opt to extend the period of time for an organisation to complete a task. A range of different scenarios could be written into the smart contract to reduce, or even eliminate, the need for the client to engage in renegotiations mid-project.

Legal Programmers

Many business operations are being automated to reduce human error and lower costs, and laws may become enforced in a purely digital manner using smart contracts, to enable similar benefits for the legal sector. There may emerge a demand for so called 'legal programmers' who combine the functions of lawyer and competent coder, particularly in relation to blockchain scripting. Employed by the client, or other companies in the Built Environment sector, these individuals would define and code rules into smart contracts.

Data Storage

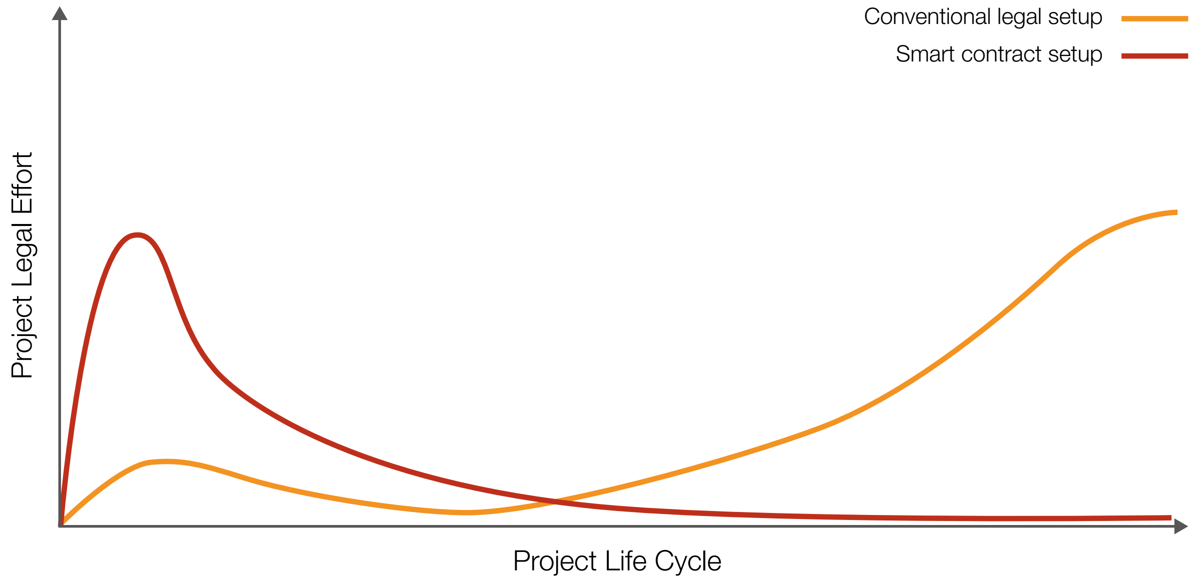
Blockchain technology underpins decentralised cloud storage platforms, such as Storj, with increased security, more uptime, faster speeds and lower costs relative to traditional cloud storage. However, while centralised cloud storage companies can be held liable in the event of hacking, outages or loss of data, this may not be possible with decentralised platforms where no individual or company is in control.

Auditing Laws

Blockchains may remove or alter legal requirements for organisations to undergo audits or employ auditors. Blockchains, notably Bitcoin, are public and immutable, so firms can use them to publicly prove they comply with rules.

Multi-Signature Contracts

Transactions on the blockchain can either be single-signature or multi-signature. Most transactions are single-signature and involve two people usually. Multi-signature transactions, involving a number of different people, are more complex and require a private key to an address to be split into a number of pieces, with each piece allocated to a different person. Funds on an address cannot be spent unless a predetermined number of people sign to spend them. For example, if a multi-signature address is 'three of five', then at least three people must sign in order



Conventional vs smart contract legal costs

> *“We can take many of the basic concepts of the current system that depend on legal contracts, and we can convert these into algorithmic contracts, into mathematical transactions that can be enforced.”*
>
> —Andreas M. Antonopoulos, Technologist

to spend the funds. If less than three sign, the wallet software will not permit it.

Multi-signature transactions could become an extremely powerful tool in the future. Companies could use them for decentralised decision making, for example board members could vote for company changes using their private key, allowing for a cryptographically secure, public record of voting.

Smart Legality Checking

Smart contracts could enable companies to automate[42] some legal processes. If a government law database was transformed into a smart contract, comprising a list of all laws in a country converted into code, companies could check their own legal smart contracts against the government’s to ensure that they comply with the laws applicable to that country. The government database could be live-updated with new laws, and automatically notify companies of changes, saving time and money spent on research.

Intellectual Property

Blockchain technology can allow individuals and organisations to publicly prove ownership of intellectual property, eliminating any uncertainty as to the owner. An example could be Revit families within BIM models.

Map of nodes around the world, Storj network nodes

Sensitive Information

The immutability of blockchain technology has a negative side in that undesirable information embedded into a blockchain cannot be removed. Personal employee or sensitive project information could be uploaded to a blockchain and would have to remain there for all to see, with the associated legal implications. However, this downside is mitigated by the fact that any sensitive data is buried amongst other information and would need to be specifically searched for. The risk is also arguably no different from the World Wide Web, where personal information can be uploaded to a website and never fully removed, except in cases where law enforcement would intervene.

Implications for Society

Laws Cannot be Applied to Blockchains

All blockchains are decentralised and global, therefore they cannot be shut down by any one legal system. This makes them extraordinarily resilient, and allows for use cases never possible before, such as decentralised currencies, companies, marketplaces, and more.

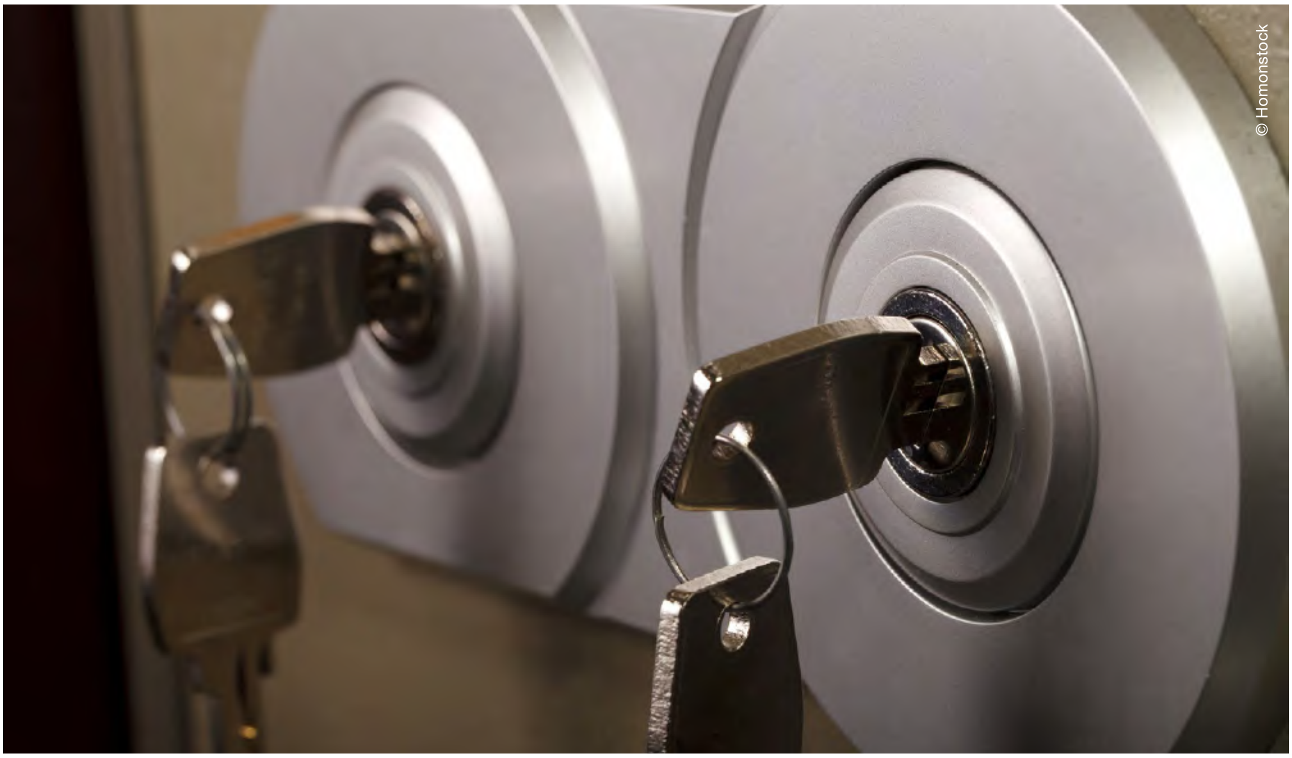
DAOs

Decentralised Autonomous Organisations, i.e. corporations that exist solely as computer code in the cloud, are a potentially hugely disruptive force for society. Although individuals who invest in a DAO are liable, the DAO‘s themselves operate outside of conventional law and cannot be shut down or modified by regular government-enforced laws, so if something goes wrong, for example if funds are lost due to a hacking attack, then liability is difficult to assign. However, as with *The DAO,* which was built on the Ethereum blockchain, it is possible for investors to get their money back, but only if the blockchain is forked, which is highly controversial and not guaranteed to happen.

DAOs essentially allow any individual to start their own company without having to complete legal forms, comply with any laws, or register the company. It is possible that in the future, DAO-building websites or computer programs will launch to enable users to create their own decentralised company, choose a name for it, and define its operational properties.

ICOs

An Initial Coin Offering is the blockchain equivalent of an IPO that allows the public to buy a share of a company's blockchain tokens in exchange for other tokens. For example, a company could sell a 10% stake in its business as new blockchain tokens, bought by the public using a digital currency like bitcoin or ether. This is an extremely fast and simple way for businesses to raise money to allow them to expand.



Multi-signature keys

> *"You can't stop things like Bitcoin. It will be everywhere and the world will have to readjust. World governments will have to readjust."*
>
> —John McAfee, Founder, McAfee Associates

While some ICOs are legitimate, many of them are scams looking for money to create a 'pump and dump'. The founders hype their platform before its launch, which creates excitement amongst certain investors who buy some of the tokens, raising their value. The founders then sell their own tokens (which they allocated to themselves for free) when their value has risen significantly, which crashes the price and earns the founders large sums of money. This can leave regular investors in the ICO holding tokens with a significantly reduced value, meaning their investment may never break even.

The United States Securities & Exchange Commission (SEC) has warned[43] the public about the dangers of investing in some ICOs. Government agencies will most likely start regulating ICOs in some way in the future. This could have a positive effect on the blockchain industry as a whole, as it would provide confidence to investors and members of the public.

Tax Laws

Blockchain-based digital currencies exist completely outside of traditional finance, forcing tax legislation to adapt. If blockchains become widespread, either in a single country or globally, governments may have to reduce income taxes and increase VAT. Unscrupulous individuals could use digital currency to hide their money and evade tax, and this may trigger an increase in taxation on the general population to recover the funds lost. Digital currencies can be obtained in a 'peer-to-peer' manner through decentralised exchanges

© Underworld

The darknet

that allow people to buy and sell digital currency without having to adhere to Anti-Money Laundering (AML) and Know Your Customer (KYC) laws.

The *Panama Papers*, leaked in 2016, exposed the level of tax evasion in the traditional fiat financial system. The potential risks of anonymous, decentralised digital currencies are comparatively much greater as no shell companies, expensive lawyers, or papers are needed. All that is required to hide digital currency is a small, cheap hardware wallet. The money could even be hidden within someone's brain as a password.

Darknet Markets

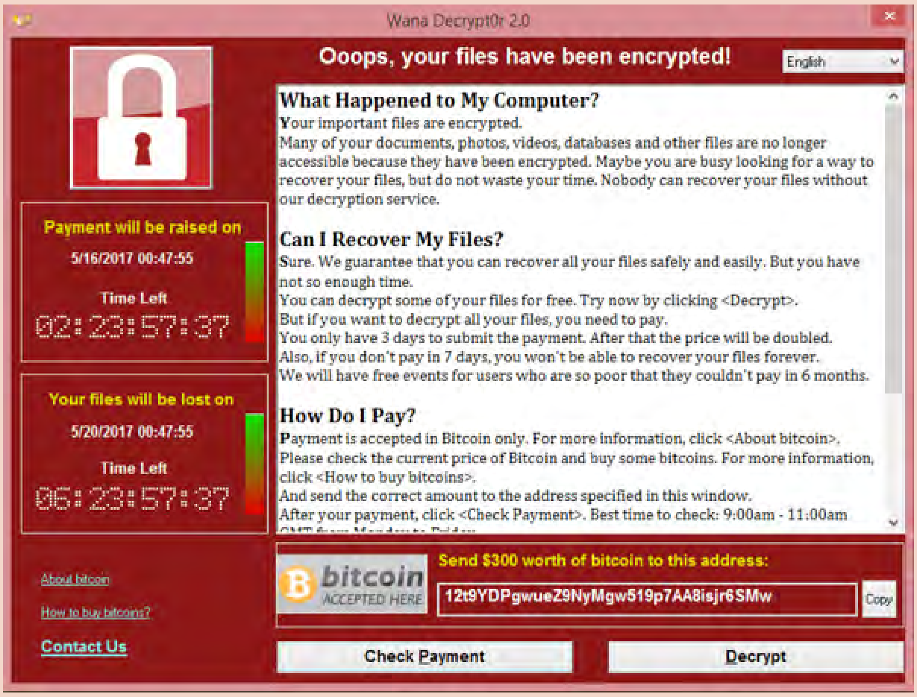
For several years, Bitcoin has been the currency of choice on darknet markets where large quantities of illegal drugs are sold. Other blockchain-based currencies, such as Monero and Zcash, are starting to take over this role due to their higher level of anonymity. Law enforcement have had some success in tracking down criminals due to the relative transparency of the Bitcoin blockchain, but as fully anonymous currencies on darknet markets become more commonplace, it may be extremely difficult or even impossible for law enforcement to track the movement of funds.

Gambling

Gambling is currently outlawed in many countries, but blockchain-based gambling websites would be very difficult to shut down because the monetary system exists globally and outside the control of any government. Decentralised downloadable programs could allow people to gamble without the need for a centralised website with a named owner, making it impossible to outlaw. On the positive side, some existing websites that allow people to bet with digital currencies have been proven cryptographically fair, meaning that the company owner/operator cannot cheat.

Unaccountable Theft

Blockchain-based digital currencies must be properly secured by the user, or they will be vulnerable to theft. As transactions are irreversible, stolen funds could not be returned, and the high degree of anonymity of many digital currencies makes it unlikely that thieves could be caught. However, hardware wallets can provide extremely high levels of security, coupled with good usability.



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

© Malware

Wannacry Ransomware Virus

ARV (Autonomous Ransomware Virus)
Autonomous Ransomware Viruses could be initially programmed into a DAO by a human being, to infect individual and corporate computers and hold them to ransom. The use of powerful encryption would force users to pay, in digital currency, to regain control of their information, with the funds held by the ARV and periodically sent to its anonymous creator. Some of the funds could be used to help expand the virus to infect more devices.

Summary

The decentralised nature of blockchain technology has serious legal implications likely to impact on currency, companies, contracts, databases, data centres and more. One tremendously positive use case is the ability to instantly, securely, and privately transfer money to anyone in the world, at any time, without regulation - after all, sending an email doesn't require government approval for most people, so why should sending money?

Many of the legal implications with regards to society are quite negative, but the technology's use in this manner will be very small in the grand scheme of things, as there are far more law abiding citizens that would use blockchains for positive use cases.

Decentralised technologies are almost impossible to shut down, which is controversial, but an important characteristic for their survival. This has proved to be the case with the internet, whose decentralised approach allowed it to expand, become popular and deliver numerous benefits for society. The same will be true for blockchain technology.

© Wanchai

Smart Travel for Smart Cities: A Thought Experiment

Thanks to blockchain technology, an anonymous individual (let's call them The Creator) possibly could, in a few years from now, launch their own company called AutoCab, with the following attributes:

- Create it as a smart contract known as a Decentralised Autonomous Corporation (DAC), built on top of the Bitcoin blockchain. This means that no one would be in charge of it, not even The Creator, who would be anonymous, as would the location and amount of profit The Creator would earn from this corporation.

- Fund it via an ICO (Initial Coin Offering), issuing company shares as tokens on the blockchain to stakeholders.

- The stakeholders could review the company's open source code for errors, and could also issue updates, only with the approval of the majority of the stakeholders (>95%). This protects the code from being manipulated by malicious actors, whose incentives may not be aligned with those of the stakeholders.

- Stakeholders would not be refunded in the event of a catastrophic hack, unlike with The DAO, and the blockchain would not be forked in such an event. Stakeholders assume all risk.

- The company would regularly and autonomously issue profits to the stakeholders and also to The Creator.

- The company's business model would be to offer a taxi service, utilising a fleet of solar powered electric autonomous aerial vehicles (AAVs). This eliminates the cost and errors associated with human pilots/drivers.

- Being aerial vehicles rather than ground vehicles, they would not be confined to the restrictions of roads that do not point exactly in the direction of the destination. This saves time in terms of travel, reduces the cost of travelling, and reduces emissions. It would also reduce other huge costs such as road upkeep as there would be less cars on the roads.

- They would not be required to follow road traffic laws as they are aerial vehicles. They would be fitted with a collision detection system to avoid buildings and other aerial vehicles. A decentralised AAV traffic control system could also be implemented. The AAVs would be fitted with an air horn to scare away birds, to avoid mid-air collisions.

- Due to the lack of human pilots/drivers (that require sleep), profits could be maximised by running the AAVs 24 hours a day.

- Payment from passengers would be made using bitcoin via the AAV's built-in bitcoin lightning network payment channel. All payments would be secure, instant, anonymous and non-refundable - digital cash.

- Upon entering an AAV, one of the passengers would be required to pay a deposit. Tiny surveillance cameras on the inside and outside of the AAVs would record all activity. The deposit would be revoked if any of the passengers cause damage to the AAV. All surveillance footage recorded during the rental period would be automatically deleted upon return of the deposit at the destination. This could also allow the company to assign liability in the event of deliberate damage to any AAVs.

- The AAVs would connect with customers via a decentralised version of Uber, to remove that middleman, maximise profit margins and eliminate legal disputes. Costs for customers would be even lower as tips would be eliminated because there are no human pilots/drivers.

- The AAVs would pay for their own repairs and upkeep at a local drone maintenance centre via a Bitcoin blockchain powered smart contract. A portion of company profits would autonomously be kept aside to pay for this.

- Roads would be less congested as most ground-based human taxi drivers would be made redundant. The AAVs would be unable refuse customers based on age, race, gender etc.

- The sheer time and cost savings for regular humans using this type of transport would allow the company to autonomously set aside a portion of its profits for capital acquisition (purchasing more AAVs). This would allow the company to rapidly expand its AAV fleet and eliminate most human, ground-based competition.

- Having taxis be AAVs would be a much more exciting experience for customers than current ground-based taxis. This would be a strong incentive for attracting customers, allowing for the company to grow at a rapid pace.

All of the technologies in this interesting example will be a reality within a few years, with many of them available now. With technology currently advancing at an incredible rate, many things that seem new and cutting edge right now, may be ‘Uber’d’ in the near future, ironically including Uber itself. If software developers can create mobile Dapps (decentralised apps) to allow individuals to use a decentralised network like Bitcoin, the same can be done for a decentralised version of Uber eventually.

Passenger drones are currently being explored as a better alternative to road-based travel. There will most likely be operational examples within a few years. Passenger drones aim to automate travel, and Decentralised Autonomous Corporations (DACs) aim to automate the operation of entire businesses. Blockchain technology allows for the creation of DACs, so the AutoCab company, funding and operating structure is possible now. It is more likely that passenger drones will be operated and maintained by traditional companies at first, because drone development and adoption is currently far ahead of that of DACs. However, in time, DACs will inevitably become more adopted by society as a whole, especially if there are strong incentives for doing so.

The challenge for those in the Built Environment sector, which includes Arup, is how to adapt to the changes to society that the above example (and others like it) could allow for. Technologies like these are going to happen. Those within the Built Environment sector should research them to be in a position to take advantage of the positive opportunities and innovation they provide, particularly with regards to the ideas of a Circular Economy, but also prepare for any challenges they present, especially from a legal perspective.

© Sergey Yarochkin

Quant: The Engineering Currency

Overview

Quant is a new cryptocurrency that is currently being developed in the U.S. by a group[42] of engineers, led by Daniel Robles, founder of the Integrated Engineering Blockchain Consortium.

Quant's purpose is to enable a global network of engineers to record and share their knowledge, enhance collaboration for the good of the profession, and reward them more appropriately for the vital role they play in society. The credentials of those already involved with the project are impressive, and it has the support of industry partners such as IBM and Lockheed Martin.

Similar to the website LinkedIn, Quant can act as a social network that provides access to engineer's qualifications, skills and experience. The system enables an engineer who requires help on a project (defined as a student) to connect with another engineer able to provide assistance (defined as a teacher). Students find teachers by searching the network using keyword searches and all identities are kept private until connections are made.

Rather than charge a fee to access the service, as with LinkedIn's premium service, Quant's blockchain acts as a decentralised intermediary, taking no payment and instead awarding engineers with free Quant 'tokens' as an incentive to join.

Quant's tokens, built into its blockchain, are awarded to engineers who verify the credentials of anyone else who joins, thus 'linking' everyone together to form a network. More Quant is awarded when engineers upload information to its blockchain about projects they worked on, case studies, or analysis etc., or if they engage in 'smart contract' transactions with others to share knowledge. The experience and reputation of an engineer can therefore be gauged by analysing Quant award and verification history, and this acts as a 'certification'.

There is the potential for Quant to become a key knowledge and reference resource for the engineering industry, in which case the currency could represent engineering productivity. The more engineers that use this blockchain, the more valuable it would become. Quant tokens could even be sold on the open market in exchange for traditional currencies.

Daniel Robles has defined the modern economy as a three-legged stool that involves banking, insurance, and engineering — break off one leg and the stool falls over. Since engineering is the only field out of the three that creates physical things, such as buildings, he claims the information engineers provide to create them should have similar value to that evident in the financial industry. Quant allows any amount of engineering knowledge to be quantified in value terms, and this value could be sold to the other two sectors when they require it, in the process allowing the engineering industry to be more fairly rewarded.

Quant operates differently to other blockchains. It consists of licensed engineers, who generate digital tokens by solving real-world problems, not by mining for hashes. The security of the network is provided by the engineers, instead of a hashing program generating cryptographic keys.

What could make Quant a game changer for the industry is how it might support insurance and finance. The Quant blockchain only enables contracts to be generated and settled by professional engineers, which reduces the risks associated with using it and makes it more attractive for one of the other legs of the stool — the insurance industry — to insure. Allowing blockchain-based contracts to become insurable would encourage banks to participate in projects using Quant, creating a whole new paradigm of collaboration for those involved in future engineering projects.

Over the last twenty years, 'platforms' have become more and more prevalent, massively disrupting many industries. The auction platform eBay usurped the idea of people bidding at physical auctions, and the e-commerce platform Amazon enabled businesses to reach a much wider market for their products than having physical stores. Quant has the potential to become the disrupting platform for engineering, however, it offers to *enhance* it, rather than replace existing companies in the sector.

Bitcoin, the first ever blockchain, is an extraordinary human achievement, but its currency units have no 'intrinsic' (or built-in) value. In fact, most things in the world have no intrinsic value whatsoever. Value is applied by people, and most things only have value because people *think* they do. Engineering is about creating the things that people really *need*, such as homes, buildings and transport, some of the essential elements of modern life. The Quant currency has been described as having intrinsic value, by capturing and linking the value associated with the knowledge, skills and experience of engineers to it. This could strengthen the engineering industry and increase the rewards for those who are part of it.

Summary

Quant is a new cryptocurrency that is built specifically for the engineering industry. It creates a globally connected network of engineers and an immutable record of the knowledge that they share, which could enhance the engineering profession enormously. The currency can be linked to the knowledge, skills and experience of engineers, thereby arguably giving it intrinsic value, potentially allowing the industry to gain additional income for the services that it provides. Quant can be earned by engineers uploading information about projects that they worked on, helping other engineers, or providing valuable (and vital) knowledge to external parties. This could be the type of platform that disrupts engineering, the Uber of the sector. If individuals and companies within the sector embrace systems like Quant, the industry could really benefit in terms of more collaboration, which would mean problems could be solved faster, cheaper and better.

First Arup Blockchain Technology Workshop

Arup hosted its first ever workshop on blockchain technology at the Berlin office on February 6 and 7, 2017. The event brought together leading experts from organisations in the fields of Engineering/Construction, Business/Consulting, Legal, and Bitcoin/Blockchain, including Arup's own staff, to discuss the potential future impact of this innovative technology.

The workshop began with presentations, delivered by the authors of this report, that explained blockchain technology in detail. The entire group then discussed various pre-defined topics related to potential use cases, the impact on society, and their own fields of expertise.

A 'World Café' section saw participants discuss different topics in small groups. In addition, a supply chain role-playing exercise was set up to explain the difference between current opaque flow of construction sector payments and a more open and transparent method of payment using the blockchain. This also highlighted the advantages in terms of reducing corruption in construction.

An attendee from Deloitte played a video clip that explored four potential scenarios[44] for blockchain technology in the future. Two attendees from Volkswagen Financial Services presented a smart contract-based web application they created.

Free bitcoins were distributed to participants, kindly donated by Nicolas Cary, President and co-founder of Blockchain, the world's most popular Bitcoin wallet, to enable them to test out the technology on their smart phones.

The response to the event was overwhelmingly positive, many participants said they learned a great deal, particularly with regards to the technology's potential impact on their own profession. Many of the ideas and lessons from the workshop were incorporated into this report, particularly those related to BIM.

© Arup

Participants

Arup
– Associate, Foresight + Research + Innovation
– Associate, Foresight + Research + Innovation
– CAD Technician, Host
– Consultant, Host
– Engineer, Building Performance & Systems
– Industrial Trainee
– Industrial Trainee
– Senior Engineer
– Solicitor

Deloitte
– Chief Data Scientist

Ellen MacArthur Foundation
– Research Analyst

Harper Macleod LLP
– Partner

HM Government BIM Task Group
– Chairman

Körber AG
– Management Consulting

Monax
– Senior Product Manager

Planned Cities
– Entrepreneur

PricewaterhouseCoopers
– Consultant
– Consultant

Skanska
– Director, Innovation and Business Improvement

VW Financial Services AG
– Corporate Strategist
– IT Innovation Manager

Agenda

The workshop agenda was structured in such a way as to first explain the technology, then explore the potential use cases and impact on society, and then discuss major topics which are critical to the technology, as well as the participants.

The entire workshop agenda topics are shown below:

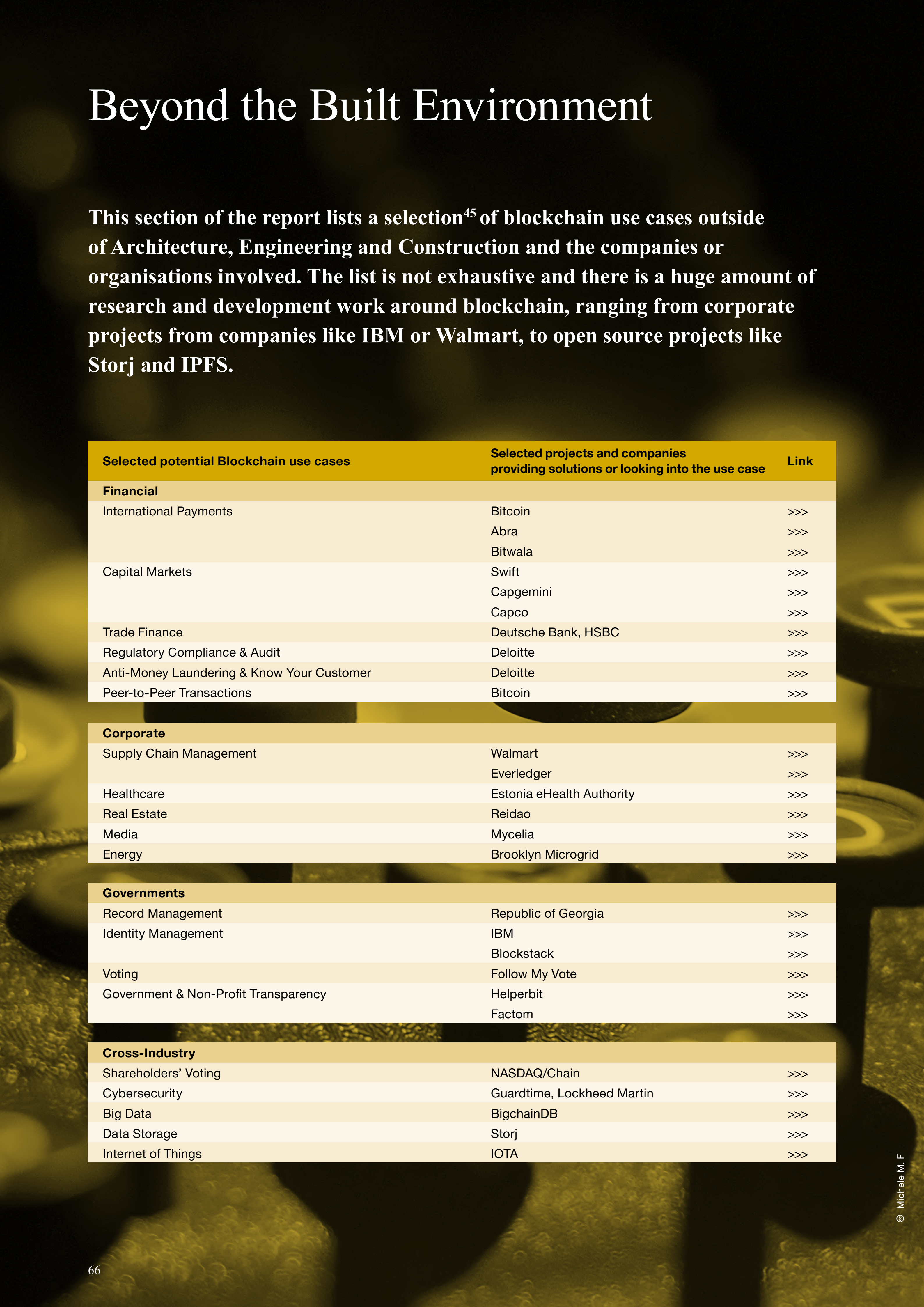
Day One — Monday 6th February 2017
– Who Are We & Why Are We Doing This?
– Participant Introductions & Expectations
– How the Bitcoin Blockchain Works
– What is Blockchain Technology?
– Blockchain Use Cases
– World Café
– Bulletproof Blockchain
– Smart Contracts, Machine-to-Machine Payments & Distributed Autonomous Organisations
– Hands-on Experience — Transact on the Bitcoin Blockchain

Day Two — Tuesday 7th February 2017
– Blockchain for the Supply Chain
– Decentralise All the Things
– Blockchain for the Built Environment & the Circular Economy
– The Legal, Economic & Tax Implications of Blockchain Technology
– BIM Presentation from Mark Bew
– Conclusions & Final Thoughts

Beyond the Built Environment

This section of the report lists a selection[45] of blockchain use cases outside of Architecture, Engineering and Construction and the companies or organisations involved. The list is not exhaustive and there is a huge amount of research and development work around blockchain, ranging from corporate projects from companies like IBM or Walmart, to open source projects like Storj and IPFS.

Selected potential Blockchain use cases	Selected projects and companies providing solutions or looking into the use case	Link
Financial		
International Payments	Bitcoin	>>>
	Abra	>>>
	Bitwala	>>>
Capital Markets	Swift	>>>
	Capgemini	>>>
	Capco	>>>
Trade Finance	Deutsche Bank, HSBC	>>>
Regulatory Compliance & Audit	Deloitte	>>>
Anti-Money Laundering & Know Your Customer	Deloitte	>>>
Peer-to-Peer Transactions	Bitcoin	>>>
Corporate		
Supply Chain Management	Walmart	>>>
	Everledger	>>>
Healthcare	Estonia eHealth Authority	>>>
Real Estate	Reidao	>>>
Media	Mycelia	>>>
Energy	Brooklyn Microgrid	>>>
Governments		
Record Management	Republic of Georgia	>>>
Identity Management	IBM	>>>
	Blockstack	>>>
Voting	Follow My Vote	>>>
Government & Non-Profit Transparency	Helperbit	>>>
	Factom	>>>
Cross-Industry		
Shareholders' Voting	NASDAQ/Chain	>>>
Cybersecurity	Guardtime, Lockheed Martin	>>>
Big Data	BigchainDB	>>>
Data Storage	Storj	>>>
Internet of Things	IOTA	>>>



© Michele M. F

What Blockchains Won’t Solve

Many companies are in the process of trying to understand the implications of blockchain technology, and others still have false expectations of its capabilities and future applications.

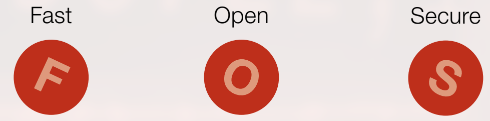
Blockchain should not be thought of simply as a data structure and its success will heavily depend on the specific implementation used. For example, a ‘closed-ecosystem’ blockchain cannot solve issues related to centralised control.

Bitcoin is one of the most open and secure blockchains available, defined by its robust underlying cryptography, high level of network decentralisation, immutability and related computing power.

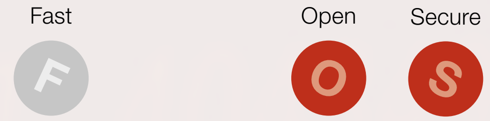
Although transaction settlement times are extremely rapid compared to traditional financial networks, relative to other blockchains, it is much slower in terms of activating development changes and achieving community consensus. This trade-off is a result of the open nature of the system, without a single entity in control of its future, and is something that is mostly looked upon positively among Bitcoin users.

Closed (or permissioned) blockchains can be fast and reasonably secure but lack the advantages of open participation. Their central authorities, which may comprise one or several entities, could be prone to manipulation, which reduces the security of the system. Blockchain technology alone will not prevent human greed or crime, but it does help create a system that is resilient to these types of behaviours.

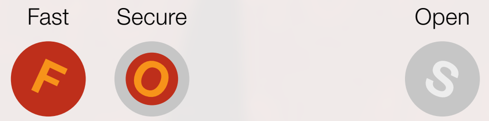
Any blockchain implementation will involve some form of trade-off between being fast, open and secure, and only two of these qualities can ever be present at the same time.



For the Bitcoin blockchain the illustration would look like this:



Permission-based blockchains are geared more towards speed of decision making and control at the expense of openness:



© Blogtrepreneur

© Nasa

Conclusion

Since the inception of the Bitcoin blockchain in 2009, the ledger for global transactions has managed to achieve 24-7/365 availability and over 99.99% uptime[46], with zero hacks and many updates and improvements to its codebase. Given this impressive track record, perhaps now is the time to recognize the benefits that blockchain technology can bring to individuals, companies and society as a whole.

Much like the now omnipresent internet, blockchain technology has the potential to change the world for the better, and even power the fourth industrial revolution by building a new foundation for machines and humans to interact and transact with each other. The implementation of a trust network can underpin huge operational improvements for many industries, particularly those prone to corruption or disputes.

Blockchain could help turn around stagnating output in construction, relative to employment,[47] by improving contract management, enabling more transparency in supply chains, and providing the technological backbone needed to combine aspects of the Circular Economy, BIM, IoT systems and smart sensors. It adds a new layer on top of internet infrastructure for the tamper-proof exchange of value and information.

The risks associated with Satoshi Nakamoto’s agnostic protocol are not insignificant, but just as the internet brought with it benefits of open innovation and transparency, blockchain can deliver huge advantages for society as a whole.

1. https://bitcoin.org/bitcoin.pdf
2. http://hackingdistributed.com/2017/06/19/bancor-is-flawed/
3. http://www.coindesk.com/understanding-dao-hack-journalists/
4. https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/
5. https://trends.google.com/trends/explore?date=all&q=blockchain
6. http://www.information-age.com/emerging-bitcoins-shadow-rise-blockchain-123461780/
7. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
8. https://miguelmoreno.net/wp-content/uploads/2013/05/fYFBsqp.jpg
9. https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
10. https://bitcoin.stackexchange.com/questions/161/how-many-bitcoins-will-there-eventually-be/9962#9962
11. http://digiconomist.net/bitcoin-energy-consumption
12. https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html
13. https://en.wikipedia.org/wiki/MIT_License
14. https://www.youtube.com/watch?v=Rw8W92iIHZ8
15. https://en.wikipedia.org/wiki/Smart_contract
16. https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html
17. https://www.cryptocoinsnews.com/smart-contracts-12-use-cases-for-business-and-beyond/
18. https://en.wikipedia.org/wiki/The_DAO_(organization)
19. https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/
20. https://www.forbes.com/sites/pamelaambler/2017/09/10/how-blockchain-is-fixing-the-diamond-industrys-rampant-ethical-issues/#467fed2625bc
21. http://www.sciencedirect.com/science/article/pii/S0969701200000137
22. http://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/the-construction-productivity-imperative
23. Circular Economy in the built environment, Arup 2016
24. Circular Business Models for the Built Environment Report, Arup BAM 2017
25. https://www.bamb2020.eu
26. https://www.forbes.com/sites/alextapscott/2016/08/08/the-internet-of-things-needs-a-ledger-of-things/#315513f640d1
27. Blockchain Revolution, p.153, Don Tapscott, Alex Tapscott
28. https://github.com/iotaledger/iri/graphs/contributors
29. https://github.com/bitcoin/bitcoin/graphs/contributors
30. https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d
31. http://brooklynmicrogrid.com/
32. http://www.autodesk.com/solutions/bim/overview
33. https://www.thenbs.com/knowledge/bim-levels-explained
34. https://storj.io/faq.html#faq-1-1
35. http://www.pcsg.co.uk/services/information-management-bim-levels-2-3-4/
36. https://www.forbes.com/sites/alextapscott/2016/08/08/the-internet-of-things-needs-a-ledger-of-things/#7b8cbf3a40d1
37. https://lightning.network/lightning-network-paper.pdf
38. https://www.iso.org/committee/6266604.html
39. http://www.craigsewell.co.uk/guide-to-bim-object-data/#cobie
40. https://coincenter.org/entry/what-are-smart-contracts-and-what-can-we-do-with-them
41. http://www.coindesk.com/making-sense-smart-contracts/
42. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings
43. https://www.nspe.org/sites/default/files/resources/pdfs/NSPE-Whitepaper-Blockchain-Technology-2016-final.pdf
44. https://www2.deloitte.com/de/de/pages/strategy/articles/future-of-blockchain.html
45. https://www.moodys.com/research/Moodys-Blockchain-can-bring-benefits-to-the-financial-industry-and--PR_352414
46. http://bitcoinuptime.com/
47. EC Harris, ONS 2014

Authors

Christopher Kinnaird
CAD Technician
Buildings Scotland

Matthias Geipel
Consultant
Advisory Services

Contributors

Cinthia Buchheister
Associate

Daniel Robles
Co-Founder
Integrated Engineering Blockchain Consortium

Fabian Stelzig
Senior Project Manager

Gereon Uerz
Associate
Europe Lead, Foresight

Josef Hargrave
Associate Director
Global Foresight Manager

Katharina Adelt
Industrial Trainee

Dr. Mark Bew MBE
Chairman
Digital Built Britain

Martin Pauli
Senior Architect

Stephanie Schemel
Researcher

Yi-Jin Lee
Associate

Design

Mark Pearsall
Senior Designer
Foresight, Research and Innovation

Isabel Heinemann
Graphic Designer

Copy Editor

Stephen Cousins
Freelance Writer & Journalist

The authors see this report as their small contribution to help inform the industry, educate and ultimately…

Shape a better world.

This report should be considered food for thought.

We would like to thank everyone who supported us during the workshop and writing of the report.

For more information please contact:
blockchain@arup.com

p01	© Ekaterina_belova
p08	© Wavebreak Media, Fotolia
p10	🅭 Rafael Matsunaga, Flickr, CC BY 2.0
p11	🅮 Jason Benjamin, Flickr, Public Domain
p12	🅭 Rick Turoczy, Flickr, CC BY 2.0
p14	© Kuzmick, Fotolio
p20	🅭 Steve Jurvetson, Flickr, CC BY 2.0
p27	🅭 Mike Caldwell, Flickr, CC BY 2.0
p28	🅭 Benedikt S. Vogler
p30	🅭 Noam A.
p31	🅮 Steve Snodgrass
p32	© Brooklyn Microgrid
p33	© alkas.it, Fotolia
p34	© Volkswagen Group
p35	© AndSus, Fotolia
p36	🅭 Christian Lambert, Wikimedia Commons, CC BY 2.0
p38	© Ethan Rohloff
p42	© Arup
p44	© Transport Scotland
p45	© Arup
p50	© Arup
p51	© Arup
p52	© Arup
p54	🅭 Tim Evanson, Flickr, CC BY-SA 2.0
p57	© Homonstock, Fotolia
p58	© Underworld, Fotolia
p59	🅮 Malware, Wikimedia Commons, Public Domain
p60	© Wanchai, Fotolia
p62	© Sergey Yarochkin, Fotolia
p64	© Arup
p66	🅭 Michele M. F, Flickr, CC BY 2.0
p67	🅭 Blogtrepreneur, Flickr CC BY 2.0
p68	🅮 Nasa, Wikimedia Commons, Public Domain
p72	© Ekaterina_belova

ARUP

13 Fitzroy Street
London WIT 4BQ
arup.com
blockchain@arup.com