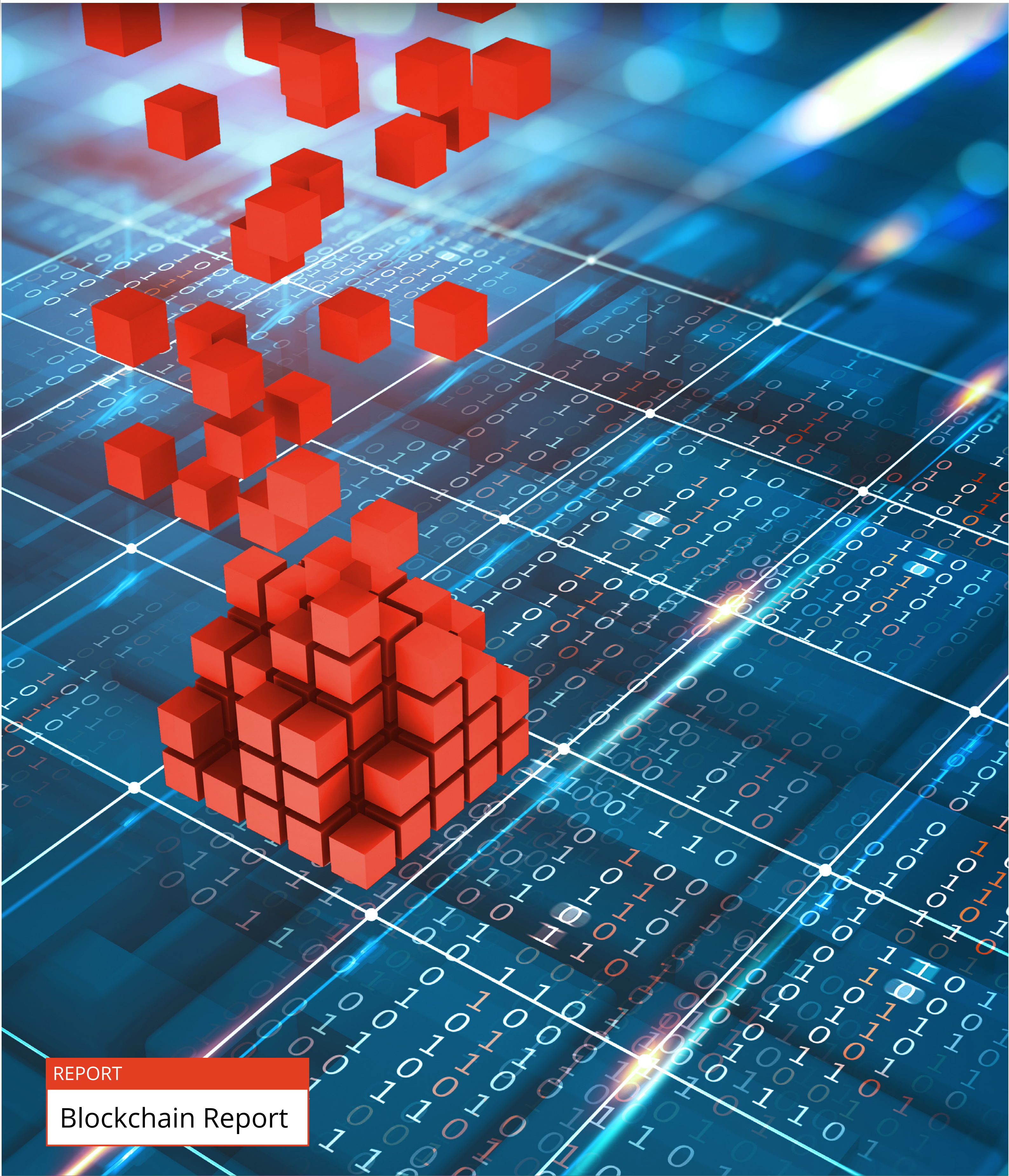
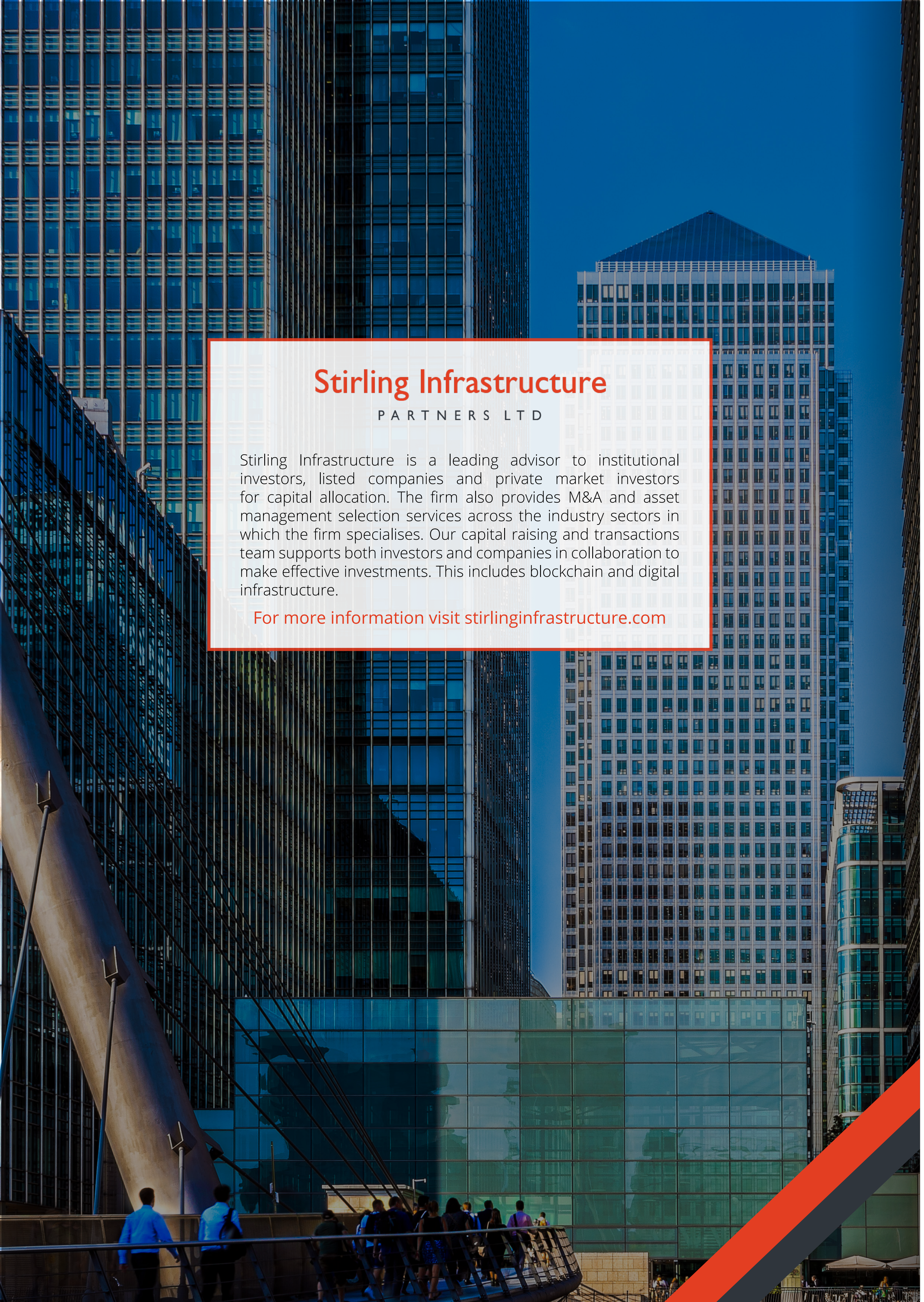
Introduction to Blockchain

Stirling Infrastructure
PARTNERS LTD



REPORT

Blockchain Report



Stirling Infrastructure

PARTNERS LTD

Stirling Infrastructure is a leading advisor to institutional investors, listed companies and private market investors for capital allocation. The firm also provides M&A and asset management selection services across the industry sectors in which the firm specialises. Our capital raising and transactions team supports both investors and companies in collaboration to make effective investments. This includes blockchain and digital infrastructure.

For more information visit stirlinginfrastructure.com

Stirling Infrastructure
PARTNERS LTD

Contents

FOREWORD

This paper is part of a series whose aim is to help investors and our clients understand blockchain technology and evaluate the future of the industry. To achieve these aims, this paper provides overviews, analysis, and insights on various aspects of blockchain including the fundamentals of the technology itself, including its various validation methods, current regulatory landscapes around the world, and its implementation strategies for businesses among many others. The material is split into three sections, and a glossary of key terms (highlighted in **bold**) with their definitions are provided at the end of the paper.

EXECUTIVE SUMMARY

Stirling Infrastructure believes it is essential to achieve ahigh level of technical expertise in blockchain in order to make informed decisions on growth strategies and capital allocation. As a result, this paper sets out an informational guide for understanding blockchain technology and offers various modes of analysis for objectively evaluating its applications.

Blockchain is a decentralised database that stores transactions across a **peer-to-peer network**. This means that any individual on the peer-to-peer network can freely access the database and view all data stored in it. Blockchain does not require a trusted third-party, such as a central server or traditional bank, to store or validate transactions. Instead, transactions can be validated through mechanisms that ensure trust by gathering consensus from the majority of individuals on the network.

Trust, transparency and security are key features of blockchain that make it a technology that adds value over current systems.

The features of a blockchain allows the corresponding database to be transparent and secure, simultaneously increasing trust between users. The emergence of blockchain has heralded the creation of new business models and ecosystems that could transform industries such as finance and healthcare as well as global supply chains. Companies in different industries around the world have signalled significant interest in blockchain and its potential use cases through their increased investment and early implementations of the technology.

Major market players such as JP Morgan, IBM and Microsoft are already implementing blockchain technology.[1]

In this paper, we describe what blockchain is and explain the technology behind it. We also provide an assessment on the blockchain industry today and analyse why leading companies are attracted to it.

1 Biggest enterprise blockchain players, 2020, https://cointelegraph.com/news/12-of-the-biggest-enterprise-blockchain-players-of-2020

AN INTRODUCTION TO BLOCKCHAIN

Blockchain has shown promise as an enabler of the future of the internet. A significant part of this development has come through enabling our ability to exchange value over the internet.[2]

The storage of information has been a pervasive and essential part of human history. Primitive records have been kept by ancient civilisations in a range of unique ways, each iteration slightly more advanced and efficient than the last. The tale of human advancement is on many levels a profound one, and, with blockchain technology, we find ourselves at the forefront once again.[3]

Blockchain offers a new method of storing information in a decentralised way. Proponents argue that blockchain, in combination with other technologies, has the potential to reconfigure business models, societal structures, and economic activity around the world. It is, some claim, poised to become the latest technological revolution.

FUNDAMENTALS OF BLOCKCHAIN

A blockchain is a decentralised **ledger** of all transactions that occur across a **peer-to-peer network**. In simpler terms, it is a database that contains information and does not rely on a trusted third-party such as a central server. Information is broken up into blocks which are then stored in a chronological chain. Blockchains run on a set of **protocols**, or rules, that determine how transactions are validated and trusted by the network.[4]

The premise of how transactions are handled on a blockchain is outlined in Satoshi Nakamoto's Bitcoin white paper.[5] Typically, on a blockchain, when new transactions occur, the information is broadcast to all individuals (often referred to as **nodes**) on the network. **Validators**, or **miners**, validate the transactions using different methods which depend on the blockchain's **consensus mechanism** (see section 2 - *Blockchain as a Technology*). Once the transactions are validated (with proof of work being the most common form of consensus mechanism), they are reviewed by the rest of the nodes on the network. If more than 50% of the network agrees that the transactions are valid, they are grouped into a block and added to the chain. Each block contains a reference to the previous block, which allows the transactions to be stored on the blockchain in chronological order. All nodes on the network can access and view the blockchain and all data stored in it.[6]

Using blockchain technology, participants can validate transactions of any kind, such as those involving money or data, without the need for a trusted third-party such as a traditional bank, a feat which hitherto could not reliably be carried out over the internet. By ensuring trust without a third party, blockchain has shown promise as an enabler of the future of the internet and our ability to exchange value over it.

A BRIEF HISTORY OF BLOCKCHAIN

1991 First description of a cryptographically secured chain of blocks was developed by Stuart Haber and W. Scott Stornetta, who described a system in which timestamps could not be tampered with in their paper titled How to Time-Stamp a Digital Document.[7]

2009 Blockchain 1.0, in the form of Bitcoin, was developed by Satoshi Nakamoto to serve as a public ledger for transactions made using the cryptocurrency. It included improvements from Haber and Stornetta's initial design, such as an increase in the difficulty at which blocks could be added to the blockchain to stabilise the value of the cryptocurrency.[8]

2015 Blockchain 2.0, in the form of Ethereum, was introduced by Vitalik Buterin and Gavin Wood, who envisioned asset management and trust agreements as potential use cases of blockchain. Ethereum paved the way for applications of the technology beyond cryptocurrencies through the introduction of **smart contracts** and the ability to build decentralised apps (**Dapps**).[9]

Several of the world's largest banks including JP Morgan and Goldman Sachs collaborated as part of the R3 Consortium to explore blockchain technology and to develop industry standards for security and regulation compliance in blockchain.[10]

Present Blockchain 3.0 was introduced, with the appearance of more scalable blockchain platforms such as EOS.IO and Cardano to facilitate many transactions per second. Further, private blockchain development increased as companies seek to leverage blockchain technology to make business operations and processes more efficient.[11]

2 Wikipedia, Blockchain, 2021, https://en.wikipedia.org/wiki/Blockchain
3 101 Blockchains, History of Blockchain Timeline, 2020, https://101blockchains.com/history-of-blockchain-timeline/
4 Investopedia, Blockchain Explained, https://www.investopedia.com/terms/b/blockchain.asp
5 Bitcoin cash system, 2008, https://nakamotoinstitute.org/bitcoin/
6 101 Blockchains, History of Blockchain Timeline, 2020, https://101blockchains.com/history-of-blockchain-timeline/
7 How to time-stamp a digital document, 1991, https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.8740
8 Bitcoin cash system, 2008, https://nakamotoinstitute.org/bitcoin/
9 What is Ethereum, 2021, https://ethereum.org/en/what-is-ethereum/
10 R3, 2021, https://www.r3.com/
11 ICAEW, History of blockchain, 2021, https://www.icaew.com/technical/technology/blockchain/blockchain-articles/what-is-blockchain/history

WHAT IS THE PURPOSE AND RELEVANCE OF BLOCKCHAIN?

When Bitcoin, the first **cryptocurrency**, was introduced in the wake of the 2008 Financial Crisis[12] , it provided a payments system that was alternative to the status quo. Individuals were able to use Bitcoin as a currency for transactions that did not require mediation or settlement by the traditional banks, whose reputations were hit as public sentiment against them grew. In other words, Bitcoin effectively decentralised money.[13]

Blockchain is the enabling technology behind Bitcoin, and it serves a much broader purpose: it provides individuals with the ability to exchange value over a network, or the Internet, without a third-party middleman. On a blockchain, individuals can perform activities such as transferring money, monitoring supply chains or company auditing on a peer-to-peer basis, bypassing slow and inefficient intermediaries. As a result, blockchain makes processes more efficient in the technological sense and moves those processes away from centralisation by an authority. In practice, this means blockchain offers industries around the world the following benefits:

Trust

Trust is a fundamental part of any successful relationship, and it gives transacting parties confidence to exchange value. In the absence of a middleman, blockchains use technology and the power of consensus to provide trust. This is significant because it means, for example, that one individual can transfer money to another without the use of a bank or payments company such as PayPal. Blockchain-enabled trust can grow the Internet from a platform for exchanging information to a platform for exchanging value.

Efficiency

Blockchains allow individuals to transmit data in real-time and transact at fast settlement times. Since transactions are peer-to-peer, less time is spent waiting for processes and validation carried out by intermediaries. Also, consortium blockchains allow different stakeholders access to the same information, which is more efficient than reconciling each of their independent databases.

Provenance

Items of value that are exchanged on a blockchain leave audit trails that detail the transaction history of that item. Data, inventory, or money can be traced back to their first instance on the blockchain to verify provenance or investigate manipulation. Blockchain can offer reliable tracking compared to current methods, as it is both real-time and reliable.

Transparency

Participants on a blockchain can view all transactions, creating transparency and thereby optimising business processes and supply chains. Traditionally, all stages of the supply chain – from producers and shippers to distributors and retailers – have centralised databases that are not synchronised, which makes the tampering of data and fraud possible. A blockchain, however, can serve as a transparent, incorruptible, and decentralised database where any stakeholder in a supply chain can log information so that a complete timeline of a product's metadata exists and is viewable by all stakeholders.

12 Trust, Confidence, and the 2008 Global Financial Crisis. https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1539-6924.2009.01230.x
13 Investopedia, Blockchain Explained, 2021, https://www.investopedia.com/terms/b/blockchain.asp

BLOCKCHAIN: BENEFITS AND RISKS

Benefits

Efficiency

As third-party mediation is no longer a requirement; digital transactions can be processed faster with reduced risk of human error. All stakeholders have access to the same database which eliminates the need to reconcile information held by different stakeholders using separate databases.

Decentralisation

As the network is distributed across all nodes on the network, there is no single point of vulnerability, leading to there being reduced reliance on a single entity, as opposed to current, centralised networks, which are thereby more vulnerable to modification and accessibility by involved stakeholders.

Traceability

Different stakeholders have access to the same information so each can trace and monitor transactions to ensure malpractice does not occur.

Security

Resistance to modification significantly reduces risk of fraudulent and unauthorised activity.

Risks and Issues

Security

Blockchains may be susceptible to hackers exploiting vulnerabilities in blockchain code. **51% attacks** can occur when the majority of the network is controlled by malicious or dishonest individuals. Attackers can revise transaction history, prevent the validation of new transactions, or **double spend**.

Sustainability

Some blockchain networks require large amounts of energy to run, which can be of concern if energy is sourced unsustainably. A blockchain's demand for energy depends on the consensus mechanism used (see section 2).

Regulation (Explained further in the section *Blockchain as a Technology*)

Blockchain is a relatively new technology and current regulatory frameworks are pending, inconsistent, underdeveloped, or non-existent. Blockchain networks can be a hotspot for illicit activity, mainly money laundering for drug cartels and the purchase of illegal drugs or weapons.

BLOCKCHAIN AS A TECHNOLOGY

BLOCKCHAIN AS A TECHNOLOGY

PUBLIC AND PRIVATE BLOCKCHAINS

A **public blockchain** is an open blockchain network in which any member of the public can participate while a **private blockchain** is invitation-only. The table below outlines some key similarities and differences between the two.

Public (Permissionless) Blockchain	Private (Permissioned) blockchain
Both function as an append-only ledger where records can be added but cannot be altered or deleted. This means that the ledger is an immutable record and cannot be modified after being created.	
Each node in both a public and private blockchain network has access to the ledger. Both types of blockchain are decentralised and distributed over a peer-to-peer network of nodes.	
Both blockchains have a verification process for any record added, increasing the record's validity until a consensus is reached. More than 50% of the participants must agree that a record is valid for a consensus. The process helps to stop tampering with the records.	
Both networks rely on numerous users to authenticate edits to the distributed ledger, aiding in creating a new master copy that any participant can access at all times.	
Anyone can join the network, read, write, or participate in the blockchain (however, data remains entirely secure as it is not possible to modify or alter data once validated on the blockchain)	Only the people invited can participate in the network.
It is fully decentralised, so no single entity controls the network – hence, more trustworthy	More centralisation than a public blockchain since only a small group of participants control the network – however, still decentralised for those members (only the entities participating in a transaction will have access to the record; others will not see it)
Harder for anyone to attack the system and gain control of the consensus network	People can scale up the blockchain far easier as there are fewer nodes on the network. As a result of fewer nodes, more transactions can process per second
Higher chance of **collisions** since no one knows who each validator is	Consumes less energy than a public blockchain as it requires less electrical power to achieve a network consensus to validate transactions

Depending on the specific needs of individual businesses, one can opt for either of these two types of blockchains– it is difficult to ascertain which type is suitable for the business purely based on the sector in which it is involved. Generally, however, public blockchains tend to be used for B2C relationships, whereas private blockchains tend to be used for B2B relationships.[14]

HOW ARE TRANSACTIONS VALIDATED?

Consensus can be reached through various validation techniques, each of which has its merits and drawbacks

Validation techniques, also known as consensus mechanisms, determine how new blocks are added to the blockchain.

Consensus mechanisms need to ensure that new blocks are valid, also known as timestamping, and achieve consensus, meaning all nodes on the network reach an agreement on the new ledger.

Different consensus mechanisms mainly force a trade-off between the decentralisation of validation and other perks such as scalability. Some advanced methods also include the operations of blockchain alongside validation. Amongst these, the two most common validation techniques used are proof of work and proof of stake, the similarities and differences of which are shown below. However, it is important to acknowledge that there are also many other validation techniques, most of them uniquely developed by a certain company.[15]

14 Public Vs Private Blockchain: Introduction to Two Major Types of Blockchain, https://101blockchains.com/public-vs-private-blockchain/
15 Saini, ConsensusPedia, 2018, https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f

Proof of Work[16]	Used by Bitcoin, Ethereum	Requires nodes to provide evidence that they have expended energy by competing to solve the complex puzzles needed for mining. The process of solving the complex puzzle involves having the miner's computer produce a hash value that matches the blockchain network's current target computation. A correct hash value would have a sufficient number of zeros in the front of the value. For example, the hash of block #660000 of Bitcoin was 00000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6.[17]
Proof of Stake[18]	Used by Peercoin, Ethereum 2.0	Selects participants based on their held stake in the blockchain, i.e., currency in the cryptocurrency pool, to be allowed to validate new blocks.
Other forms similar to Proof of Stake (generally categorised as Proof of Weight) holds other assets as a stake. For example putting reputation at stake in: Proof of capacity, pproof of authority, and proof of importance .		

Differences:

Proof of Work vs Proof of Stake	
Proof of Work	**Proof of Stake**
Very stable method to achieve consensus and validation, while being decentralized with low barriers of entry.	More energy efficient and faster since there's no need for a puzzle to be solved.
Requires increasingly huge large amounts of energy that incentivizes economies of scale, such as having mining setups in China that have low electricity cost, in Siberia where less cooling is needed, or Iranian mosques for free energy.	However, not requiring much energy causes it to have a nothing-at-stake problem where miners are encouraged to mine all fork (when two or more new blocks is are added to the blockchain, usually only the most reputable fork is accepted but it could be exploited to double spend). Mining all forks guarantees rewards for the miner if only one of the forks is accepted later, but ultimately damages the blockchain by not giving the correct fork more reputational validation. → There are precautions to this such as applying sanctions on anyone producing invalid blocks.
Susceptible to tragedy of commons, a future point in time when little or no miners will exist → easier target for a 51% attack.	Less incentive to perform a 51% attack as an attack would then reduce the attacker's stake's worth (in order for one to perform a 51% attack in a proof of stake consensus method (unlike in the proof of work method), they are required to have 51% of the entire "stake", i.e., they need to own 51% of the network. If one does hold 51% of the network, they have less incentive to perform the attack because by doing so, they are reducing the value of the entire blockchain and thereby the value of their own holdings. It's instead in their best interest to maintain a secure network)
Low scalability in numbers of transactions per time duration, as the arbitrarily complex puzzle requires a significant amount of time to be solved.	Delegated proof of stake is even faster than standard proof of stake but becomes more centralized in comparison.
Delayed proof of work is more energy efficient with increased security, but harder to implement and needing multiple blockchains to have similar validation techniques.	

16 Frankenfield, Proof of Work, 2021, https://www.investopedia.com/terms/p/proof-work.asp
17 Blockchain Explorer, Block: 660000, https://www.blockchain.com/btc/block/660000
18 Frankenfield, Proof of Stake, 2021, https://www.investopedia.com/terms/p/proof-stake-pos.asp

Other validation techniques all have their benefits and trade-offs. Some are better designed for a private blockchain such as Proof of Reputation, where validators are chosen based on reputation or authority; or Proof of Elapsed Time, where participants require a single unique identity to be equally likely to be chosen to validate.

WHY ARE SOME BLOCKCHAINS DIFFERENT FROM OTHERS?

The value of a blockchain depends on size of block, consensus mechanism, smart contracts, permissions and multi-layered protocols

Since 2008, blockchain technology has been rapidly evolving. There have been several major advancements in blockchain technology that have helped to solve issues such as blockchain mining's environmental impact and, more recently, scalability. Such improvements have rendered blockchain a more mature technology that has the potential to feasibly provide an alternative to the status quo. As a result of its increased adoption, there are many thousands of different blockchains that have been created, with some of them claiming to provide novel features and capabilities. We explore the properties of a blockchain's architecture that can be changed to allow these blockchains to be different, a vital step when evaluating a blockchain.

Size of block

In a blockchain, transactions are stored in blocks. Each block has a maximum capacity which determines how much data can be stored in it. This capacity is determined by the developer and is built into the blockchain's programming, after which it cannot be altered. Larger block sizes mean each block can store more transactions, which increases the number of transactions that can be processed per second. Similarly, smaller block sizes mean fewer transactions are processed per second.[19]

Bitcoin's block capacity is fixed at 1MB which yields 7 TPS (transactions per second). Bitcoin Cash, a **hard fork** of Bitcoin, increased block sizes to 8 MB and subsequently to 32 MB in 2018. Bitcoin Cash was created primarily to solve Bitcoin's scalability issues.[20]

Ethereum's block capacity varies and is determined, in units of gas, by the miners. Gas measures the amount of computing power required to validate blocks. ETH Gas Station is a website that makes gas transaction prices more transparent.[21]

Consensus Mechanism

Trust allows participants in a blockchain network to transact items of value between one another, and it relies on the honesty of other individuals on the network. In order to ensure this, different blockchains use different consensus mechanisms that are programmed to incentivise honesty and trust, and to disincentivise bad acting. The most commonly used consensus mechanisms are proof-of-work and proof-of-stake, however, there are many other mechanisms that can, and have been, adopted.

There are different advantages and disadvantages that accompany each consensus mechanism such as environmental concerns, increased transaction speeds, and reduced decentralisation. As such, when evaluating the utility of a blockchain, it is important to analyse, on an individual use case basis, the consensus mechanism used.

Smart Contracts

Smart contracts are programmed protocols that are automated to execute different functions or contracts when the conditions for execution are met. At the time of their first implementation in Ethereum's blockchain, smart contracts were an innovation that offered new methods of interacting with blockchain technology and made different blockchain use cases possible. Smart contracts enable the development of decentralised applications, which are claimed to derive their economic value in the greater efficiency, transparency, responsiveness, and elimination of human error that they offer to firms.[22]

Blockchains that are smart-contract-enabled are often classed as Blockchain 2.0. They serve as a more advanced blockchain infrastructure that herald the potential decentralisation of industries and markets globally.[23]

Permissions

Blockchains can be private or public and this has implications on different aspects of the blockchain such as trust, security, and maintenance.

Multi-layered Protocols

Blockchain layers refer to different protocols or technologies that are stacked on top of one another to create a system that is based on a blockchain.

19 Saini, ConsensusPedia, 2018, https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f
20 Bitcoin Cash. https://www.investopedia.com/terms/b/bitcoin-cash.asp
21 ETH Gas Station, 2021, https://ethgasstation.info/
22 Law Commission, Smart Contracts, 2021, https://www.lawcom.gov.uk/project/smart-contracts/
23 Blockchain 2.0, 2016, https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges

- Layer 1: the blockchain itself, the ledger (or database) that records transactions
- Layer 2: different blockchain projects have sought to develop layering technologies that aim to solve issues such as scalability. Layer 2 solutions help scale the blockchain application by redirecting and handling transactions off-chain before sending the net results of these transactions back to Layer 1 where they are validated and recorded. Layer 2 provides an infrastructure that runs adjacent to Layer 1, which consequently becomes less congested and more scalable.

Multi-layered protocols stack different technologies to build a use case that is fundamentally built on a blockchain, but it also benefits from increased scalability and additional features such as a user interface. It is worth noting that not all blockchains are multi-layered.[24]

BLOCKCHAIN IN ECONOMICS AND LAW

Adopting blockchain technology requires legal compliance, the landscape of which currently remains uncertain

Jurisdictional problems

Unlike centralised ledgers where records are maintained in a relatively compact area, nodes of decentralised ledgers can span multiple locations. This raises the question of which jurisdictions' laws and regulations must be complied with by such blockchain networks, and the importance of providing an answer to this is particularly illuminated by the fact that – especially at this early stage of blockchain development – laws are severely inconsistent between different jurisdictions[25 26]

Privacy and data protection

The foundational purpose of blockchain networks is to facilitate peer-to-peer transactions without the need of a central party, and this leads to a situation where in a permissionless public blockchain system, no single party takes responsibility for the availability or security of a blockchain network, and all users of the system may have access to the data recorded on the network. Not only may this present a risk for the privacy of individuals whose identities are recorded on the blockchain, but these attributes can also conflict with the structure of privacy laws currently in place.

- E.g.: European Union's General Data Protection Regulation

The GDPR requires parties to uptake a position of controller (who determines the purposes and means of processing particular personal data) and processor (who are responsible for processing personal data on behalf of a controller, such as an outsourced service provider) because they have distinct duties in a conventional network of records. However, how these positions will be allocated is not so clear in blockchain systems because they are operated by all the users in a peer-to-peer network environment. This undoubtedly has great repercussions for how blockchain networks are regulated under the law and may even prompt the alteration of current legislation.[27]

Smart contracts

The most significant issue with smart contracts is the question of whether smart contracts are as legally binding as conventional contracts in law. Fortunately for the future of blockchain technology, it seems as though multiple jurisdictions are affirming their legal enforceability.

- In the US, all states have defined blockchain, and most have defined smart contracts, expressing an explicit recognition of smart contracts within the law. Further, they have also recognised smart contracts to be at par with traditional contracts. Hence, although the treatment of smart contracts does differ between states, many, such as Arizona, have created legislation to allow enforceable legal agreements to be created via smart contracts.
- In the UK, the regulatory scene of smart contracts has not been so clear, due to the lack of certainty in the area. However, in November 2019, the UK Jurisdiction Taskforce affirmed that the requirements of contract creation in conventional contracts, which are intention to create a legal relationship, valid consideration, and offer/acceptance, can also be satisfied by smart contracts, to conclude that as a result, they will be granted contractual and legal force. Although this has not been tested in English courts yet, this affirmation is likely to have persuasive authority if such a case does arise. Further, the UK Law Commission, which is a governmental body that creates recommendations of legal developments to Parliament, is currently in the process of publishing their recommendations regarding smart contracts, and they are intended to be published later in the year. This will greatly increase certainty in the area.[28]

24 Cryptopedia, Layer-1 and Layer-2 Blockchain Scaling Solutions. https://www.gemini.com/cryptopedia/blockchain-layer-2-network-layer-1-network
25 EU Blockchain Observatory and Forum, Legal and Regulatory Framework of Blockchains and Smart Contracts, https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
26 International Finance Corporation, Blockchain and Associated Legal Issues for Emerging Markets, https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffcd1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf?MOD=AJPERES&CVID=mxocw9F
27 EU Blockchain Observatory and Forum, Legal and Regulatory Framework of Blockchains and Smart Contracts, https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf
28 Law Commission, Smart Contracts, 2021, https://www.lawcom.gov.uk/project/smart-contracts/

BLOCKCHAIN IN INDUSTRY

HOW DO COMPANIES IMPLEMENT BLOCKCHAIN TECHNOLOGIES?

The process of implementing blockchain into a firm runs as a similar timeline to that of most new technologies with a few key differences and steps that are specific to blockchain.

1. Begin with a use case

In identifying a use case, questions such as that regarding the purpose of the blockchain implementation specific to the business, and the targets, aims, and objectives of the implementation should be answered. From this, relevant cases where blockchain could be implemented are selected.

2. Create a **Proof of Concept (POC)**

This requires a more rigid planning phase and requires the identification of the business problem attempting to be solved through blockchain implementation, and the potential benefits garnered by the business in doing so. The steps of creating a proof of concept should be to develop a set of guidelines which explain the extent of the business problem, and then building and testing a small-scale prototype for blockchain, this entails coding and testing.

3. Select the blockchain

This process is specific to individual business needs, and the variety of blockchain platforms must first be evaluated before selecting the correct one.

4. Build and test the blockchain solution

After building the blockchain, it is evaluated based on certain factors such as: does the technology add value, the quality of the technology (or if it offers valuable security benefits), and the vastness of the technology and how compatible it is with other platforms.

5. Select a consensus protocol

Again, this step is specific to individual organisational needs; each of the various consensus mechanisms must be understood and evaluated before choosing the most suitable.

6. Build the **blockchain ecosystem**

It is crucial to outline the terms of engagement and mechanisms of governance, meaning who runs and operates the blockchain itself to ensure it runs smoothly.

During this whole process, the prospect of efficiency gains and the most significant challenges of implementing blockchain, scalability and energy usage should be considered thoroughly.[29]

29 Saini, ConsensusPedia, 2018, https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f

WHICH SECTORS ARE ADOPTING BLOCKCHAIN AND WHY?

Blockchain technology is regarded as the next big thing after the internet, changing how businesses operate in the financial services industry. Blockchain as a form of distributed ledger technology, by leveraging its decentralised properties and being transparent, aims to lower the costs, increase the efficiency of executing transactions, and auditability of operations.

The following will address how blockchain technology has made changes to operations in capital markets, asset management, payments and trade finance.

Capital Markets

Capital markets refer to the places where savings and investments are moved between suppliers of capital and those in need of capital.

Blockchain reduces settlement times for transactions. Transactions can normally take up to days to clear and settle. However, using a cryptocurrency "token" to act as a proxy to the transaction allows for immediate transfer to the beneficiary's wallet, confirming the settlement of the transaction. Through decentralised utilities, it can eliminate the single point of failure. This means that the system is more stable when executing transactions.[30]

Asset Management

Investors are facing demands to improve liability risk management, introduce a more dynamic decision-making structure and overcome the increasingly stringent and ever-changing regulations.

Fund subscriptions and investment lifecycle management has been relying on heavy paper-based processes which involve a lot of intermediaries which are prone to human error, fraud, and data manipulation. Blockchain can digitise security lifecycle in a single platform and retains a single source of truth for activity across the whole platform. This facilitates data accessibility and removes the need for manual reconciliation.

Having a fully digitised asset lifecycle management can improve investor relations, allows for real time capitalisation table (cap-table) management. This results in increases in efficiency and reduces costs. On the other hand, compliance attributes can be programmed to digitised assets to adhere to a specific set of regulations according to different geographic distribution and jurisdictions. This enables transparent reporting to relevant stakeholders which reduces investor and regulatory uncertainty and helps promote approval and adoption.[31]

Payments

Global payments and remittances are executed by a handful number of intermediaries that charge service fees and transactions can take up to 7 days to reach the other account. Blockchain can streamline payment and remittance processes, reduce costs and enables faster settlement times. Blockchain technology can provide real-time gross settlement between central banks, commercial banks and independent banks. This can provide rapid and secure domestic or cross border payments. Digitised **KYC** and **AML** data and transaction history can also reduce the risks of fraud and enable real time authentication.[32]

Supply Chains:

Blockchain also currently plays a vital role in improving the transparency of organisations' supply chains, and in the future will likely help protect against problems such as fraud and counterfeiting of goods. Organisations can digitize physical assets and create a decentralised immutable record of all transactions, making it possible to track assets from production to delivery or use by end user. The following will assess 3 main areas of both current and potential future benefit of blockchain usage in supply chains.

Protection from counterfeiting:

Current systems of protection against counterfeiting are reliant on centralized authorities or intermediaries; this creates the potential for dishonest nodes in the supply chain to undermine the authenticity of records. Blockchain however, provides an identifying element at every step within a supply chain, which is done in real time. This makes it possible to see mistakes as and when they happen, and to adjust as necessary.

30 Cryptocurrency Token, 2021, https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/
31 Digital Asset Lifecycle, 2019, https://www.cleanpix.com/blog/2019/08/22/digital-asset-lifecycle/
32 Blockchain use cases for banks, 2019, https://www.finextra.com/blogposting/17857/blockchain-use-cases-for-banks-in-2020

This technology, however, is still in its infancy, with most products still at the explanatory/sense making phase. The issue at hand is that these products still require independent verifiers, increasing transparency is a benefit, but not a full solution. Firms such as EZ Lab Wine have pioneered blockchain technology to track wine and prove its authenticity, but the system is not fool proof, and still requires trust throughout the supply chain.[33]

Transparency:

The key benefit of blockchain lies in transparency; with increased transparency due to a single central ledger, firms can improve the speed, connectivity and accuracy of records. As information and inventory flows are codified and recorded in the blockchain ledger, supply-chain managers gain complete visibility into the transactional history between retailers and suppliers. This also eliminates many blind spots that exist in traditional record keeping and provides a level of visibility that improves coordination between parties.

Back-and-forth communications are reduced, because there's a single source of truth that each party can refer to. Instead of calling a distributor to see whether a shipment is on its way, the ledger provides dynamic access to that information. Applications of this are very far reaching, from improving sustainability and accountability of corporations, to improving the audit process of firms. Through tracking data and materials on the blockchain as they move through your supply chain, you can be certain of exactly how they are manufactured from start to finish.

For organisations aiming to display social responsibility, this is an essential tool to promoting such features to the public. With a decentralised ledger of transactions, it is possible to track every asset from production to delivery and use by the end-user. This provides extreme visibility of the supply chain network while delivering greater product history and transparency. In terms of visibility, blockchain offers more for both businesses and consumers regarding the products they encounter. This is the key benefit for supply chains and will have far reaching implications, particularly for global retailers with many parties involved in the supply chain.

Walmart's implementation of the blockchain into the supply chain with the help of IBM demonstrates the benefits of transparency. To meet sustainability aims and reassure consumers, Walmart implemented blockchain systems which allowed both consumers and managers to track and understand where shipments had come from. After implementing this and building the ecosystem with members of the supply chain, Walmart were not only better able to prove sustainability of produce, but also track potential contaminated shipments far better.[34]

Fraudulent transaction prevention:

Finally, a likely future benefit of blockchain implementation within the supply chain is the prevention of fraudulent transactions. Blockchain acts like an escrow account since it requires all parties must confirm transactions. It protects buyers and sellers by holding funds until all parties can verify which can be executed via smart contracts. With the use of smart contracts, such as those developed by Ethereum both buyer and seller can create "if / then" contracts in which one step of the process won't be fulfilled until the one before it has been verified complete.[35]

Blockchain can serve as an objective, trustworthy, third-party mediator in pretty much any interaction, deal, or partnership you can imagine. It helps ensure trust and transparency, even amongst those who don't trust each other. Currently this technology is in its infancy, and its only widespread use is for escrow accounts for large cryptocurrency transactions. However, there is some development in the real estate sector, with more pioneering firms looking to use blockchain to lower the cost of transactions between firms.

33 EzLab blockchain, https://www.econotimes.com/EY-EzLab-create-blockchain-platform-to-trace-and-certify-Italian-wines-646432
34 Walmart blockchain, 2020, https://theleadershipnetwork.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency
35 Blockchain fraud prevention cases, 2017, https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/

JD.COM – A BLOCKCHAIN CASE STUDY[36]

As China's largest online retailer and its biggest overall retailer, JD claims the smart business upgrade of enterprises will inevitably go through three progressive stages of 'digitalization, networking, and intelligence'. Since first mentioning in the 2019 JD Global Technology Explorers Conference their desire to 'through Internet software and hardware, network communication, Internet of Things, AI, blockchain and other technical applications, digitize the multi-dimensional information and industrial knowledge of the physical world, and digitally connect online and offline information,' JD has independently developed a prototype system of 'Federal Learning + Blockchain' integration, and achieved multi-party cooperation through technical consensus on encrypted and trusted networks.

This was then utilised in June 2020, when JD and second-hand trading platform Paipai launched China's first blockchain traceability system for second-hand goods. This was in recognition of the fact that achieving the full potential of China's second-hand market (which has reached a trillion Chinese Yuan, i.e., 155 billion USD) was hindered by lack of quality information. The implementation of a blockchain traceability platform, therefore, meant there was greater second-hand goods quality supervision.

- As of July 2020, JD Retail has nearly 20,000 traceable foods on sale, and JD International has achieved cross-border traceability across the entire blockchain process with more than 10,000 commodities. Consumers can scan the source code or view the quality traceability information of the product to make their purchase more assured.
- As of Q3 2020, as the world's leading application of supply chain traceability, JD's Zhizhen Chain anti-counterfeiting traceability platform has cooperated with more than 1,000 brands, with over 1 billion data on the chain, and more than 7.5 million consumers 'quality traceability' queries.
- JD Zhizhen Chain and China Europe-ProLogis Supply Chain and Service Innovation Center cooperated in 2020. Through a comparative study of 438 traceable product samples of different categories, it is concluded that the use of the Zhizhen Chain anti-counterfeiting traceability platform has brought about an overall increase in sales of 9.97%. Among them, the additional purchases of maternal and infant products increased by 23.4%, the repurchase rate of nutrition and health products increased by 44.6%, and the return rate of infant milk powder decreased by 31.7%.

In summary, JD's integration of blockchain in its retail business has resulted in greater trust by its customers, owing to the conveyance of information regarding the provenance of its items. This has had the overall effect of increasing sales for the business and illustrates a positive use case of the technology.

36 JD.com, JD Digits Blockchain, 2020, https://blockchain.jd.com/en/

GLOSSARY

51% attack: a malicious attack on a blockchain network that occurs when an individual, or group of individuals, control the majority of the network's processing power. This enables the attacker(s) to revise transaction history, prevent the validation of new transactions, and double spend.

AML: stands for "Anti-money laundering"

Blockchain ecosystem: the smaller community inside the wider blockchain environment, for example members of a supply chain.

Collisions: where two miners randomly generate the same hash value.

Consensus mechanism: the process by which individuals establish agreement to validate blocks. Proof-of-work and proof-of-stake are examples of consensus mechanisms.

Cryptocurrency: a virtual currency where transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralized authority.

Dapps: Decentralised Application – an open-source software application that runs on a peer-to-peer network.

Double spending: a problem in digital currencies in which the same digital coin, or token, is spent more than once.

Hard fork: a change to a network's validation protocol that makes the previously valid blocks on the blockchain invalid.

Hash: a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length, a process that allows blockchains to achieve security.

KYC: stands for "Know Your Customer" and it is the process of verifying the identity of customers to increase the chances of successful business.

Ledger: database synchronised across multiple sites, institutions, or geographies, shared, and made accessible by multiple stakeholders upon consensus.

Metadata: a set of data that describes and gives information about other data.

Miner: a person that records every transaction on a blockchain.

Node: a point on a network where data can be created, transmitted, or received. On a blockchain network, nodes are usually a physical device such as a computer.

Peer-to-peer network: a network where equally privileged individuals (nodes) interact without a central authority such as a server.

Proof of concept: a strategic procedure that is used to evaluate how realisable the blockchain implementation would be for appropriate businesses.

Protocol: a set of rules for how data is transmitted in a network. These rules determine different features of a blockchain such as its consensus mechanism or smart contract compatibility.

Scalability: the ability of a blockchain network to support many transactions per second.

Smart contract: computerised transaction protocols that execute terms of a contract

Validator: someone who is responsible for verifying transactions on a blockchain

FOR FURTHER INFORMATION

This paper provides insights into trend data with analysis for institutional investors to make an informed investment decision into blockchain technologies.

The firm provides a comprehensive range of services which includes M&A transaction services and raising both debt and equity to finance blockchain technologies globally.

For further information please contact:

Stirling Infrastructure Partners Limited
84 Brook Street
London
W1K 5EH
Tel: +44 (0)20 7629 3030

contact@stirlinginfrastructure.com
www.stirlinginfrastructure.com

DISCLAIMER

This document has been developed by our analysts and does not constitute investment advice. It is prepared for information purposes only and does not constitute an investment recommendation.

Stirling Infrastructure Partners Limited
84 Brook Street
London
W1K 5EH

For further information please contact:

Tel: +44 (0)20 7629 3030
contact@stirlinginfrastructure.com
www.stirlinginfrastructure.com

Stirling Infrastructure
PARTNERS LTD