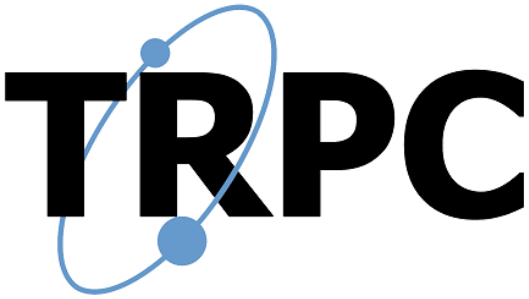


Briefing Paper

Blockchain and its Applications

March 2017

Future of Blockchain Overview

Blockchain's rise to prominence started with the invention of Bitcoin by Satoshi Nakamoto in 2008 as a decentralised, peer-to-peer, digital payments mechanism with a distributed ledger across a global network.[1] Because of the rise to prominence through this digital currency, blockchain is sometimes – and wrongfully – only assumed to deal with financial transactions. The transformative nature of blockchain technology and a distributed ledger system has the ability to touch many more aspects of the economy besides purely financial, from supply chain management to smart contracts to national identifies and passports. Anything that has a transaction or an event to be recorded can take advantage of this technology.

Blockchain is a technology that is a decentralised, *immutable* ledger of ordered transactions that is distributed across many computers and servers for a collective verification of transactions. A transaction can be of monetary value, such as an exchange of currency, or purely logging events, such as movement of goods around a warehouse. The advantage of the immutable ledger is that no one can alter a past transaction or event, they can only amend or reverse in the present to create corrections. The ledger itself can also be used to create automatic transactions when triggered, such as in a smart contract that automatically settles contract commitments if an event occurs. An example of this would be an invoice that is automatically sent and paid when a package is delivered to someone's house.

Two of the best known uses of blockchain are in the cryptocurrencies Ethereum and Bitcoin. Ethereum has the added feature of implementing smart contracts, which automatically conduct the agreed upon contract without human intervention. Despite some security flaws in several of the crypto-currency exchanges, the blockchain technology itself has proved successful. However, central monetary authorities who are concerned both about security and about control of the national currency, when contemplating the use of blockchains and the issuing of their own digital currencies, require a central authority to manage the system of accounts and transactions. A central authority does not undermine the advantages that a distributed database has in terms of transparency and identification of fraud or of money laundering – the blockchain is a digital audit trail – but it does lose some of the advantages of cost efficiency. Final authorization by a central authority may also slow up the completion of the transactions process, but other aspects, such as the clearing process, will still benefit. Currently, NASDAQ is using a blockchain company to manage its NASDAQ Private Market Platform for its equity management functionality.[2]

Characteristics of Blockchains

By definition, the technology is: transactional, distributed, immutable, created by consensus, virtual, and encrypted.[3]

Transactional: Each transaction is recorded into the ledger that is distributed across the network of users and verifiers. This is the main basis for creating a blockchain, to create records of events or transactions.

[1] J. Brito (2013), 'Bitcoin: A Primer for Policymakers', https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf
[2] Finextra, (2016) 'Nasdaq sees in the New Year with first blockchain transaction', https://www.finextra.com/news/fullstory.aspx?newsitemid=28285
[3] Kumar Ujjwall (2016), 'Blockchain as a Service', Microsoft

Distributed: The ledger is sent to the network of participants, which allows for the transactional history to remain secure from a single breach of data storage or an outage at a cloud service provider. The distributed nature of the blockchain ledger allows for the mitigation of fraud – due to the increased transparency – and removes the need for centralised verification or oversight. Any attempted illegitimate change to the system will be immediately noticed by the rest of the participants and deemed invalid.

Immutable: Due to the time-stamped and ever-linked blocks in the chain, tampering with a sequence of past events in the chain is denied. A brute-force hack might conceivably break the chain, but it would be an extremely difficult task to succeed.

Created by consensus: Each transaction that is added to the block is verified by the network. This allows for the consensus or majority of the users of the chain ensuring that if one node of the system was acting maliciously or failed, the integrity of the entire blockchain would not be disturbed.

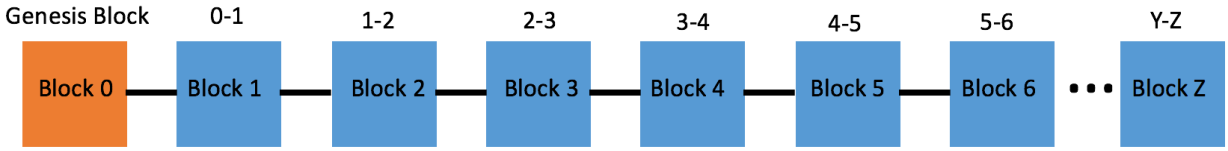
Virtual: The blockchain is held virtually on a distributed network of computers that allows for quick and efficient verification of transactions. Since almost any transaction can be expressed as a digital entry, the technology of blockchain has wide application.

Encrypted: Due to the need to trust each transaction that is created by the consensus verification system, the data is encrypted. Once a block is placed into the chain, it becomes immutable. The data cannot be deleted and the continuity of the chain is assured.

Creation of the Ledger

The chain, or ledger, is created by forming linked blocks that are tied to each other by the information in the proceeding block. Each block is made up of one or more ordered transaction until the block has reached a pre-set data size. After this block is formed it is placed into the chain with a tie to the proceeding block and distributed to all holders of the decentralised ledger.

Figure 1: Basic Structure of Blockchain



Source: TRPC

In order to add a new block to the chain, the transactions are sent to every computer within the ecosystem to validate the answer. Currently, the most commonly used technique for cryptocurrencies is to 'mine' the answer, that is, to create new units of the currency. Mining consists of trying to organise and validate each transaction, primarily through trying to solve a mathematical problem or random number generated to put the events in the correct order, sometimes equated to prime factorisation of large number. The miner that solves the block will then receive a reward, sometimes in the form of the cryptocurrency they are mining or another form of incentive. The

combination is difficult to solve, but rather simple to validate once the answer is known, which allows other computers in the system to quickly validate it is correct and add the new block to the end of the chain. When the block is attached to the end of the chain, miners will start mining the next block and the process of decentralised validation continues as more transactions occur to form the next block. A warning however: malware can take advantage of cryptocurrency mining software installed on a computer, and 'mine' for its own benefit.[4]

When the validation of transactions is within a trusted, or private, blockchain, the validation technique requires much less work as the trusted computers will be the only ones that can send transactions to the chain – such as in an inventory management system. This is what is known in the telecoms world as a closed-user group or CUG.

Validation Techniques – Proof-of-Work vs. Proof-of-Stake

The concept of mining invokes the 'proof-of-work' validation technique that bitcoin and some other cryptocurrencies use. The proof-of-work validation uses the collective computing power of the network to solve the mathematical equation previously mentioned. This is to prevent malicious miners from amending or putting fraudulent transactions into the block. It can take up to 10 minutes to solve the problem, as with Bitcoin, and uses a tremendous amount of the world's computing power.[5] In the first 5 years of existence Bitcoin, mining has used enough electricity to power the Eiffel Tower for 260 years.[6]

The intensive computing power needed by the collective blockchain community is causing other blockchain implementations to think about using alternative techniques. This is also to deal with the '51% problem' of proof-of-work, where if a single entity were to garner over 51% of the computing power of the collective, they could overpower the system, possibly override old blocks or enter incorrect new blocks into the chain, thus rendering thousands of transactions null and void and creating a lack of trust in the system-as-a-whole.

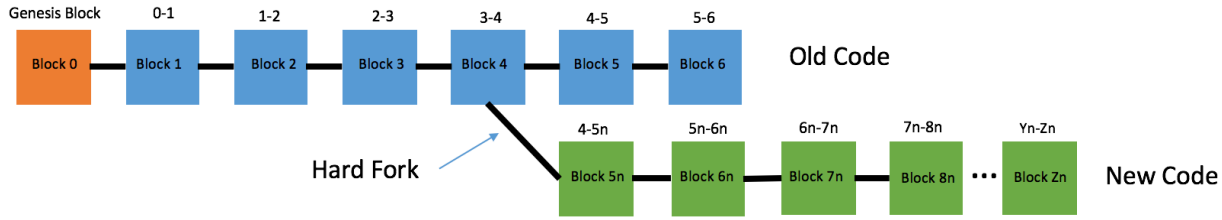
To move away from the 51% problem, Ethereum and some others are moving toward a proof-of-stake model. Proof-of-stake either randomises the person's ledger as the valid one or is built on a pre-programmed model that allows for a single computer to be the builder of the next block based on a variety of factors, but never more than once in a given period, such as once a month.[7]

Ethereum will have to preform what is known as a 'hard fork' (see Figure 2) in order to change their system from proof-of-work to proof-of-stake. As the technology of blockchain develops over time and companies continue to build out the functionality of their systems, there will naturally be needs for upgrades to the code. These can be preformed quickly and with relative ease, as programmers can send upgrades to each of the nodes, or stakeholders, directly via their interconnected networks. A system that fails to upgrade will no longer be able to validate the latest blocks in the chain, but the

[4] How to Geek, 'Cryptocurrency Miners Explained: Why You Really Don't Want This Junk on Your PC', accessed 6 March 2017 https://www.howtogeek.com/211694/cryptocurrency-miners-explained-why-you-dont-want-this-junk-on-your-pc/
[5] Capgemini (2016), 'Introduction to Proof of Work or Stake in the Blockchain', https://www.capgemini.com/blog/capping-it-off/2016/04/introduction-to-proof-of-work-or-stake-in-the-blockchain
[6] Bloomberg Technology (2014), 'Bitcoin Miner Taps Dad's Power Plant in Virtual Money Hunt: Tech' https://www.bloomberg.com/news/articles/2014-04-16/bitcoin-miner-taps-dad-s-power-plant-in-virtual-money-hunt-tech
[7] Bitcoinmining.com (2016) 'Ethereum's Gold Rush is Drawing Bitcoin Miners to Ethereum' https://www.bitcoinmining.com/ethereum-miner-gold-rush/

older blocks will remain readable for the upgraded nodes. Because of the peer-to-peer nature of the upgrades it is impossible to foresee all the changes that will be widely adopted in what remains a nascent technology. The technology needs scale before standardisation can be fully achieved, yet without commonly accepted standards achieving scale may be a challenge. This is where Blockchain-as-a-Service offered by cloud computing service providers may have an advantage.

Figure 2 - Hard Fork



Source: TRPC

Types of Blockchains

There are three main types of blockchains: public, consortium, and private.[8]

Public: Public blockchains, such as Bitcoin or Ethereum allow for anyone to read the chain, write to the chain, and participate in the consensus building. These are the most publicly known and most publicised. The information is open source and publically available.

Consortium: Consortium blockchains, such as R3 – a blockchain consortium of 70 of the worlds largest financial institutions[9] – are closed user groups, and only members may write or help validate the transactions of a chain. This is appropriate for use by banks that regularly transact with one another. In the case of R3, it takes a two thirds majority of them to verify the next block each time, though other agreements can be made internally in the bylaws of a newly created blockchain consortium. This allows for groups of continually transacting entities to create an immutable distributed ledger, irrespective of whether they are competitors or not. The information stored on the ledger can be either confined to the closed user group or shared with the public.

Private: Private blockchains are principally used internally by companies where the information held is considered confidential, and, for example, used for record keeping. An example would be warehouse management, where each piece in the warehouse has a radio-frequency identification (RFID) tag and goes through scanners as movement around the warehouse occurs. This would keep a record of where each piece was located, and how many they had in stock. With smart contracts, they could also re-order when a given threshold was reached. Writing to these blockchains would be permissioned –based and entail only known entities having the ability to provide validation. Besides security, this also reduces latency in validation in contrast to public ledgers where the need for anonymity and of proof-of-work or proof-of-stake are required. (See above for Proof-of-Work and

[8] BlockchainHub (2017), 'Types of Blockchains' https://blockchainhub.net/blockchains-in-general/
[9] R3 Worldwide, 'Who Is R3', http://www.rthree.com/en/?gclid=COvflfijwdICFdOGaAodWV0MPw

Proof-of-Stake)

Figure 3 - Differences Between Public and Private

	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-Stake	Pre-approved participants
Identity	Anonymous/ pseudonymous	Known identities
Asset	Native assets	Any asset

Source: https://blockchainhub.net/blockchains-in-general/

Advantages of Blockchains

The advantages of increased transparency and efficiency that come from using a distributed authenticated ledger will be multiplied when blockchains are enabled to transact with one another across economic sectors.

Lower Transaction Costs and Higher Efficiency: Without the need for independent oversight or clearinghouses, companies can conduct business with reduced transaction costs. Capgemini Consulting estimates that banking and insurance companies will save up to USD16 billion in fees alone by implementing blockchain.[10] The reduction of friction allowed by automatic settlements will enable payments such as bank transfers to cross borders in seconds or minutes rather than days.

Transparency and Trust: As a public ledger system evolves everyone concerned can see the transactions taking place. Any two parties can ensure their transaction is valid, given that the system can independently verify the digital identification of the user. Higher transparency in the supply chain will cut down on the need for intermediation between humans and shipments. Digital identification from each transaction or user associated with an account can also help reduce the Know Your Customer and Anti Money Laundering requirements that banks have to comply with because the sender and receiver of money will already be known and authenticated across the system. Traceability between transactions will be increased and digital audits will become easier. A company named Tieron has created a system where the blockchain is used to create verifiable records for two parties to ensure they are exchanging goods they actually own - from insurance records to health records.[11] And Onename has created a digital ID that allows creates a digital

[10] Capgemini (2016), 'Consumers set to save up to sixteen billion dollars on banking and insurance fees thanks to blockchain-based smart contracts says Capgemini report', https://www.capgemini.com/news/consumers-set-to-save-up-to-sixteen-billion-dollars-on-banking-and-insurance-fees-thanks-to

[11] Tierion (2015), 'Your Bridge to The Blockchain', https://tierion.com/

version of the user and allows entrance into websites more securely than passwords.[12] Blockchains for passports is a possibility for the future, and if international cooperation allows, this could become a global event.

Data reliability and User Oversight: The decentralised storage of the ledger allows for the data across the system to be more reliable and less likely to be manipulated. The complete ledger - of a public blockchain - is accurate, widely available and does not have a single point of failure. Business Continuity Plans can be upgraded to include blockchain technology, using a public or a private blockchain. This will allow for companies to maintain data integrity even should a natural disaster occur or there be a system-wide outage in their cloud computing software.

Select Applications

Finance: The first scaled use of blockchain began with cryptocurrencies, but financial institutions are some of the biggest investors in blockchain technology, not only for cryptocurrencies, but other financial vehicles, such as trade financing or overnight paper. The increased efficiency of transaction between accounts, digital auditing systems and asset management are other major areas of interest. There are, for example, significant slowdowns in the system when the common Over-the-Counter (OTC) trades settle on T+3, or three days after the trade, as opposed to T0, on the day they occur. With the increased speed and transparency from ownership visibility across the blockchain, financial institutions can trade bonds at a much faster rate. The reduction of need for the clearinghouses also allows for these to settle on a T0 or T+1 basis.

Financial payments across borders and remittances are another driver of investment by finance companies in blockchain. Bank-to-bank transfers can currently take multiple days and currency fluctuations cause large financial institutions to hedge their currency positions on a daily basis. Increasing the speed and ease of transfer can save the industry time and money. Currently, remittance companies are taking advantage of cryptocurrencies to disrupt the high fees imposed by the traditional players, such as Western Union.[13] This is because the transaction costs associated with using a cryptocurrency are far lower than traditional SWIFT payments, and these remittance companies have far fewer costs than Western Union due a leaner, less 'on the ground' presence needed.

Smart Contracts: A smart contract is a contract that automatically settles when an event occurs, such as a futures contract closing after a price point is reached or an automatic loan disbursement when short term cash is needed by a company. The code automatically enforces and verifies the contract without the need for human intervention. By turning these legal obligations into automated processes, the smart contracts can guarantee the contract will be fulfilled, reduce the reliance on human-human trust, reduce fraud, provide greater security and lower transaction costs between the two parties obligations. At this stage in the development of smart contracts, they are being used where the contracts themselves are standard, frequent and require very little due diligence or more complex legal advice. They have yet to be fully tested in courts of law, although the keeping of legal records, and, for example, the records of prison terms and convictions, also lend themselves to

[12] Onename (2015), 'Introducing Blockchain ID, Your Digital Identity', http://blog.onename.com/blockchain-id/
[13] Chris Skinner's Blog (2017), 'The five major use cases for financial blockchains', http://thefinanser.com/2016/03/the-five-major-use-cases-for-financial-blockchains.html/

blockchain database technology.

Smart contracts can also be created with relative ease, thus making smaller transactions that would never have contracts built into them possible to be automated. A system in which a smart contract automatically settles when a loan repayment is due provides a basis of trust even when the lending has no personal knowledge of the borrower. This could include quite small and remote payments, such as a USD10 payment over the Internet or an agreement to give a microloan to a vendor in a developing country.[14] Ethereum is the best-known use case of smart contracts where thousands of users a day are using the Ethereum Virtual Machine to handle the settlements.[15]

Land registry: Reducing the transaction time between the sale and change in ownership of land can reduce a friction point on what is often the largest purchase of an individual's lifetime or a large investment for a company. By assigning a unique identifier to each title, and including the transfer history in the identifier, the reduction of fraud is yet again a major benefit, as well as reducing the need for intermediaries. The entire transaction record will be visible through the blockchain and dispute resolution between property owners could be solved quickly and easily.[16] Sweden is already testing the use of blockchain for land registry, and the implementation may go live later in 2017.[17] With the ingress of smart contracts into the transaction, a monetary exchange for the property could be executed with little or no transaction costs. Loans could be pre-approved to be settled in real-time and ownership transferred the same day.

Supply chain: Availability of information and track-ability of each individual inventory stock allows immediate visibility for both supplier and purchaser. This facilitates just-in-time manufacturing as supply availability and demand can be easily matched. Using a smart contract eases the transaction, and does away with paper work and the need for manual accounting. Walmart is running a pilot program during the first four months of 2017 to attempt to streamline and increase efficiency, all while reducing errors.[18] There can also be higher visibility in the tracking of shipments, both across borders and between warehouses. As each good can have its own unique identification number, customs clearance can be both quicker and more accurate as each item in the shipment is on the ledger.

Concerns

Disintermediation: Disintermediation is already a common feature of the growing use of the Internet in commercial transactions. For example, airline tickets are just as frequently booked online as booked through a travel agent. In that sense these technologies can be regarded as disruptive insofar as they change the allocation of resources and shift jobs. However, just as the more complicated travel arrangements still benefit from the expertise of travel agents, so the more

[14] BlockchainHub (2017), 'Smart Contracts', https://blockchainhub.net/smart-contracts/
[15] Blockgeeks (2017), 'What is Ethereum? A Step-by-Step Beginners Guide', http://blockgeeks.com/guides/what-is-ethereum/
[16] Deloitte (2016), 'Blockchain applications in the public sector', https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-public-sector.pdf
[17] Reuters (2016), 'Sweden tests blockchain technology for land registry', http://uk.reuters.com/article/us-sweden-blockchain-idUKKCN0Z22KV
[18] Bitcoin Magazine (2016), 'Walmart Testing Blockchain Technology for Supply Chain Management', https://bitcoinmagazine.com/articles/walmart-testing-blockchain-technology-for-supply-chain-management-1482354996/

complex transactions using blockchains will benefit from the expertise of lawyers, freight forwarders and so on. Furthermore, although each member of the public can check the ledger to confirm their transactions, in many cases they may not feel able to do so because of time restrictions or lack of knowledge on their part. In these cases, there will always be a role for trusted third parties to provide support services, in exactly the same way, for example, that a private citizen renting out a property may rely upon a property management company or agency to supervise and monitor the tenancy on their behalf. In these cases, the blockchain can be managed by a trusted third party.

Scalability: Transactions can occur at a rate of many thousands per second. Currently, Bitcoin can only handle a maximum of seven per second due to the size limitation for each block of 1Mbit, while Visa can handle up to 56,000 transactions per second and averages around 2000 per second.[19] Increasing the ability to handle transactions at high volume will be key not only for currency exchange but the remaining applications of blockchain as well.

Imagine the supply chain management or goods tracking of Walmart if they were to track all of their goods on a second by second basis via blockchain, which is in theory possible. They average 100,000,000 customers a day and almost USD35,000 worth of transactions every second.[20] The blockchain needed to handle the amount of these movements needs to be able to settle, in chronological order, each transaction or movement in an efficient way. Technological advancement will need to occur in order to scale to the point where speedy and accurate implementation of blockchain can occur in all applications. If blockchain is meant to be used at scale, the validation techniques and speed of translation need improvement.

Cybersecurity and Fraud: During 2016, two major cryptocurrencies saw their systems penetrated. DAO, a crowdfunded venture capital fund that allows investments using Ether – the nomenclature for Ethereum's cryptocurrency – was hacked and lost one-third of its value. And Bitfinex, a digital currency exchange, was similarly hacked for USD65 billion in 2016. The cybercrime was committed not along the blockchain, but at the entry and exit points where fiat currency was exchanged for digital currency.[21] The entry and exit nodes of the blockchain faces the same security risks that other databases face, the human element.

The long told fables of the easiest way to hack the CIA is to drop a thumb drive in the lobby and wait for someone to stick it into their work computer still applies to the blockchain. In reality, an easier way is to sending phishing emails, especially targeted spear phishing emails, the hack-of-choice apparently of the Russia's shadowy APT 28.[22] As and when the use of blockchain spreads to strategically important areas of the economy and society, so will cyber-risks to the systems – not to the technology *per se* – that use them. However, the innovation in cybersecurity will benefit from the fact that a community of users are involved with an incentive to ensure the trust of the network is maintained. Part of the value of the distributed ledger system is that cyber-attacks should become more apparent to more users in a shorter timeframe than with other systems.

---

[19] International Business Times (2016), 'Bitcoin's Big Problem: Transaction Delays Renew Blockchain Debate', http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renew-blockchain-debate-2330143

[20] Statistic Brain (2016), 'Walmart Company Statistics', http://www.statisticbrain.com/wal-mart-company-statistics/

[21] Financial Times (2016), 'Cyber attacks raise questions about blockchain security', https://www.ft.com/content/05b5efa4-7382-11e6-bf48-b372cdb1043a

[22] Financial Times (2017), 'Russia mobilises an elite band of cyber warriors', https://www.ft.com/content/f41e1dc4-ef83-11e6-ba01-119a44939bb6

A blockchain company's inevitable bankruptcy: Questions of loss of continuity of data or loss of storage continue to be a concern, just as today, for example, it would be difficult to find an 8-track magnetic tape music player or a laser-disk reader. In order to ensure continuity across the blockchain, there must be a way to ensure that the technology is backwards readable. What happens *when* a blockchain company goes out of business? Where is the chain stored? Can transactions be validated? The decentralised nature of the chain would suggest that it would continue to be stored on individual's computers and/or servers, but in a world where users change computers once every 2-3 years this decentralised digital ledger *could* be lost. This raises concern for long life transactions, such as land registry, that could have zero transactions related to a piece of land for many decades.

Does this mean there needs to be a centralised authority, such as a government regulator, where there is a repository of blockchains? Or is a repository something that the market could provide? In bankruptcy proceedings, should it become an obligation to create a repository or to provide for safe storage of a 'master' blockchain database?

Future of Blockchain

The increased trust and transparency of the blockchain technology reaches far beyond the current use cases. Between the inception of blockchain in 2008 and 2016, there has been over USD1 billion of venture capital funding into new companies trying to revolutionise the way information is managed.[23] Digital Currency Executive estimates that the value of cryptocurrency will be almost USD8 billion by 2024, up from USD509 million in 2016.[24]

The International Data Corporation (IDC) reports that there are three main areas which make blockchain technology and improvement to the current way that information is recorded, specifically for government use:[25]

- Data authority – the record keeping of transactions can be improved due to the transparency of when, who and where the transaction occurred. It also manages who can and cannot read or write the information, creating more secure data storage.
- Data accuracy – with the immutability of blockchain, the data being stored can be verified to be more secure than traditional ledgers.
- Access control – blockchain has the ability to keep the recording of a transaction and can be coded to be a public or private ledger. This allows the governments the same ability to keep the same confidential information, confidential, but creates a more transparent system for non-secret information, such as purchases or laws.

Trusted transactional information enables the reduction of verification and validation friction and can help automate the way the leading enterprises conduct business. PwC estimates that with the use of blockchain, by 2020 many areas of identity and transactions validation and verification will no

[23] Weusecoins (2016), 'Venture Capital Investments in Bitcoin and Blockchain Companies', https://www.weusecoins.com/en/venture-capital-investments-in-bitcoin-and-blockchain-companies/
[24] DCE Brief (2017), 'Report Forecasts Blockchain Industry Value of $7.74 Billion by 2024', https://dcebrief.com/report-forecasts-blockchain-industry-value-of-7-74-billion-by-2024/
[25] Bitcoin.com (2016), 'IDC Report Says Blockchain Could Improve Gov't Functions', https://news.bitcoin.com/idc-report-blockchain-improve-gov/

longer be necessary, and routine and repetitive tasks will be automated through the use of smart contracts.[26] Financial institutions were the first to embrace blockchain, but others are also starting to adopt the underlying technology in both the private and public sectors. For example, Canada and Japan already issue digital currencies – Cancoin and Yencoin – and the People's Bank of China is planning to do the same, using the technology. Distributed ledger technology will continue to move past proof-of-concept and become an integral component of the digital economy. But like all general purpose technologies, its adoption will require many forms of adaption, cooperation on standards will become a requirement across many sectors, its benefits will continue to attract cyber-criminals seeking weaknesses in the business models, and government policy and regulations will need to be selective and focused on strategic areas, such as digital finance, without closing down upon new entry, competition and innovation.

[26] PWC (2016), 'Blockchain and smart contract automation introduction and forecast', http://www.pwc.com/us/en/technology-forecast/blockchain/introduction.html