EDISON

Blockchain adoption

Sector report

Implications for the financial services sector

Financials/technology

27 February 2020

The use of distributed ledger technology (DLT) looks set to disrupt the financial services industry through the emergence of a new asset class and its use to improve business processes. The early years of growth in digital assets largely involved virtual currencies, dominated by retail investors, and early issuance of digital securities was driven by start-ups. As regulation brings certainty to the sector and security and scalability concerns are addressed, we are now seeing concerted investment by major companies and we expect to see institutional adoption accelerate. In the longer term, as well as opportunities from asset tokenisation, we see threats to traditional financial services businesses as the role of intermediaries evolves.

Blockchain supports a new asset class

As well as supporting the emergence of cryptocurrencies such as Bitcoin, DLT can be used to tokenise existing real assets, such as shares or real estate, and create new assets that are digital representations of traditional securities. Investment in digital assets has been a mainly retail phenomenon so far, but with the introduction of new regulations to the industry and digital asset start-ups professionalising their businesses, this is becoming a more attractive market for institutional investors.

Potential to disrupt existing processes

DLT has the potential to replace many existing processes in the financial sector, such as clearing and settlement, trade finance and data management. As well as reducing back-office costs and improving transaction processing speeds, this also has the potential to reduce income streams from intermediary roles. We see new opportunities for providers of services to certify the accuracy of data before it enters the blockchain and to monitor and keep the real assets underlying tokens safe.

Early-stage market; incumbents starting to enter

The tokenisation of assets is still at an early stage, with many pilots and small-scale projects underway. Joining a plethora of digital asset start-ups, traditional financial services businesses are starting to enter the market. We expect a gradual transition to the use of blockchain technologies, with applications being adopted for those use cases with a strong commercial rationale. Ultimately, we expect to see a shift towards asset tokenisation across a number of asset classes including in particular non-listed equity, debt with small issue volumes and real estate. Strong interest from central banks in issuing their own digital currencies further supports our belief that a tipping point has been reached in the institutional adoption of blockchain.

Longer term, blockchain will reshape the industry

As well as the revenues to be earned from issuing, trading and managing digital assets, the use of DLT for business processes such as clearing and settlement has the scope to reduce operating costs. However, removing the middleman from many processes will also affect the revenues of those financial institutions that act as intermediaries. At this early stage, we expect to see more partnerships between traditional financial institutions and digital asset specialists, and longer term we expect to see incumbents acquiring to access expertise and regulated businesses.

Analysts	
Milosz Papst	+44 (0)20 3077 5700
Katherine Thompson	+44 (0)20 3077 5730

financials@edisongroup.com

This report has been commissioned by Diginex

Contents

Executive summary: Blockchain adoption in financial services

DLT disruptive to the financial services sector

DLT offers the ability to transact without the need for a trusted central authority: this disintermediation offers the potential to improve efficiency and transparency across many sectors and many business processes. We see scope for the application of DLT to be disruptive to the financial services industry in two ways: through the creation of a new asset class, digital assets, and, more specifically, security tokens; and through its use in business processes to improve efficiency and reduce costs. In the second case, it will be vital for companies to undertake a rigorous cost/benefit analysis to ascertain whether moving to the blockchain is in fact an improvement on the existing process.

Security tokens offer better liquidity and fractional ownership

Looking specifically at security tokens, the use of DLT offers the potential to reduce transaction costs and improve processing speed, while the increased transparency and trust could lead to more accurate pricing of risk. Moreover, smart contracts introduce liquidity to asset classes that were traditionally considered illiquid and allows for fractional ownership, reducing the minimum ticket size for investors. Digital assets may also allow for the creation of more innovative financial products, which may, among others, extend access to un/underbanked populations. Small-scale security token offerings (STOs) have shown how different types of assets can be tokenised, such as equity in private companies, real estate and debt. We believe that in the shorter term, many of these deals will be structured as hybrids, with the majority stake still offered through traditional financing routes and a minority stake tokenised as proof of concept. As the number of STOs to date is low and regulation is still taking shape in this area, secondary trading has been predominantly OTC driven; in the longer term, as volumes grow, we would expect to see the emergence of regulated digital securities exchanges.

Blockchain projects funding becoming more mature

During the cryptocurrency boom in 2017 and early 2018, initial coin offerings (ICOs) represented the most popular funding option for blockchain-based projects. Subsequently, ICO funding volumes declined due to higher regulatory scrutiny coupled with deteriorating investor sentiment. At the same time, the focus of venture capital (VC) funding has shifted from companies focused merely on cryptocurrencies and exploratory projects to businesses developing specific marketable products, as well as those active in cryptocurrency mining or digital asset infrastructure (including secondary market trading and custody, and asset tokenisation). STOs constitute a viable funding option and may be considered the next generation of ICOs. This is because: 1) security tokens are better structured in that they represent rights to actual assets and cash flows similar to traditional financial instruments; and 2) they are better regulated and normally fall under same/similar regulations as off-chain securities.

Incumbents starting to engage in pilots, new services

As well as undertaking internal projects to test the use of DLT technology, many of the larger traditional banks are starting to get involved in pilot projects involving other banks or developing services for digital assets. Fidelity has launched a digital assets business that offers secure custody and trade settlement for Bitcoin. Nomura and Vontobel have entered the digital asset custody market. Both the Swiss and London Stock Exchanges are actively involved in the development of security token exchanges and the ASX is in the middle of a project to shift its clearing and settlement system to the blockchain.

Emergence of digital asset players in financial services

The digital asset market has been driven by start-ups, many focused on specific areas such as virtual currency exchanges (VCEs), security token issuance platforms, digital asset custody and crypto mining. Recognising that institutional investors require access to regulated services, digital asset-focused banks and service providers are emerging such as Bakkt, Diginex, Sygnum and SEBA. Some of the large VCEs are looking to expand into regulated security token trading. A number of asset management companies have developed as pure-play digital asset investors, offering institutional investors exposure to the sector.

Institutional adoption to date has been held back by regulatory, security and scalability issues

As the digital asset market has developed, we have seen extreme cryptocurrency price volatility, criminal involvement, numerous coin losses through hacks and errors, the ICO boom and bust, lack of regulation and issues with the scalability of certain cryptocurrencies. These issues have served as barriers to adoption for institutional investors. We believe that many of these issues are being addressed, paving the way for institutional investors to adopt digital assets as a new asset class.

Fast-evolving regulation is bringing certainty to the sector

Regulators are starting to take digital assets seriously. While some countries have a draconian approach to digital assets, others are keen to balance the protection of consumers with the commercial benefits that use of innovative digital assets can bring. Although digital assets are decentralised and hence global in their scope, regulation is undertaken on a country-by-country basis. The lack of a cohesive global framework provides scope for regulatory arbitrage and raises issues around jurisdiction for contracts and data security. The more open countries are bringing digital asset issuance, trading, custody and asset management under their existing or new regulatory frameworks, including the application of know your customer (KYC), anti-money laundering (AML) and combating the financing of terrorism (CFT) processes. Although stricter regulation is likely to reduce the level of anonymity enjoyed by the sector, it should make it a more attractive sector for institutional investors. Further clarity from regulators on areas such as tax, accounting, data protection and the treatment of smart contracts is still required.

Addressing security and scalability concerns

The larger players in the market understand the need to be seen to take the security of their and customers' assets seriously. This includes seeking security and control audits from third-party specialists, obtaining ISO 27001 certification, using or creating custody services and putting insurance in place. For public blockchains, the shift to proof-of-stake (PoS) consensus mechanisms and the use of sharding or Layer 2 solutions should improve processing speeds. Private blockchains suffer less from scalability issues, as they do not need to use such complex consensus protocols and have a limited membership. While use of DLT results in disintermediation of traditional players, it adds a new requirement for trusted third parties to verify information is accurate before it is put on the blockchain and to ensure real assets' underlying tokens have not been stolen or damaged.

Longer term, DLT represents both a threat and an opportunity to the financial services industry

We expect a gradual transition to the use of blockchain technologies, with applications being adopted for those use cases with a strong commercial rationale. Ultimately, we expect to see a shift towards asset tokenisation across a number of asset classes including non-listed equity, debt with small issue volumes and real estate. Strong interest from central banks in issuing their own digital currencies further supports our belief that a tipping point has been reached in the institutional adoption of blockchain. We view this shift as presenting both threats and opportunities for the financial services industry. As well as the revenues that can be earned from issuing, trading and managing digital assets, the use of DLT for business processes such as clearing and settlement, trade finance and identity verification has the scope to reduce operating costs. However, removing the middleman from many processes will also affect the revenues of those financial institutions that act as intermediaries, for example, fees earned on cross-border transactions, foreign exchange, payments and security registration. At this early stage in the market, we expect to see more consortium activity and partnerships between traditional financial institutions and digital asset specialists. While we see corporate VC activity already picking up, longer term we would also expect to see the incumbents acquiring to access expertise and regulated businesses.

Introduction

In this report, we examine the current status of DLT adoption in the financial services sector, with a particular focus on institutional engagement with the technology. We identify the current barriers to adoption of DLT-based assets and services within the sector and investigate what is being done to overcome these. We also highlight areas where work still needs to be done to make the technology more appealing to institutional investors.

As well as undertaking desk-based research, we have interviewed companies involved in different areas of the sector, including technology companies, NGOs and investment companies.

An introduction to DLT

The basics

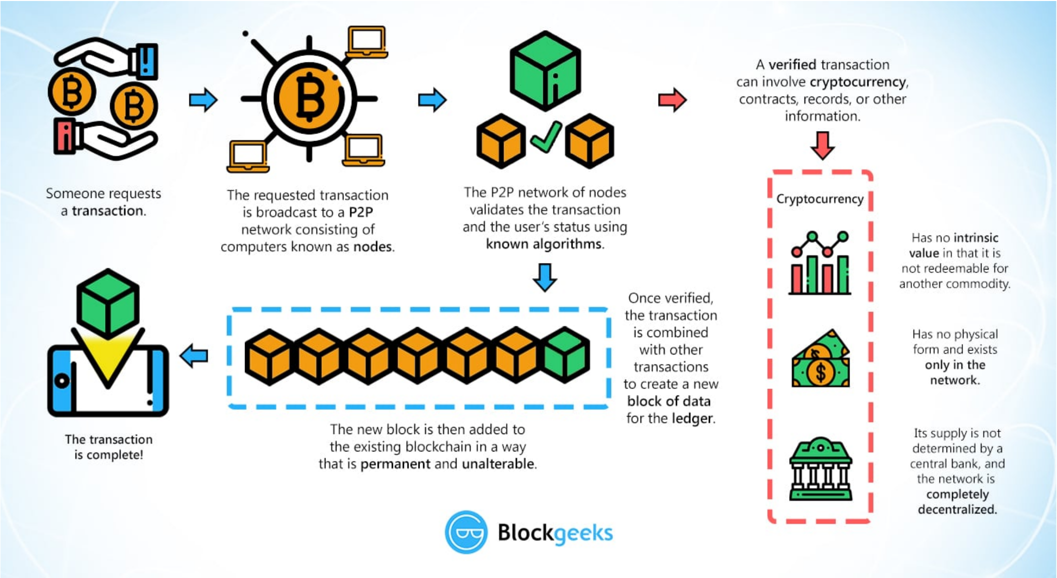
A distributed ledger is a database that is shared across a peer-to-peer network, synchronised so that all nodes in the network have a copy of the same data and based on all nodes agreeing on the data (consensus).

Key advantages of DLT include:

- It represents a reliable mechanism for transparent validation of transactions without the need for an independent third party.
- Data security is underpinned by a decentralised database based on cryptographic algorithms.
- Transactions are recorded in a chronological order (creating an immutable chain of records), with all blocks timestamped and linked to the previous one, translating into improved traceability.

A blockchain is a type of distributed ledger. It creates a linked list of transaction updates to a virtual digital public ledger. Each block in a blockchain consists of a group of transactions. To contribute transactions to a block and for that block to be added to the blockchain, a particular process is followed (see Exhibit 1). First, the initiator of a transaction sends it to the address of the recipient (public key) after signing it with their digital key (private key) to authenticate it. It is then broadcast to the entire network for each node to validate. Certain nodes, called ‘miners’ or ‘validators’, use the blockchain’s consensus mechanism to add transactions to a block. Once complete, the block will be added to the blockchain with a timestamp and a reference to the previous block, then broadcast to the network. The cryptographic link from one block to the next means previous blocks cannot be altered.

Exhibit 1: Transaction cycle for blockchain


Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers known as nodes.
The P2P network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
Cryptocurrency
Has no intrinsic value in that it is not redeemable for another commodity.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank, and the network is completely decentralized.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain in a way that is permanent and unalterable.
The transaction is complete!
Blockgeeks

Source: Blockgeeks (www.blockgeeks.com)

Different ways to achieve consensus

Proper functioning of blockchain networks depends on a coherent mechanism used by the distributed nodes to validate subsequent blocks that can be added to the chain, referred to as the consensus algorithm. The blockchain sector is still looking for a consensus protocol that will provide the optimal trade-off between efficiency and the level of decentralisation or democratisation and safety of a public network. The former is measured by power consumption requirements (in Watt hours) and the number of transactions it allows to process (transactions per second, TPS), while decentralisation may be tracked by examining the contribution of the respective block validators (which is a function of how the processing power is distributed between them).

Bitcoin uses proof-of-work

The first protocol, which was embedded in Bitcoin (and later in Litecoin), is the so-called **'proof-of-work' (PoW) algorithm**. Here, block validators use their computing power to compete against each other to solve a 'mathematical puzzle' that is hard to crack but easy for others to verify the solution (in the case of Bitcoin, it is called 'hashcash'). Whoever does it first is allowed to add the next block to the chain. In exchange, the validator receives a certain amount of the cryptocurrency or token as a reward. Consequently, these validators are often referred to as cryptocurrency 'miners'. The more computing power a validator has, the more likely it is they will solve the equation first.

PoW requires high levels of computing power and electricity

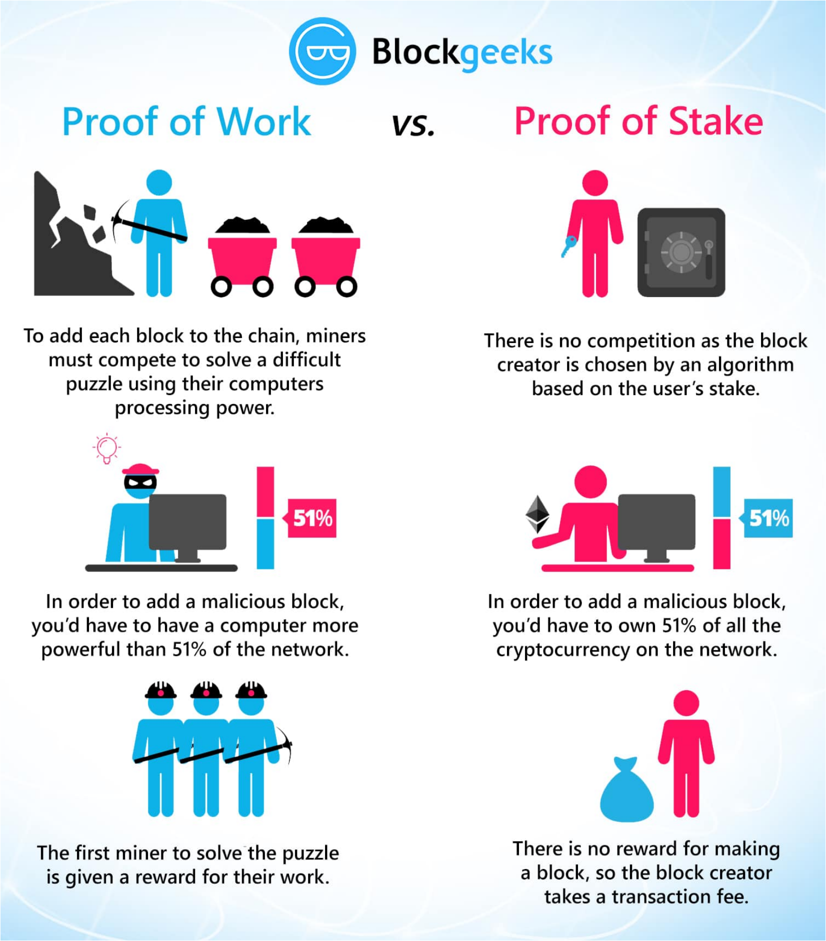
Unfortunately, this block-validation process requires immense computing power available only to large mining pools deploying application-specific integrated circuits, which results in a high concentration of miners (as illustrated by the so-called hash rate distribution). Currently, four China-based mining pools (F2Pool, Poolin, AntPool and BTC.com) control more than 50% of Bitcoin's total mining power, according to BTC.com data. Another issue is the considerable amount of electric power consumed by miners to conduct the cryptographic calculations (69TWh per year according to the Cambridge Bitcoin Electricity Consumption Index, which is more than Switzerland consumes annually), which is used exclusively to maintain the blockchain's security. At the same time, the algorithm behind Bitcoin allows for limited processing speed (at around 7TPS calculated based on an average transaction size). Finally, the PoW consensus algorithm is susceptible to the so-called '51% attack'. In theory, a group of attackers could gain control over the majority of mining power and monopolise the generation of new blocks. Consequently, even though Bitcoin remains by far the largest cryptocurrency by size (making up c 66% of the total cryptoassets market capitalisation) and is solidifying its position as a digital equivalent of gold, it has a limited range for future applications. This is because it is merely a digital currency as opposed to for example Ethereum, which is designed to accommodate the so-called 'smart contracts' (see below for details), which are the key tool used to tokenize assets.

PoS rising in popularity

An increasingly popular alternative protocol is the **'PoS' algorithm**, which allocates mining power based on the percentage of cryptocurrency held by the respective block validators in a dedicated wallet (locking these coins). Miners do not compete with computing power, but with the amount of cryptocurrency they have 'staked' (and in some versions of the algorithm, also the duration of the stake). As a result, this protocol is characterised by lower power consumption and potentially faster transaction processing (eg Tezos based on PoS can handle up to 40TPS or the non-blockchain DLT network Hedera HashGraph, which claims that it can handle 10,000+ TPS). Ethereum, the second-largest cryptocurrency by market capitalisation (characterised by a speed of c 15–20TPS), is on its way to transition from a PoW to a PoS environment (through the so-called Casper update).

Rather than being awarded a certain amount of cryptocurrency, block validators earn transaction fees (this is why they are sometimes called 'forgers' rather than 'miners'). The blockchain's stability is facilitated by the interest block validators have in keeping the network secure (given they have 'skin in the game'). In some cases (eg the planned Casper implementation in the case of Ethereum) stakers who validate the wrong transactions have their staked coins confiscated. Nevertheless, the algorithm still promotes centralisation to some extent, as it is favouring those validators who stake the highest amount. Moreover, PoS networks are susceptible to a potential '51% attack' (see page 33 for further detail).

Exhibit 2: Proof of work versus proof of stake


Blockgeeks
Proof of Work
vs.
Proof of Stake
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.
There is no competition as the block creator is chosen by an algorithm based on the user's stake.
51%
51%
In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.
In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.
The first miner to solve the puzzle is given a reward for their work.
There is no reward for making a block, so the block creator takes a transaction fee.

Source: Blockgeeks (www.blockgeeks.com)

A number of further block validation algorithms are applied in public blockchains, such as delegated PoS (DPoS, applied in the EOS blockchain), which is a variation of the PoS protocol, delegated Byzantine fault tolerance (used by the NEO blockchain platform) and many others.

We asked **Yorke Rhodes, head of blockchain at Microsoft,** his thoughts on the competing consensus algorithms:

> *Proof-of-stake is the future of blockchain, with a validator pool that is demonstrably decentralised enough (as opposed to the DPoS solution used by EOS), which is particularly important in a public network. Ethereum is on a path to transition to a proof-of-stake framework, from its current proof-of-work origins. It is worth keeping in mind that public blockchain implementations are quite difficult (Bitcoin is a good illustration of this). By necessity upgrades are executed through soft and hard forks.*[1] *A quite promising and mature example of a proof-of-stake system is Celo (a fork of Ethereum). It represents a reserve-based PoS environment and implements functionality to include representation of stablecoins in the base layer. Facebook's Libra also relies on a reserve-based PoS framework.*

[1] A change to the blockchain network's protocol resulting in new consensus rules (with non-upgraded nodes excluded from the validation of new blocks).

Private blockchain consensus requirements less onerous

At the same time, we note that consensus algorithm requirements differ in a private blockchain. This is because the consensus layer in a private blockchain is usually more relaxed in comparison with a public blockchain, given there is strict control over who is being allowed into the chain, facilitating a secure set of participants. The most popular consensus algorithm in private blockchains is proof of authority, where transactions and blocks are validated by approved accounts (validators), allowing much faster transactions. Having said that, there is a number of alternative consensus algorithms and the optimal choice may be different for specific implementations.

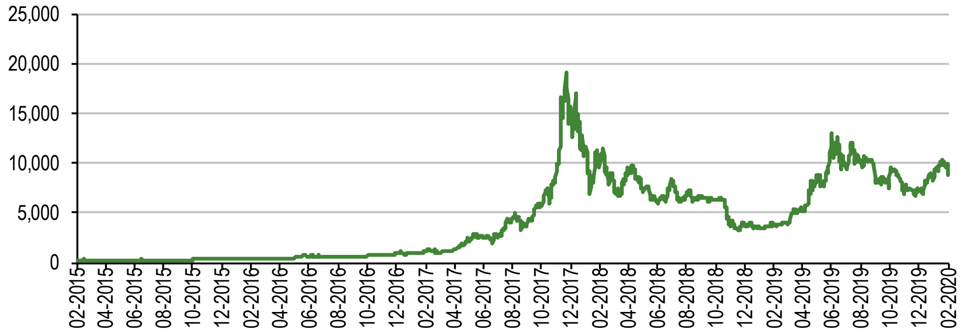
Digital assets explained

Cryptographically based assets are described in many ways: cryptoassets, cryptocurrency, security tokens, digital assets, etc. For the purposes of this report, we use the term digital assets. The broader public associate digital assets primarily with Bitcoin, which is only one manifestation of the technology (although the largest in terms of market cap, Exhibit 4). Any digital asset may be classified into one of three main categories: exchange, utility or security tokens.

Exchange tokens: Bitcoin the best-known

Also referred to as cryptocurrencies, virtual currencies or payment tokens, exchange tokens were the first class of blockchain-based digital assets to emerge, with some prominent examples including Bitcoin (the first cryptocurrency launched in 2009) or Litecoin. Although designed mainly as a means of value exchange representing a potential alternative to payment systems based on traditional (fiat) money, cryptocurrencies attracted significant speculative demand resulting in a boom and bust in 2017 and 2018. The price of Bitcoin went up from c US$1,000 in early 2017 to US$20,000 at peak at end-2017, then declined to around US$8,000–10,000 at present (Exhibit 3). This speculative wave has not only affected the most popular cryptocurrencies but was marked by the emergence of a plethora of new digital assets (most of which may be classified as utility tokens, see below).

Exhibit 3: Bitcoin price evolution (US$)



Source: Refinitiv

Stablecoins introduced to cope with exchange token volatility

High price volatility remains one of the main disadvantages of plain exchange tokens as a payment means. As a result, a new digital asset class (called **stablecoins**) has been developed, which has its value pegged to another currency or asset (stabilising the coin's value). In most cases this would be a traditional currency such as the US dollar (such as in the case of the standard Tether coin, the largest stablecoin by market capitalisation at present), although stablecoins may also be pegged to commodities (such as gold, eg Tether's recently launched Tether Gold, or oil, eg Venezuela's oil-backed cryptocurrency called Petro), real estate or even another cryptocurrency (with a degree of over collateralisation to absorb price volatility in the underlying asset). There is also a group of non-collateralised stablecoins with their supply regulated by a certain algorithm, which addresses increasing (or declining) demand for the cryptocurrency by issuing (or buying back) coins. Finally, hybrid stablecoins (combining the features of collateralised and non-collateralised coins) are also being explored at present.

Stablecoins pique the interest of central banks and Facebook

Stablecoins seem a promising solution for, among others, peer-to-peer payments, remittances, clearing and settlement (including settlement on crypto exchanges), as a means of value storage, as well as an indirect way for crypto exchanges to offer crypto-fiat trading pairs. We see some large incumbent players launching pilots based on coins similar to stablecoins in the clearing and settlement space (eg JPM or Wells Fargo, as discussed in more detail below).

We must note however that stablecoins based on traditional currencies (ie fiat-based) are centralised as they require a trustworthy entity that is responsible for maintaining the reserves backing up the stablecoin. The recent trust issues related to the US dollar reserves of Tether are a good example of how important this can be. Nevertheless, the asset class is considered as compelling, given that Facebook is attempting to launch its own stablecoin (using a reserve-based PoS protocol) called Libra, although it has been struggling to do so due to regulatory pushback amid concerns around AML.

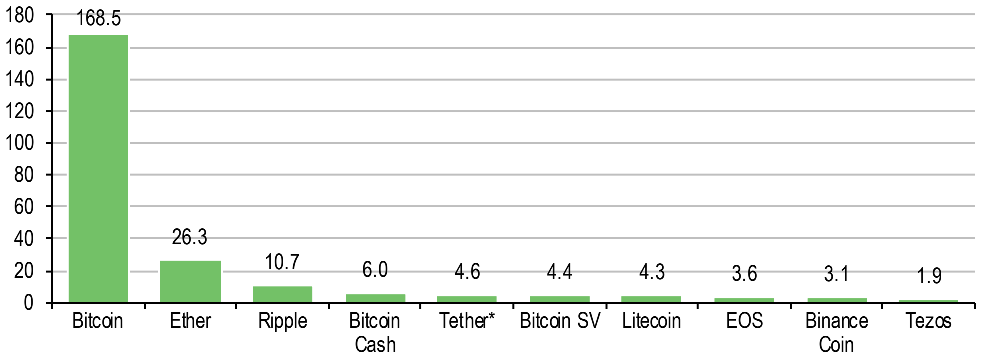
Moreover, the emergence of stablecoins has sparked a discussion around the potential introduction of central bank digital currencies (CBDC, stablecoins backed by the native currency), as highlighted by the European Central Bank in one of its papers published in August 2019 (*In search for stability in crypto-assets: are stablecoins the solution?*). A survey conducted of 66 central banks by the Bank for International Settlements (BIS) in January 2020 indicates that 80% of central banks are engaging in work on CBDCs, whereas c 40% have moved from conceptual research to experiments or proof-of-concept and another 10% have developed pilot projects. Six central banks have formed a working group with the BIS to assess the economic, functional and technical design choices, including cross-border interoperability of CBDCs. The members of the group are the BIS, Canada, the ECB, Japan, Sweden, Switzerland and the UK. The Swedish central bank has recently announced the start of a CBDC (e-krona) trial with Accenture on the Corda blockchain until February 2021.

Utility tokens: Providing access to products and services

Utility tokens provide access and use rights to a certain digital resource. A few of the most popular utility tokens include Ether (associated with the Ethereum blockchain), Ripple, EOS or Stellar. However, a variety of other tokens were issued through ICOs, often on a third-party blockchain (eg Ethereum) to finance the development of a certain product or service (eg decentralised applications), which can be subsequently used or consumed by the holders of these specific utility tokens. We present a few examples of utility tokens and their applications below:

- Basic Attention Tokens (BAT), which may be used to obtain certain advertising services on the BAT platform.
- Filecoin token, which allows users to access a decentralised cloud storage platform.
- Tronix, which can be used to buy content (eg video on demand) on the Tron network.
- FUN, which is a token acting as a betting chip in the FunFair gaming ecosystem.

Exhibit 4: Top 10 exchange and utility tokens by market capitalisation (US$bn)



Source: CoinMarketCap data at 26 February 2020. Note: *Stablecoin.

Security tokens: Tradeable digital financial instruments

These tokens are a digital version of traditional securities and usually represent an investment instrument secured by actual assets or cash flows, rather than exchange tokens (an alternative currency used for payments) or utility tokens (which are worth only as much as the service/product they provide access to). Moreover, security tokens (and STOs) are much better regulated. For example, the German watchdog (BaFin) is classifying security tokens as securities if they meet the following three criteria: freely transferable; traded in financial markets; and equipped with rights similar to those attributable to securities. For a detailed overview of the regulatory landscape related to digital assets, please see below.

Smart contracts have terms embedded directly in the code

A distinct feature of security tokens is that they are structured as smart contracts, which means they represent an agreement between buyer and seller with its **terms directly embedded within the code that are automatically executed**. This is important as it eliminates the need to involve third parties responsible for monitoring the execution of agreement terms. At present, the most popular technical standard for smart contracts used to structure security tokens is the Ethereum Request for Comments 20 (ERC-20) standard using the Ethereum blockchain. Although it is not perfect in its design, it has definitely been successful as an early standard on which providers of digital wallets could rely, helping create liquidity in the market. Although it is likely to remain the dominant standard in the near term given the support it receives from wallets, there are several promising alternative protocols that may better serve specific industry requirements.

For instance, ERC-721 (another Ethereum-powered protocol) may be better equipped for gaming items and collectibles given that, unlike ERC-20, it is not a representation of a pool of fungible digital assets, but represents a single non-fungible (unique) type of token. In fact, it already receives support from the gaming community. One of the decentralised applications that allowed the ERC-721 standard to gain publicity in the crypto collectables space was CryptoKitties, a blockchain-based virtual game (released by Axiom Zen) allowing users to breed and trade unique virtual cats (its transactions peaked in December 2017, visibly clogging up the entire Ethereum network).

A token standard under development that may play an important role in STOs in the future is ERC-1400 (compliant with ERC-20), which aims to replicate traditional securities more accurately, introduce a more transparent transaction process and facilitate legal and regulatory compliance (eg with respect to KYC/AML) specific to the respective jurisdictions (eg it allows automatic whitelisting of investors based on their residency). It also features the functionality to reverse the crediting of tokens to a given wallet.

DLT use cases in general

Growing awareness of the significant potential associated with DLT technology is illustrated by the results of a survey conducted by Deloitte in 2019 among senior executives of US companies with US$500m+ in annual revenues and non-US companies with annual sales of US$100m+. According to the survey, 83% of respondents see compelling use cases for blockchain, with 53% placing blockchain within their top five strategic priorities. Key advantages over the existing systems they highlighted included: new business models and value chains; greater security/lower risk; greater speed compared to existing systems; greater transparency; lower costs; improving identity control; and fraud reduction.

There is a plethora of prospective blockchain use cases across industries and it is difficult to mention all of them. Below we present selected applications across industries and society (with specific use cases in the financial industry discussed later in the note):

- **Supply chain management** – addressing the complexity and limited transparency of supply chains that leads to inefficiencies and increased risk of fraud (eg counterfeit goods). The use cases include the provenance of commodities, as illustrated by the Tracr platform launched originally by De Beers (one of the largest diamond mining companies globally). Blockchain may also facilitate food safety.
- **Digital identity management** – allowing for quicker and safer onboarding of clients through smoother KYC/AML procedures while providing stronger data protection.
- **Voting systems** – facilitating an efficient and safe system for remote voting, such as during political elections or general meetings of shareholders.
- **Healthcare** – multiple possibilities for medical record access, clinical trial monitoring, analysis of credentials/track record of health professionals, communication between patients and doctors, etc.
- **Intellectual property rights** – blockchain seems to be a good setup to record and timestamp ownership of IP rights to eliminate legal disputes.
- **Energy** – tracking the provenance of green energy production in a decentralised power network involving rooftop solar and other small sources of renewable energy.
- **Media and entertainment** – potentially eliminating the need for a content aggregator such as Netflix by introducing a convenient environment for peer-to-peer transactions between content providers and consumers, as well as reducing copyright infringement risk.
- **Marketing and advertising** – helping reduce or eliminate advertising fraud and lack of transparency.
- **Law** – introducing a reliable, transparent and immutable setup to digitally sign and store legal agreements, including ownership records; leveraging smart contracts to reduce paperwork.
- **Justice system** – providing a platform to secure digital forms of evidence.
- **Charity** – introducing a transparent trail for donations.
- **Human rights** – using blockchain to track migrants with the aim of reducing the incidence of modern slavery. The UN's International Organization for Migration is working with Diginex to use the blockchain to reduce the illegal fees charged to migrant domestic workers.

It is important that the organisations considering the use of DLT have a strong business rationale for doing so. Due to the cost of building and moving to the new technology, as well as remapping business processes, it is not always appropriate to use blockchain technology. Projects that are best suited to using blockchain include those where trust is core to the application, participants are motivated to share information and there is potential for disintermediation.

DLT use cases in the financial industry

DLTs (including blockchain) offer compelling solutions both standalone and as a native environment for various types of digital investments (in particular security tokens). As highlighted above, one of the main distinctive advantages of blockchain technology is the ability to take over the role of a middleman (eg notaries, insurers, registrars, transfer agents or banks in some cases) and **validate data integrity** in a decentralised setup (which facilitates faster and more comprehensive data access for all participants). These features are further strengthened by the deployment of smart contracts, where the rights of the respective counterparties (eg investors) and desired compliance rules are embedded in the token code and thus automatically executed (without third parties). This includes, among other things, coupon and dividend payments, voting rights, escrow arrangements and collateral management. This translates into **reduced transaction costs** and **faster processing speeds** due to a lower number of market participants and touchpoints that have to be involved, as well as **increased transparency and trust**, leading to a **more accurate pricing of risk**.

Moreover, smart contracts introduce **liquidity** to asset classes that were traditionally considered illiquid, which may potentially lead to improved valuation on the back of a reduced illiquidity discount applied by investors. They also allow for **fractional ownership**, reducing the minimum ticket size for investors. Digital assets in a blockchain environment may also assist the **creation of more innovative financial products (or reinvention of existing products)**, which may, among other things, extend access to un- or underbanked populations. In this section of our report, we discuss selected potential DLT implementations in finance.

Payments and trades settlement

Legacy bank systems are characterised by complexity and inefficiencies leading to elevated costs. Blockchain offers the potential for faster processing speeds (in real time), improved accuracy, lower counterparty and settlement risk, freeing up of collateral, as well as reduced costs and requirements to handle exceptions. Blockchain is a promising solution to introduce real-time, trade date settlement (including cross-border operations) by creating a direct, transparent and secure transaction framework between custodians and counterparties. In this context, we note that the introduction of a digital currency (in particular a form of stablecoin) for the payment leg of security settlement will be necessary to reap the full benefits of DLT.

A number of banks have already embarked on blockchain-powered pilot projects. In February 2019, JP Morgan announced the creation and successful testing of a digital coin based on the US dollar (called JPM coin) for payments between institutional clients. JPM coins are issued on the Quorum blockchain and are redeemed for the equivalent amount of US dollars once the transfer is complete. A similar pilot project, Wells Fargo Digital Cash, was announced in September 2019. In June 2019, the *Wall Street Journal* reported that 14 financial companies led by UBS plan to use a blockchain-based token called utility settlement coin (USC) in cross-border trading activity.

More recently, the press reports that JP Morgan is in discussions to merge its Quorum blockchain unit with ConsenSys, a blockchain start-up focused on developing enterprise applications and building developer tools. ConsenSys was founded in 2014 by one of the original co-founders of Ethereum.

However, there are some voices expressing caution over the efficiency of the existing blockchain technology, such as the president of the German Central Bank, who declared in May 2019 that in a trial project the bank has conducted with Deutsche Börse (initiated in 2016), deployment of blockchain for transfer and settlement of securities and cash turned out to be more expensive and slower than traditional solutions. Similarly, in a recent report called *The Tokenisation of Assets and Potential Implications for Financial Markets*, the OECD highlighted the application of DLTs in clearing and settlement has produced mixed results and hurdles in the development of the technology will need to be overcome for the application to arrive at the stage where it can provide better performance than systems currently in use. However, the OECD's comment may be largely based on the pilot conducted by Bundesbank and Deutsche Börse mentioned above.

We note that the ASX is in the process of moving its clearing and settlements system from the existing CHESS system to a blockchain-based system designed by Digital Asset Holdings. The new system is targeted to go live in April 2021. In the US, the Depositary Trust & Clearing Corporation (DTCC) is developing a blockchain-based post-trade system for derivatives. It had planned to launch this in the latter part of 2019, but has delayed it until after Brexit.

Lending

Live implementation of digital assets is progressing in **mortgage lending**, translating into faster lending decisions, elimination of excessive commission structures, process automation, as well as risk reduction through improved transparency. An example of digital mortgage originators is Provenance, a private (ie permissioned) PoS blockchain launched by Figure Technologies (a US fintech unicorn offering retail loan products). The blockchain will not only be used to originate loans and receive loan payments, but also to buy and sell loans in the secondary market. In May 2019, Figure announced it has implemented an up to US$1bn asset-based financing facility on the blockchain alongside Jefferies and WSFS Institutional Services to drive further lending on the network. At the same time, we note that other loan issuers are to operate on the network (which is not owned by Figure). In September 2019, Caliber Home Loans (one of the leading US mortgage lenders and an approved seller/servicer for both Fannie Mae and Freddie Mac), became the first outside lender on Provenance.

Blockchain-based smart contracts may also help improve efficiency of both transaction execution and subsequent loan servicing in the case of **syndicated loans**. The first syndicated loan on the blockchain (Ethereum) with a volume of US$150m was completed in November 2018 by the Spanish bank BBVA alongside two partner banks (MUFG of Japan and BNP Paribas of France) for Red Electrica (a Spanish grid operator).

Trade finance

International trade remains constrained by cumbersome paper-based processes, especially affecting small and medium-sized enterprises, as well as trade with emerging and frontier markets. The Asian Development Bank estimated the trade financing gap in 2017 (as measured by rejected trade financing transactions) at 10% of global merchandise trade volumes (c US$1.5tn). The gap was mostly attributable to SMEs (75%) and to Asia (c 40%). This is where the new technologies such as blockchain (and artificial intelligence (AI) or the Internet of Things) come into play. As in the case of other applications, blockchain introduces faster processing using smart contracts, quicker credit risk assessment based on transaction history, enhanced transparency, reduced risk, coupled with lower costs and the ability to conclude small-ticket transactions. According to an analysis prepared by Bain & Company in 2018, DLT should enable US$1.1tn of new trade volume by 2026, whereas 40% (or US$0.9tn) of traditional documentary trade will move to DLT.

The first pilot transactions involving letters of credit (LC) in a blockchain environment have already been conducted using, for example, the Voltron platform, a project built on R3's Corda blockchain technology and developed by a consortium of eight banks including HSBC, ING, Standard Chartered, BNP Paribas, CTBC Holding, Bangkok Bank, NatWest and SEB. For example, in August 2019, the platform was used by Standard Chartered to complete its first blockchain-based LC transaction in less than 12 hours. In September 2019, HSBC completed its first yuan-denominated blockchain-based LC transaction using Voltron, allowing the exchange of documents within just 24 hours (compared to standard processing time of five to 10 days). The platform has just completed the pilot phase and has gone into full commercial production. A new legal entity called Contour was created to operate the platform, owned by seven of the original eight banks (NatWest chose not to participate) and has since received investment from Citi Ventures.

Moreover, R3 has recently completed a trade finance trial (focused on receivables finance, namely factoring) on the Marco Polo platform involving more than 70 organisations from 25 countries, including ABN AMRO, Commerzbank, BMW, Sumitomo Corporation and SBI Holdings. Marco Polo was established by R3 together with TradeIX, a Dublin-based technology company that recently attracted Accenture as an investor and strategic partner.

Digital identity

Using blockchain in identity verification for KYC, compliance, AML and CFT processes may bring additional efficiency and savings to the financial industry while improving the customer experience through enhanced data protection. The technology should, for instance, allow the consolidation of all client-related identification documents in a digital framework. It can also be used to give individuals control over their identity information, enabling them to choose who they share the data with. In November 2017, IBM announced it has completed the proof-of-concept of a shared KYC project together with Deutsche Bank, HSBC, Mitsubishi UFJ Financial Group and Cargill. In May 2019, the identity and authentication provider SecureKey Technologies announced that its blockchain-based digital identity network Verified.me (built on the IBM Blockchain Platform) was introduced to customers of five Canadian financial institutions (CIBC, Desjardins, RBC, Scotiabank and TD). Network participants of Verified.me include banks, telecom companies and credit and government agencies, such as the Digital ID and Authentication Council of Canada, the Science and Technology Directorate within the US Department of Homeland Security or Equifax. Another project in the KYC area is KUBE, which was launched by four major Belgian banks (Belfius Bank, BNP Paribas Fortis, ING Belgium and KBC) to share corporate KYC data.

Data management

A good example of the efficiency improvement potential in data management is the **investment fund** industry, where data distribution faces a number of challenges at present, with the majority of unlisted data still being transmitted via email and the prevalent inability to obtain data from a single provider translating into high error rates (creating litigation risk arising from incorrect fund pricing) and issues with timeliness and cost efficiency. Blockchain technology has the potential to solve this problem. For instance, technology company BC Gateways is commercialising a solution in Australia, called The Gateway, that uses a hybrid private/public blockchain network environment (with the private part based on Hyperledger Burrow and the public part using the Ethereum blockchain). This allows participants to publish and/or subscribe to pricing and other fund data via The Gateway. Direct participants can view the data on the private blockchain on a permissioned basis. Data are hashed and stored on the private blockchain; hashes of those blocks are then stored on the public blockchain to provide an audit trail.

Security tokens on the verge of disrupting investments

We believe there is considerable potential for asset tokenisation, which represents two types of operation: the creation of unique tradable digital representations of existing real assets (and the associated future cash flows) on a blockchain network; or the issuance of new assets in a tokenised form, which resemble traditional asset classes. According to the Technological Tipping Points survey conducted among over 800 executives and experts from the IT and communications sector by the World Economic Forum in 2015, up to 10% of global GDP will be stored and transacted on a blockchain by 2025 (as expected by 58% of the respondents). This compares with less than 1% of GDP currently (almost exclusively consisting of exchange and utility tokens, namely cryptocurrencies such as Bitcoin).

Although the above is a raw indication and awareness of all potential applications of digital tokens is still in its early stages, there are several projects being launched across different asset classes, proving the digital asset disruption has already started (see below). At present, they mostly constitute pilot projects that are tailormade for investors who have already expressed interest in the particular asset ahead of the offer structuring and were open to embracing the new technology. **It is likely that, in the initial stages, some deals will be structured as hybrid transactions where the majority stake is offered using traditional financial instruments, whereas a minority stake is offered as a digital asset**. An example here is the tokenisation of a 12-unit luxury condo Manhattan property development described below. **However, we believe a growing number of successful pilots will create a foundation for more standardised tokenisation services and encourage investors to participate in transactions with ownership entirely through digital assets**. We already see pure digital deals being executed, such as the first Swiss IPO of tokenised shares recently launched by OverFuture (which through its subsidiary operates in the Internet of Things (IoT) industry).

One of the critical prerequisites driving digital representations of physical assets is the deployment of credible custodians who will guarantee the connection between the off-chain assets being digitalised and the blockchain remains intact (for instance, real assets have not been stolen or damaged).

Equities – attractive for non-listed companies

We believe asset tokenisation is a more compelling solution for non-listed equities (especially start-ups and shares in VC funds, but also private equity and infrastructure investments) than listed equities. Here, the lack of a marketplace where stakes in businesses could be traded often represents an unmet need. This translates into longer lead times to exit or IPO (often forcing VC funds to extend their lifetime), the inability to liquidate assets and a resulting pressure on management to complete exits or list prematurely. It also often leads to the so-called block risk (a large exposure to a single holding) in the case of founders and business angels. The introduction of a digital process should reduce the costs and time associated with start-up funding rounds. As a result, start-ups will not be forced to bundle financing activity in large funding rounds (and consume the proceeds over a long time) but instead conduct smaller and more frequent capital raises whenever the need arises.

On the contrary, in the case of listed equity, the trade-off between potential benefits and implementation costs is rather poor. In fact, the introduction of on-chain trading could potentially divide the stock's liquidity into two separate pools (off-chain and on-chain) and have a negative impact on its off-chain liquidity (although this may potentially be mitigated by a high level of interoperability between the off- and on-chain environment).

Tokenised non-listed equity may be particularly interesting for certain investor groups, according to **Stefan Schütze, board member at FinLab**, a German VC fund specialising in fintech investments (covered by Edison):

> *STOs of non-listed equity (eg stakes in limited liability companies) provide an interesting entry point for several investor groups, in particular business angels and family offices, who normally do not require the same extent of controlling rights as VC funds and at the same time would appreciate the possibility to exit the investment more easily. Moreover, these investor groups are able to participate in offerings (including STOs), which are exempt from the issue prospectus publication requirement in Germany (ie where, among others, the ticket size is at least €100k and the number of investors participating in the offering is fewer than 150).*

The tokenisation process requires specialised technological and legal know-how. Consequently, a number of companies have established STO platforms (such as Polymath, Securitize, Harbor, Swarm and Cashlink) to provide services to potential issuers, including a technical framework for STOs; standardisation of issued digital securities and contractual agreements; an automated, cost-effective offering process; compliance with local regulations; and access to various other service providers involved in an STO (eg custodians). Importantly, these platforms also arrange STOs representing financial instruments other than equity.

However, they should not be considered the primary marketplaces for secondary trading, as outlined by **Michael Duttlinger, CEO and co-founder of the issuance provider of digital securities Cashlink** in a recent discussion with Edison:

> *While one of the main advantages of digitalizing assets is providing liquidity to non-listed assets, at the current early stage of the digital assets market (characterised by limited transaction volumes), there is no immediate need for providing significant liquidity. Consequently, the secondary market will likely be limited to OTC peer-to-peer trading in the short term. However, as the number and scale of digital assets becomes more meaningful, large crypto exchanges as well as traditional exchanges willing to expand into the digital assets space will play a greater role as liquid secondary markets. It is worth highlighting that some issuance providers of digital securities (such as Cashlink) do not intend to become centralised markets to trade already issued digital securities and rather focus on providing the sophisticated technical framework, deal structures and post-issuance services compliant with current regulations (which may potentially be developed into a white-label solution), as well as connecting issuers and investors to trusted service providers. Also, they do not necessarily have to be responsible for the distribution of digital securities during the issuance process.*

Debt – testing the market

For **bond issuance**, a good example is the bond-i issue conducted by the World Bank, with the first transaction announced in August 2018 (raising US$81m proceeds) and the second offering completed in August 2019 (US$33.8m proceeds). Bond-i was an implementation in the form of a smart contract (as the technical representation of the bond) on a private version of the Ethereum blockchain with a limited number of actors (financial institutions) involved. Although the issue volume was comparably small when considering the World Bank's standard bond issues, it constitutes an important signal to the market that the blockchain technology will play a significant role in financial markets going forward. In late 2019, South Korea's central bank reportedly initiated a proof-of-concept project to move bond transaction records to a blockchain-based record base available to several nodes operated by South Korea's regulatory authority, the Korea Fair Trade Commission, the Bank of Korea and other financial institutions. Another example is the €100m, one-year corporate note (Schuldschein) issued by Daimler through the German regional bank Landesbank Baden-Württemberg. Asset tokenisation seems to be particularly interesting for bonds issued as part of private placements in low volumes, which are normally illiquid/less liquid.

Real estate – well suited to tokenisation

Real estate investments represent another important emerging area where tokenisation may introduce liquidity and lower minimum investment requirements through fractional ownership. This is illustrated by a number of projects, with some of the most prominent outlined below:

- The tokenisation of a 12-unit luxury condo Manhattan property development for c US$30m on the Ethereum blockchain announced in the second half of 2018.
- In Germany, the B2B technology service provider Brickblock has tokenised a residential vehicle owning a property in Wiesbaden (worth c US$2m) in March 2019, which marked the first real estate share tokenisation in the EU.
- In July 2019, the blockchain company Fundament received the green light from the German watchdog (BaFin) to launch the offer of the first BaFin-approved real estate token (subordinated token-based bond on the public Ethereum blockchain) representing a German commercial real estate portfolio (offering a yield at 4% per year) with a volume of €250m.
- In October 2019, Fundament announced that Bauwens, a large German real estate developer and asset manager, became a strategic investor acquiring a 15% stake in the company. The

cooperation with Bauwens gives Fundament access to the former's extensive development pipeline at c €6.7bn, providing scope for further tokenisation projects.

- Liechtenstein's regulator has recently approved the first tokenised real estate fund.

Blockchain-powered solutions are also being introduced in residential real estate brokerage, as illustrated by the recently announced partnership between ShelterZoom (which runs a platform for buying and selling houses using blockchain) and Berkshire Hathaway HomeServices Professional Realty (a broker with more than US$1bn in annual sales).

Tokenisation of other assets

There are multiple other types of assets that may benefit from tokenisation, such as art, royalties, gaming items or carbon credits.

We asked **Yorke Rhodes, head of blockchain at Microsoft**, about his thoughts on what further assets classes are likely to be tokenised in the future:

> *I believe that loyalties are an interesting asset class for tokenisation, as they are opaque and easy to manipulate, and because tokenisation would make them more easily tradable. Other assets which could get tokenised quickly include game items, as well as travel and hotel points. There is also increased interest in alternative asset classes, such as carbon credits, which is a relatively opaque market with high risk of fraud. Blockchain adoption in this space should be driven by new regulation requiring companies not only to purchase carbon credits, but also produce green energy onsite and be able to prove its origin. An example of such a regulation is Local Law 97 in New York which should incentivise energy generation on real estate properties using rooftop solar/wind equipment. This kind of law should be implemented across other geographies really quickly. Another interesting opportunity are commodities (eg grains) which could be tokenised at the warehouse or in the field, which would dramatically change the commodity futures trading markets.*

Adoption: Slowly but surely

We believe that there will be a gradual transition to blockchain technology within the sector. The incumbent players, much in the same way as for other fintech developments, will need to start to adopt the technology or else slowly be outcompeted.

When we interviewed Patrick Lowry, **CEO and Managing Partner of Iconic Holding** (a provider of enterprise grade crypto investments and ventures), he gave us his view on how he expected to see the adoption of blockchain develop:

> *In my view, blockchain/crypto adoption will occur in two stages. The first will be marked by a growing number of implemented use cases and applications being facilitated by improvements to blockchain's scalability, proper business cases and seamless user experiences. This will attract people's attention and encourage them to engage with these solutions without ever having to know they are engaging with blockchain technology itself. This is similar to the adoption of the internet where people are not attracted by the HTML standard itself, but the possibilities provided by webpages and applications built on it. The second stage will be associated with crypto as an asset due to the growing importance of asset tokenization. I believe it is inevitable all equities, debts, derivatives and financial instruments, as well as tangible assets like real estate and even art, will be cryptographic assets on the blockchain. As a result, there will be a growing number of index products providing exposure to this asset class. In the future, the largest crypto asset fund managers, and even traditional fund managers, will be largely focussed on tokenized assets and financial instruments rather than just cryptocurrencies.*

Investments in blockchain/crypto businesses

Blockchain/crypto investments' development in recent years displays certain similarities to internet adoption, with the early stages marked by the dotcom bubble in the late 1990s when investors were attracted by a plethora of businesses of which only a limited number represented viable use cases to monetise, followed by a market crash and finally gradual adoption characterised by a more mature approach towards the technology. We believe that in the aftermath of the sobering cryptocurrency crash of early 2018, blockchain/crypto projects are gradually attracting investors with a more educated approach who appreciate the compelling use cases displayed by some of the products being currently developed and launched.

Investments in blockchain/crypto businesses by institutional investors are determined by the early stage of development of the whole sector. Consequently, the investment activity is characterised by relatively limited transaction values for now (compared to the broader VC/private equity market) and a skew towards early-stage funding, as seed/business angel financing made up c 65% of all deals in H119, according to CB Insights. A few larger, late-stage funding rounds have been closed in the last two years (see Exhibit 5). VC players active in the space may be divided into 'evangelist' funds specialising in blockchain/crypto investments (eg Digital Currency Group, Blockchain Capital and Pantera Capital) and those having a broader investment universe (although these often have a tech angle, eg Andreessen Horowitz, Union Square Ventures or Digital Horizon Capital). We believe the increased adoption of blockchain solutions and asset tokenisation will attract more institutional funding (including traditional players) to the sector in the coming years.

During the cryptocurrency/token boom and bust in 2017 and 2018, investments in blockchain projects were at first fuelled largely by so-called **ICOs,** which are issues of exchange or utility tokens (see below). At the peak of the cryptocurrency speculative wave in Q118, amounts raised through ICOs globally reached close to US$7.0bn, according to CB Insights (see Exhibit 6). Nevertheless, the sector gradually started attracting more traditional equity financing from VC funds, which, while lagging the ICO volumes, were significantly up at US$0.55bn in Q118 (reaching the level posted during the whole of 2016).

The most meaningful uptick in equity funding (mostly VC) occurred in subsequent quarters of 2018, with US$4.3bn raised in total that year. Meanwhile, ICO activity gradually faded on the back of deteriorating investor sentiment coupled with higher regulatory scrutiny and, as a result, VC funding surpassed ICOs starting in Q318. The pace of equity investments slowed markedly in 2019 compared to the prior year but was still above US$3.0bn invested (according to CB Insights data). Although the above estimates of funding levels vary depending on the data source provider, the overall trend and readthrough remain the same.

The approach of VC funds has matured, with the emphasis changing from companies focused on Bitcoin (and other exchange tokens) and private blockchain providers to secondary market trading and custody, cryptocurrency mining and asset tokenisation. Investments are increasingly directed towards companies developing specific marketable products and solutions rather than those having an exploratory and project-based focus. We also see continued growth in corporate VC activity with high-profile investors such as LSE or Microsoft. With respect to token offerings, there will be clear differentiation between exchange/utility token offerings through ICOs or the so-called IEOs (initial exchange offerings – a type of ICO combining issuing and listing of tokens in one step on a crypto exchange) and security token offerings (STOs).

We have asked **Patrick Lowry, CEO and Managing Partner of Iconic Holding** about his thoughts on how the blockchain/crypto investment market has evolved in recent years:

> *During the speculative wave of 2017-2018, many VC funds and large, private investors invested in the equity of blockchain/crypto projects and were allowed to acquire a certain amount of their utility tokens ahead of the ICO for free or at a price significantly below the ICO price.*

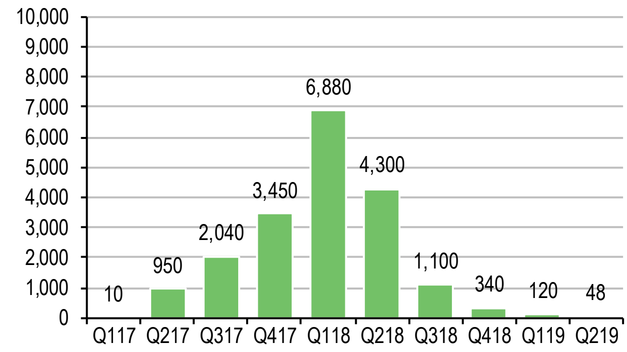
Subsequently, they liquidated their token positions in the market, taking advantage of the strong retail investor demand. The high market liquidity allowed them to perform exits within a short time span and consequently reduce the risk of a prolonged holding period while keeping the equity of the company itself. As a result, favourable token prices and high portfolio turnover translated into healthy returns for some at the expense of retail ICO investors. This was done at a time when crypto markets were immature, with no underwriting or comprehensive regulatory oversight, and the vast majority of projects behind the ICOs represented no real use cases with many being outright scams. The crypto investment market has since started to mature, with investors paying more attention to the viability of use cases behind utility tokens. Moreover, traditional equity issue as well as security token offerings have become more common funding options than ICOs. While VC interest has shifted to eg blockchain/crypto infrastructure (new protocols, exchanges, crypto mining, asset tokenization platforms etc.), prudent identification of quality investments remains critical given the higher number of projects seeking funding. For instance, there are quite a lot of crypto exchanges, but only a couple of them actually have a significant level of trading volume. Similarly, only a few of the projects around the protocol layer trying to raise capital currently represent compelling and innovative use cases.

Exhibit 5: Selected largest equity deals in the DLT/crypto sector in 2018–2019

Company	Business profile	Date	Deal value (US$m)	Deal type
Coinbase	Cryptocurrency exchange	October 2018	300	Series E
Ripple	Blockchain-based payments	December 2019	200	Series C
Blockchain Exchange Alliance	The parent company of the Bithumb cryptocurrency exchange	April 2019	200	Series A
Bakkt	Crypto exchange launched in 2018 by ICE, owner of NYSE	December 2018	183	Series A
Blocktower	Cryptoasset investment company	January 2018	140	Early stage VC
Basis*	Stablecoin developer	April 2018	133	Early stage VC
R3	Blockchain software company	May 2018	112	Series A
Circle	A Goldman Sachs-backed company behind the USDC stablecoin offering cross-border payments	May 2018	110	Series E
Figure	Blockchain-powered lending business	December 2019	103	Series C
SEBA Crypto	Crypto bank	September 2018	103	N/A
DFinity	A non-profit organisation developing a blockchain-based cloud computing project	August 2018	102	Early stage VC
Hedera Hashgraph	Public DLT platform	August 2018	101	Early stage VC
Kraken	Cryptocurrency exchange	February 2019	100	Series C
WeShare	Gift economy community group	September 2018	90	Series B

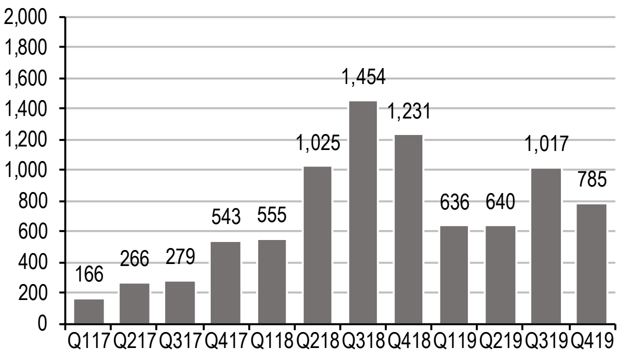
Source: Pitchbook, Crunchbase, Edison Investment Research. Note: We exclude the US$323m Series E funding concluded by Robinhood in 2019, as the company is not predominantly a blockchain/crypto play. *In December 2018, Basis announced it will discontinue its operations and return funds to investors due to regulatory concerns.

Exhibit 6: Blockchain funding – ICOs (in US$m)



Source: CB Insights

Exhibit 7: Blockchain equity funding (in US$m)



Source: CB Insights

Sector evolving to incorporate new asset class

The digital asset sector has been characterised by a high level of retail activity and a large number of digital asset start-up companies. Traditional financial services providers have been slower to enter the market but are now showing more signs of taking this new asset class seriously.

Digital asset-focused companies have tended to concentrate on one part of the market, such as cryptocurrency trading, cryptocurrency mining, security token issuance, smart contract design and digital asset fund management, and built their businesses accordingly.

VCEs adapting to appeal to institutional investors

The large VCEs started by trading the well-known cryptocurrencies such as Bitcoin and Ether and, as coins were issued in ICOs, started adding them to their exchanges. To demonstrate the size of this market, CoinMarketCap tracks trading from 314 VCEs, including fiat-crypto and crypto-crypto exchanges, trading 5,146 different assets with a total market cap of US$259bn. The approach by VCEs to regulation varies widely, with many basing themselves in countries that have little or no digital-asset regulation (eg Malta, British Virgin Islands). Others recognise that institutions have been deterred from investing in the sector because of poor security and uncertain regulations and are taking measures to address both issues. This includes establishing secure custodian operations for customers' assets (see page 33), implementing KYC/AML/CTF procedures and seeking licences to trade exchange and/or security tokens (eg Coinbase). In January 2020, Huobi launched a digital asset brokerage platform targeting institutions and high net worth individuals. In February 2020, BitGo acquired Harbor, a security token platform. Harbor has broker-dealer and transfer agent licences in the US.

Security token exchanges slowly coming to market

As the number of STOs to date is relatively small, there has not been much need for digital security exchanges (DSEs), as most secondary trading has been carried out on OTC exchanges. However, in anticipation of higher volumes of STOs, VCEs, traditional stock exchanges, banks and digital asset start-ups are starting to build DSEs and seek licences for them. The Swiss exchange SIX has developed a prototype of the Swiss Digital Exchange (SDX) for digital security trading, with full launch expected in Q420. The London Stock Exchange has trialled security token issuance – the fintech company 20/30 raised £3m through the STO, which was settled through the LSE's Turquoise equity trading platform.

We note that for an STO to be successful, the issuer needs access to potential investors – this is an area where the traditional financial institutions are at an advantage as they have an existing customer base. It is possible that we will see partnerships between traditional players and STO platforms to bring together investors and security token issuance expertise.

Digital asset fund management an emerging area

Asset managers have developed funds to give investors access to digital assets without investing directly, either by investing in single asset-specific funds (eg Grayscale Bitcoin Trust, which is traded on the OTCQX market in the US and has assets under management of more than US$2bn) or funds that contain a basket of digital assets (such as the Galaxy Crypto Index Fund, which contains a weighted portfolio of six cryptoassets, or the Iconic Funds' Crypto Asset Index Fund, which tracks the top 20 cryptoassets). With experience gained from launching its own index fund, Iconic Holdings has also launched Asset Management-as-a-Service (AMaaS), a platform for crypto asset managers to launch their own regulated crypto funds. Research from PwC and Elwood Asset Management in 2019 estimated that there were c 150 digital asset-based hedge funds with c US$1bn in assets under management.

Full-service digital asset banking

Others have taken the approach that for institutional investors to recognise digital assets as a legitimate asset class, the services provided by a traditional investment bank need to be replicated for digital assets. This would include offering the following services, all licensed by the relevant regulators:

- exchanges to trade the different types of tokens: exchange, utility, security;
- issuance of security tokens;
- broker-dealers for security tokens;
- custodian services; and
- digital asset management.

Companies following this path include:

- **Sygnum:** a digital asset bank based jointly in Switzerland and Singapore, with a Swiss banking licence and CMS licence in Singapore (for asset management). Services offered include custody (in partnership with Swisscom), brokerage, tokenisation (primary issuance platform), asset management, credit and B2B banking. Sygnum is working in partnership with Swisscom and Deutsche Börse to build a Swiss digital asset exchange.
- **SEBA:** also has a Swiss banking and securities dealer licence. SEBA offers custody, trading and liquidity, transaction banking, tokenisation and digital asset management. SEBA recently announced a partnership with Julius Baer.
- **Bakkt:** developed by the International Currency Exchange (ICE), the US-based owner of exchanges for financial and commodity markets that acquired NYSE in 2012. Bakkt initially offered Bitcoin futures (authorised by the Commodities Futures Trading Commission, CFTC) and has since added Bitcoin options and Bitcoin custody to its service offerings. It is developing a payments service that will enable merchants to accept cryptocurrency payments.
- **Diginex:** is developing a range of services for institutions including a VCE (seeking licences in Jersey and Singapore), a DSE (also seeking licences in Jersey and Singapore), trading, asset management (authorised in Jersey and Hong Kong), custody (currently seeking licences/registration in the UK and Jersey and soon to apply in Singapore) and a solutions business to help companies build their own DLT-based services.

Richard Byworth, CEO of Diginex, explained the rationale behind the company's entry into this market:

> *Diginex was founded to deliver a regulated and white hat approach to the digital asset opportunity. A partner to financial services firms from banking to asset managers, pension firms to private banks, allowing them to access this brand new asset class. By focusing on robust KYC and AML processes and hiring a top calibre team with a track record for execution in the Technology and Financial space, we have been able to consistently deliver highest quality product. Our Solutions business levers blockchain networks to deliver enterprise technology, supporting a Capital Markets business that originates, advises on and distributes securities that use blockchain networks as the delivery mechanism for digital securities. Our exchange platform will cater to both these new digital securities as well as virtual currencies and their derivatives. As well as exchange, the Diginex Markets business also comprises trading and cybersecurity industry certified custody to support the full range of digital assets. Our regulated Asset Management capability then completes the platform by creating the fiduciary shield required to deliver an on-ramp for larger capital allocations into the digital asset ecosystem.*

Expect partnerships and M&A

We are already seeing a number of traditional financial institutions starting to enter the market, in many cases in partnership with digital asset specialists. Fidelity has created a new business, Fidelity Digital Assets, which offers Bitcoin custody and trade and settlement services. Nomura has partnered with Ledger and Global Advisors Partners to provide digital asset custody services. State

Street, one of the largest US custodians, has partnered with Gemini to offer digital asset custody. Vontobel offers a white-label custody service to its private wealth manager customer base. Over time, we expect to see the incumbents extend their full range of services to encompass the digital asset class. As well as partnerships, we see acquisitions as a route to gaining access to digital asset expertise and, in some cases, regulated businesses.

Barriers to adoption

Although the cryptocurrency market has shown rapid growth since Satoshi Nakamoto first introduced the concept of Bitcoin in 2008, growing to a market cap of US$259bn across 5,146 cryptocurrencies (source: CoinMarketCap, February 2020), it has been predominantly a retail-based phenomenon. At the same time, the security token market is relatively nascent, with the necessary infrastructure and regulation still a work in progress.

A variety of factors have discouraged institutional investors from investing in digital assets.

- **Regulatory uncertainty:** high-profile issues such as failed ICOs and the use of cryptocurrency by criminals have attracted the attention of regulators. Regulation is dealt with on a country-by-country basis and is therefore progressing at different speeds in different countries. Regulation is being refined to cover issuance of and trading of digital assets, AML/KYC/CTF regimes, data protection and security, legal recognition of smart contracts, legal definition of crypto assets, clarity on settlement finality, taxation of digital assets, accounting for digital assets and how to deal with digital assets in the event of insolvency.
- **Blockchain scalability:** processing speed is affected by the fact that all nodes need to process all transactions; slowing speed is one of the reasons for forks; blockchains can be power hungry, depending on the technology used.
- **Security issues:** there have been many high-profile thefts of cryptocurrencies, whether as a result of poorly secured assets or other IT-related security issues such as code vulnerabilities.
- **Volatile pricing of cryptocurrencies**: this makes it difficult to invest in or use as a store of value.
- **High failure rate for ICOs:** this has tarnished the reputation of digital assets and reduced trust in the technology.
- **Fragmented technology:** there are many different blockchains in operation, using different standards. Companies need to develop methods to interoperate between blockchains as well as with existing technology.
- **Lack of understanding:** DLT technology and its applications can be complex and difficult to understand, particularly as the space is developing so quickly. Additionally, there is a shortage of staff with the appropriate knowledge and experience to exploit DLT technology commercially.

In the remainder of the report, we explore the current status of the market and what action is being taken to overcome the barriers listed above.

Regulation constantly evolving

The lack of regulatory certainty in a number of different areas has made it difficult for institutional investors to justify investing in the sector. The attention of regulators is now turning to this space and starting to provide clarity on how digital assets will be treated from a legal standpoint.

The level of regulation of digital assets varies widely from country to country. Some countries have decided to make most crypto-related activities illegal, with the aim of protecting consumers and ensuring that control of currency remains with the central bank (eg China, Pakistan, Qatar). Others believe DLT is here to stay and want to enable their economies to exploit the commercial benefits while protecting consumers and investors. Several countries have led the way with regulation that aims to strike a balance between innovation and consumer protection. We discuss below the approach these countries are taking and highlight the key areas that need to be considered.

Regulators fitting digital assets into existing frameworks

Regulators are deciding whether to develop new regulatory frameworks for digital assets or make use of existing regulations. We see the majority of regulatory authorities fitting digital assets into their existing regulatory frameworks, with treatment depending on the asset category each digital asset fits into. France is an exception, with its new digital asset laws passed in April 2019.

Digital asset companies come under the remit of a number of different regulators. The main entities providing guidance at a regional or global level include:

- **Financial Action Task Force (FATF)** is an inter-governmental body established in 1989 by the ministers of its member jurisdictions. The FATF's objectives are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is a policy-making body that works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. The FATF has 39 members: 37 member jurisdictions and two regional organisations. Members include 15 EU countries (including France, Germany and the UK), Argentina, Australia, Brazil, Canada, China, Hong Kong, Japan, Singapore, South Korea, Switzerland and the US.[2]
- **Global Digital Finance (GDF)** is an industry membership body that promotes adopting best practices for digital assets and digital finance technologies, through the development of conduct standards, in a shared engagement forum with market participants, policymakers and regulators.
- **EU:** the fifth anti-money laundering directive (5MLD) came into force on 10 January 2020. In particular, it states: 'Member states shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers are registered' and will thus be subject to the AML/CTF requirements of 5MLD.

Ideally national regulators should take account of the guidance of the FATF and, in the EU, must incorporate any relevant EU-wide rulings into national law. The level of regulation varies from country to country and by activity. Activities that regulators are considering include:

- running a cryptocurrency exchange;
- running a digital securities exchange;
- issuing/distributing security tokens;
- asset management; and
- providing secure custody for digital assets.

First step – classify the asset

As a first step, regulators are defining how they view different types of digital asset. We see digital assets as broadly falling into one of three categories:

- exchange token;
- security token; or
- utility token

The ICO boom and bust resulted in many investors losing money, as many coin issuers did not use the issue proceeds as originally promised and, in some cases, businesses folded. As a result, regulators are keen to ensure that if token issues are effectively the equivalent of an IPO of a security (equity or debt) then potential investors have access to all the necessary information before investing (equivalent to a prospectus) and the token issuers fulfil a set of requirements. The SEC is taking action against a number of companies that undertook ICOs over the last few years (including

[2] See here for full list: FATF Members and Observers

Telegram),[3] as it believes they were effectively issuing securities and therefore should have followed securities laws.

Regulators will examine a token to ascertain whether it is a security token or a utility token – see page 10 for further detail on the characteristics of each type of token. Broadly, characteristics that would point to it being a security token include that it:

- can be transferred;
- can be traded; and
- gives the holder rights akin to traditional securities, such as shareholder rights or creditor claims.

In general, once a regulator has decided a token is a security token, it will fall under the same regulatory regime as a traditional security. Below we discuss the regulatory treatment of assets that fall into the exchange token and utility token categories, on a national basis. VCEs were unregulated until fairly recently. Now many countries are putting licensing regimes in place for VCEs, partly due to more onerous AML/CTF requirements enacted by the EU and recommended by the FATF.

Regulators are still to decide how to categorise and regulate stablecoins.

In many countries, the lack of regulation of digital assets has left banks and payment processors unwilling to provide services to crypto-based businesses. One benefit of regulation is that banks are more confident that AML/KYC checks are being performed and are more able to justify working with businesses involved in trading digital assets.

Country-by-country analysis

We now look at several different countries that have a permissive approach to digital assets and briefly discuss their approach to and treatment of digital assets.

France – PACTE Act specifically addresses utility and exchange tokens

In April 2019, the French government enacted the PACTE Act. Within this, it provided a framework for the regulation of utility and exchange tokens (security tokens are covered by existing securities laws). The act covers ICO issuers that obtained the optimal approval of the Autorité des marchés financiers (AMF); digital asset custodians and entities allowing the purchase or sale of digital assets against legal currency; and digital asset services providers.

The AMF encourages ICO issuers to seek a 'visa' from the AMF, which requires compliance with the PACTE Act, but this is voluntary. However, those that do not have a visa will have restrictions placed on the marketing of their offerings. In addition, any of the entities covered by the list above who are registered with the AMF should be able to get access to banking services (many French banks have declined to service digital asset businesses).

Under 5MLD, VCEs and custodians will need to be registered with the AMF. Exchanges offering crypto to fiat conversions will also require a payment services licence from the Autorité de contrôle prudentiel et de resolution (ACPR).

Germany – BaFin requires authorisation

In July 2019, BaFin updated its regulations to reflect 5MLD. As part of this, it announced that cryptocurrency-related businesses would need to obtain a licence from BaFin by the end of 2019. In November 2019, BaFin amended the law to allow banks to sell and store cryptocurrencies. Any custodian of digital assets must obtain a licence from BaFin by the end of 2020 and make BaFin aware of the intent to offer digital asset custody services by the end of March 2020. According to

[3] SEC Halts Alleged $1.7bn Unregistered Digital Token Offering, October 2019

press reports, c 40 banks have approached BaFin expressing an interest in providing digital asset custody.

Security token issuance also requires authorisation by BaFin, and a number of STOs have already been authorised.

Hong Kong – opt-in for VCEs if they offer security tokens

The Hong Kong Monetary Authority and the Securities and Futures Commission (SFC) view cryptocurrencies as virtual commodities that are not subject to regulation if they do not have the characteristics of a security. If a VCE offers the ability to convert fiat to crypto, then it will be covered by AML/CTF regulations. In November 2019, the SFC announced new rules to allow exchanges to become licensed. These rules only apply to exchanges that support the trading of security tokens. To be licensed, an exchange can only offer services to professional investors, must have an insurance policy to protect clients' assets and must use an external market surveillance mechanism. A VCE will not need a licence if it does not trade tokens that are deemed to be securities. As the rules are so recent, we are not aware of any licensed exchanges, although it has been reported that OSL (part of HK-listed BC Group) is the first exchange to apply for a licence.

In 2018, the SFC announced a framework that would allow asset managers investing in digital assets and selling products in Hong Kong to obtain a licence from the SFC.

Japan – early to regulate

Japan was quicker to regulate this market than other countries, partly due to the issues surrounding the collapse of the Mt.Gox exchange in 2014. Since April 2017, VCEs have been regulated by the Payment Services Act (PSA) and required to register with the Financial Services Agency (FSA). After the high-profile hack of Coincheck in 2018 (coins worth c US$530m were stolen), additional legislation was passed to tighten up regulation. In May 2019, the government passed revisions to the PSA, which clarified the law regarding VCEs and custodians – these will come into force in April 2020. Both VCEs and custodians must be registered with the FSA and will need to meet stricter requirements. Many of the large exchanges have chosen not to seek a licence and do not service customers in Japan. Examples of such exchanges include HitBTC and Kraken. Binance recently announced it would withdraw from this market (without specifying the timeline), but separately suggested it was working with Z Corporation (previously Yahoo! Japan) and TaoTao (a licensed VCE) with a view to partnering in Japan to meet all regulatory requirements. We understand there are 21 licensed exchanges, with others still awaiting approval by the FSA (including Coinbase).

Jersey – keen to welcome crypto businesses

In Jersey, a VCE is a supervised business that needs to be registered with the Jersey Financial Services Commission (JFSC) and meet all relevant AML/CFT regulations. To encourage innovation, the JFSC has created a regulatory sandbox whereby any VCE with a turnover of less than £150,000 per calendar year can test delivery mechanisms in a live environment without paying registration fees (they must still register with the JFSC and comply will all relevant AML requirements). We are aware of only a few licensed VCEs: Binance and Criptyque, while Diginex's application is in process.

Custodian businesses will need to be regulated for 'trust company business' under the Financial Services (Jersey) Law 1998 (FSJL). Nomura's crypto custody business, Komainu Digital, was recently licensed by the JFSC.

Before a security token can be issued, it requires consent by the JFSC under the Control of Borrowing (Jersey) Order 1958. A security token exchange is regulated as an investment business (IB) under the FSJL and will require an IB licence.

Singapore – open, but tightening up regulation

In January 2019, Singapore passed the Payment Services Act bringing cryptocurrency dealing or exchange services under the supervision of the Monetary Authority of Singapore (MAS) – it came into effect on 28 January 2020. Any entity that provides any type of payment service, including 'digital payment token service', requires a licence. In addition, licensees will be subject to AML/CTF requirements. Binance has applied and Japan-based Liquid and UK-based Luno are planning to apply for a licence.

The exchange of any token constituting a capital markets product would be regulated under the Securities and Futures Act and would need approval by the MAS.

Custody of exchange tokens is not regulated, but the MAS is currently consulting on whether to bring them under the same regime as VCEs. Custody of security tokens requires a capital markets services licence (CMSL). We are aware of one licensed company, Propine.

Switzerland – an active market

The Swiss regulator FINMA does not view exchange or utility tokens as securities, so they do not fall under the scope of regulation. Security tokens are considered on a case-by-case and fall under the same regulations as traditional securities. VCEs and custody providers for exchange tokens are covered by AML regulations and required to join a self-regulatory organisation. According to FINMA, some trading activities with virtual currencies require a banking licence – this is generally the case when an organisation accepts money on a commercial basis from clients and keeps it in its own accounts; it also applies to providers who lodge virtual currency holdings from customers in 'wallets' and manage accounts for them. However, FINMA's current position is that no banking licence is required if virtual currency holdings are transferred for secure safekeeping only and if these virtual currency units are stored separately on the blockchain for each customer and each deposit can be attributed to an individual customer at all times.

The Swiss exchange SIX has launched a prototype digital securities exchange, SDX. Full launch is expected later this year.

The Swiss Capital Markets and Technology Association (CMTA) has established an ERC-20 compatible token called 'CMTA20', which is a Solidity smart contract for the Ethereum platform. It has the functionality required to implement the tokenisation model for equity securities of Swiss corporations in accordance with CMTA's blueprint. The blueprint describes the process through which shares that have already been issued according to Swiss law can be 'wrapped' into digital tokens, so the tokens and the underlying shares are tied to each other in a manner that prevents the share from being transferred without the corresponding tokens and vice versa.

UK – FCA recently clarified guidance

Since 10 January 2020, businesses including digital asset exchange providers, digital asset ATMs, custodian wallet providers, peer-to-peer providers, issuers of new digital assets and publishers of open source software have been required to register with the FCA and meet AML/CFT requirements as per 5MLD.

Derivatives that feature digital assets as the underlying investment fall under the FCA's regulatory remit, as will security tokens.

US – multiple regulators to consider, no coherent framework

The Financial Crimes Enforcement Network (FinCEN) considers VCEs to be money service businesses, which are subject to existing banking regulations such as AML, KYC and financial reporting requirements. The treasury secretary recently confirmed that FinCEN would soon be issuing new requirements for cryptocurrencies.

Certain digital assets deemed to be commodities by the CFTC, typically derivatives with a digital asset as the underlying, are subject to the same regulations as physical assets in this class.

Crypto businesses require state money transmitter licences. More specifically, any entity running a crypto business in the state of New York or servicing New York residents must apply for a BitLicense (this includes any company that transmits, controls, administers, exchanges or maintains custody of virtual currencies on behalf of others).

Security tokens fall under the remit of the SEC. DSEs require an alternative trading systems licence.

Under the Investment Advisers Act of 1940, any institution holding customer assets worth more than US$150m is required to use a qualified custodian. Custodians usually seek approval from one state licensing authority and passport this to other states. New York and South Dakota are the most common states in which custodians seek licences.

Implementing KYC for digital assets

Regulators are imposing stricter requirements for KYC/AML/CTF compliance, with 5MLD a key example and the FATF recently introducing the ‘travel rule’ (any firm facilitating a crypto transfer needs to disclose information on the customer). As the popularity of blockchain to a certain extent is due to the anonymity afforded to participants, the threat of 5MLD has prompted several European VCEs to shut down, some permanently and others transferring their businesses to unregulated countries such as Panama. Although the introduction of stricter KYC checks on exchange users and token investors will deter some, in the longer run it should reduce the volume of cryptocurrency involved in illegal activity and make the sector more appealing to institutional investors.

Full compliance with KYC requirements is not straightforward

Introducing KYC/AML/CTF checks on digital asset investors is not straightforward. Although it is possible to obtain KYC information on a new customer of an exchange by asking them to provide traditional identity information such as a passport or driver’s licence, it is much harder to determine the source of a customer’s digital assets as counterparties are identified by cryptographic addresses rather than by name or account number. Several of the larger exchanges have carried out significant amounts of work to identify who is behind a large percentage of addresses. Third-party data providers such as Chainalysis, CipherTrace and Elliptic analyse and determine the provenance of customers’ digital assets (as these data are contained within the encrypted blocks).

The use of **tumblers** by some investors makes it even harder to track the history of transactions. Tumblers are services offered to digital asset holders to anonymise their assets. The customer sends their assets to the mixing service – there the assets are added to a pool and replacement assets to the same value are transferred to the customer. This breaks the link to the customer’s identity. Tumbler services are not well regarded by the authorities due to their obvious links to money laundering and in Europe, several have been closed down by Europol or chosen to shut up shop over the last year.

A category of coins, dubbed **privacy coins**, was developed to deliberately maintain the coin owner’s anonymity. These coins include Monero, Dash and Zcash. With the imminent application of the travel rule, many of the larger exchanges, such as OKEx and Upbit, announced their intention to delist privacy coins causing a significant decline in the value of the coins. The level of privacy offered by each coin differs (Monero provides privacy by default, whereas Zcash offers various privacy options) and some coins are able to satisfy KYC/AML concerns by enabling owners to disclose the necessary information to selected parties (for example, Zcash’s viewing keys).

As part of the KYC/AML/CTF process, exchanges will also need to put transaction monitoring in place to detect suspicious behaviour. Providing and implementing a comprehensive KYC/AML/CTF process adds a material overhead to exchanges and, in our view, will be a key competitive differentiator for attracting institutional investors.

Governments grappling with taxation of digital assets

Tax authorities are addressing the issue of how digital assets should be taxed, although the amount of guidance available and the treatment differs widely from country to country.

For those countries that are not low tax/offshore jurisdictions, in the case of **exchange tokens**, typically for individuals, capital gains tax is payable on profits made when tokens are converted to fiat currency. For businesses and individuals whose business is trading exchange tokens, profits will be taxable as income. VAT is generally payable when tokens are used to acquire other goods or services. The taxation of **security tokens** is likely to be treated in the same way as traditional securities.

Other areas requiring legal or regulatory certainty

The use of digital assets has implications in other areas of business. For example, there is little clarity on how digital assets are treated in the case of company **insolvency**, either in the case of a company whose business is trading in digital assets (such as defunct exchange Mt.Gox) or for a business that held digital assets as an investment. Are the assets part of the estate? Do creditors have rights over any of the digital assets? How would the assets be distributed to creditors (particularly if the debtor cannot or will not hand over the private keys)? National courts are dealing with these issues case by case and there are no clear answers yet.

Similarly the use of **smart contracts** is untested in law. The nature of such contracts (automatic execution, no ability to reverse) raises issues such as:

- What happens if parties want to terminate or amend the contracts?
- How does the fixed nature of the contract allow flexibility in business dealings between parties, for example in managing late payments?
- What happens if there are errors in the coding of the contract, or the contract is hacked?
- Does the smart contract developer have liability?
- What happens if payment enforced by the contract fails?

In the UK, a company called The Proof of Trust is seeking to address these issues and recently filed to list on the LSE. The Proof of Trust is a digital protocol powered by distributed consensus, designed to manage arbitration or dispute resolution for smart contracts.

To appeal to the mainstream, investors need to be sure their legal rights can be protected when they trade in digital assets and use smart contracts. To this end, in November 2019, the UK Jurisdiction Taskforce of the Lawtech Delivery Panel set out the recognition of digital assets as tradable property and smart contracts as enforceable agreements under English Law.[4] However, this does not address the issue of **governing law and jurisdiction**. Where it has been agreed that digital assets or smart contracts fall under the jurisdiction of English law, this provides clarity. However, it does not provide guidance on how to determine the jurisdiction that should be applied.

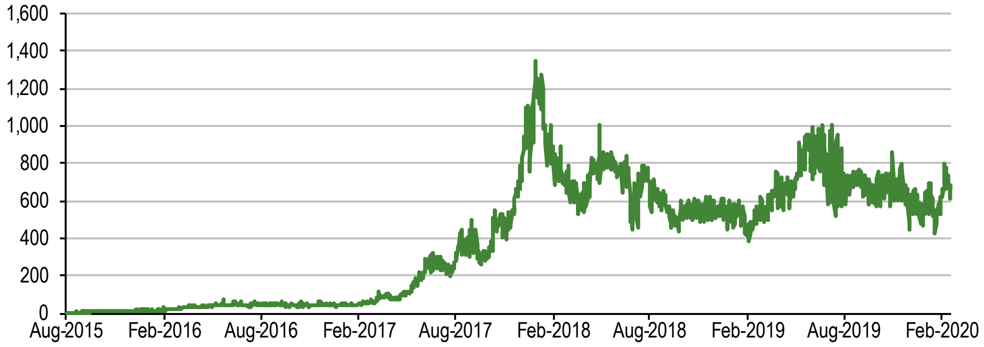
Improving scalability

As blockchain technology and digital assets have started to move towards the mainstream, certain scalability issues associated with processing speeds have become apparent. This is because current blockchains predominantly apply a linear execution model, where every node (ie computer participating in the network and adding blocks) is validating every single transaction. Consequently, the more computers that join the peer-to-peer network, the lower the efficiency of the whole

[4] Legal Statement on Digital assets and Smart Contracts, November 2019

environment, especially when compared to traditional payment systems such as Visa (which may handle around 1,700TPS compared to 7TPS in the case of Bitcoin or 15–20TPS in the case of Ethereum). However, there are several potential solutions to the blockchain scalability problem being explored at present (see below).

Exhibit 8: Ethereum transactions per day ('000s)



Source: Etherscan.io

Changes to consensus protocol

Firstly, the implementation of alternative consensus algorithms that allow for more scalability may help increase the efficiency of a blockchain network. An example would be the move from PoW to a PoS algorithm, especially using the Byzantine fault tolerant framework (or at least including some of its elements, like in the case of Casper). However, at least for now the search for an optimal solution based exclusively on the main blockchain (the so-called ‘layer 1’ solutions) is somehow limited by the trade-off between security, scalability and decentralisation. Ripple’s XRP for instance offers a much higher TPS in comparison to Bitcoin and Ethereum, but its decentralisation is often disputed given Ripple’s alleged high influence on the network and pre-mined XRP supply. EOS with its DPoS protocol is characterised by higher centralisation as measured by the number of nodes validating new blocks. There is however one promising ‘layer 1’ approach called sharding.

Sharding

This is a method originally applied to databases to perform horizontal partitioning (breakup). It can be used to spread out the computational, communicational and storage workload in a blockchain network in that each node validating blocks is responsible only for a given shard (rather than involved in processing transactions in the whole network). Theoretically, there is no limit to the number of shards, providing a high degree of scalability. As information may be freely exchanged between nodes while hashes from the respective shards are being recorded on the mainchain, the whole blockchain network remains decentralised and secure.

Having said that, the safety of the system needs to be facilitated through solutions guarding it against **shard takeover**, which would lead to a permanent loss of the corresponding data portion. Ethereum, which is currently exploring the implementation of sharding on top of the shift to PoS, is examining a way to address this issue through continuous random reassignment of nodes to the respective shards. In that way, a potential attacker would not be able to gauge which shard they would get access to through the node they intend to take over.

Another potential problem with sharding involves **thin clients**, ie computers that do not fully validate blocks in the given network and normally rely on the Simplified Payment Validation (SPV) method to verify if a given transaction is already on the blockchain. It is important to ensure that these nodes have a complete picture of the current state of the blockchain. This may be done by allowing them to communicate through separate networks and maintain local state copies for each shard.

Layer 2 (off-chain) solutions

An alternative to the above approaches represent solutions utilising 'Layer 2', which means a secondary framework set up on top of the blockchain (referred to as 'Layer 1') and often developed to solve the scalability issue in a given application, eg scaling payments, smart contracts or off-chain computation. Two important types of layer 2 solutions are:

- **State channels** – facilitating fast transactions between nodes through a dedicated channel outside of the blockchain. This enables the execution of multiple transactions, which are recorded as a single transaction on the blockchain once the channel is closed. However, this solution does not benefit from the level of security a decentralised network offers and is thus more likely to be used for relatively small transactions, while large deals will still be executed on the main blockchain. An example of a state channel is the Lightning Network payment protocol on the Bitcoin network.
- **Sidechains** – represent blockchains that are connected to the main chain and which are set up for handling a specific task. Block validation occurs within a given sidechain, ie each node is only responsible for transactions in the sidechain it is assigned to. A specific example of a sidechain framework is Ethereum's Plasma, which represents a tree of blockchains, where each of the sidechains may have its own sidechains (or 'child' chains as they are sometimes called). Each of the child chains is a customisable smart contract. A distinct feature of the Plasma solution (compared to other sidechain concepts) is that it allows users to exit the Plasma chain and prevent a potential attacker from inflicting permanent damage in case of detected flaws.

Improving interoperability

Blockchains are designed to operate on a stand-alone basis. This means that all of the blockchains that have been developed for digital assets operate as a series of unconnected systems, operating alongside but independently of each other. As blockchain technology is adopted across more industries, there is an increasing requirement for blockchains to interact with each other, as well as with traditional off-chain systems. This has driven the development of a number of different technologies to improve interoperability:

- **Cosmos** describes itself as a decentralised network of independent parallel blockchains, each powered by Byzantine fault tolerant consensus algorithms such as Tendermint consensus. It is an ecosystem of blockchains that can scale and interoperate with each other. Its inter-blockchain communication (IBC) protocol allows interoperability between Tendermint-based blockchains. For blockchains not compatible with IBC, Cosmos has created a 'Peg zone' to connect blockchains.
- **Chainlink** connects smart contracts to the required inputs and outputs. It enables data to be retrieved from off-chain APIs and put on the blockchain. Chainlink describes its technology as a decentralised oracle network and it works with SWIFT.
- **Polkadot** has a vision to create a completely decentralised web where users retain complete control over their data and identities. The Polkadot network protocol allows arbitrary data, not just tokens, to be transferred across blockchains. This opens up the possibility for cross-chain registries and computation. Polkadot can transfer data across public blockchains as well as private, permissioned blockchains. It gives the example where a school's private, permissioned academic records blockchain could send a proof to a degree-verification smart contract on a public blockchain. The network is made up of parachains (parallel blockchains that process transactions and transfer them to the original blockchain), a relay chain (central component connecting parachains) and bridges (connecting Polkadot to external blockchains).
- **Quant** has developed Overledger, which it calls the world's first blockchain operating system, to allow blockchains to connect with each other and existing networks.

Improving security

The sector has suffered from numerous high-profile hacks and frauds. In the first nine months of 2019, CipherTrace estimates that coins worth US$4.4bn were stolen. Although blockchain is touted as a secure way of transacting because transactions are immutable and publicly available to all node participants, many cryptocurrency exchanges have lost customer assets and in some cases have filed for bankruptcy as a result (Mt.Gox in 2014, Youbit in 2017, Cryptopia in 2019). This has sometimes been because insiders or third parties have been able to steal poorly secured cryptocurrency or because vulnerabilities in the blockchain software code mean exchanges do not have an accurate picture of what they hold. Often, exchanges have not had adequate financial and operational controls in place.

Every blockchain transaction has to be signed with the private key for it to be legitimate. When stealing assets, thieves are getting unauthorised access to the owner's private key, so anyone with access to the private key is able to control the assets linked to it.

QuadrigaCX highlights the risk

In one recent case, the founder of the Canadian exchange QuadrigaCX allegedly died. He had supposedly transferred the majority of the exchange's Bitcoin to cold storage for which he was the only person who knew the password. Consequently, on his death, no-one else was able to access these wallets. Investigation by Ernst & Young showed that months earlier he had in fact transferred most of the coins out of cold storage to other exchanges where he was trading on his own account and using the coins as security for a margin trading account. This case highlights several issues: the risk of losing access to digital assets in cold storage, the lack of financial and operational controls (eg segregation of roles, segregation of assets, transaction reporting and analysis, third party processor oversight) and lack of business continuity planning.

Of the exchanges that have suffered losses over the last eight years or so, the most common reason cited is that the exchange was 'hacked' – often via phishing and/or malware attacks on employees or customers, or by a disgruntled employee. In reality, it is likely that many of the losses can be put down to exit scams, where the exchange owners steal the assets themselves. We have pulled together some real-life examples of causes of digital asset loss, which highlight that in addition to internal fraud, traditional cybersecurity risks need to be considered when setting up and running a VCE.

Exhibit 9: A sample of causes of digital asset losses

Errors	Fraud	Hacking
Software programming error	Insider theft	Getting control of administrator accounts
Wallet destruction during server reboot	Identity theft and SIM takeover (to exploit two factor authentication)	Malware sent to exchange employees combined with social engineering
Loss of hardware device holding private key	Coins stolen by secret service agent investigating exchange	Phishing attacks on wallet holders

Source: Edison Investment Research

Other risks that need to be considered include:

- **Consensus hijack (or 51% attack)**. Where more than 50% of mining power (hash rate) is controlled by one entity, this entity has the power to mount what is known as a 51% attack. This could enable the attacker to double spend coins. For Bitcoin, the cost of acquiring more than 50% of the hash rate would be prohibitive but it could be possible for smaller blockchains.[5]
- **Distributed denial of service** attacks on nodes in the form of fraudulent transactions. While this is unlikely to result in losses, it could reduce transaction processing speeds.
- **Smart contracts.** Incorrect mapping of business processes into smart contract logic would result in the contracts not performing as expected.

[5] Ethereum Classic was the victim of a 51% attack in January 2019, resulting in estimated losses of US$1.1m.

We now look at the areas that need to be addressed to provide improved security for both institutional and retail investors.

Providing secure digital asset custody operations

Digital assets (ie the private key) can be stored on a user's own device, at an exchange or with a dedicated digital asset custodian. Digital assets are typically stored in hot storage, which is connected to the internet, or cold storage, which involves storing the private key on an isolated hardware device. Assets stored in hot storage are immediately available to trade with, whereas it takes time to retrieve assets from cold storage. For maximum security cold storage makes sense, but for maximum liquidity, hot storage is better. Investors want both security and liquidity for their assets, so the ability to quickly and securely move assets back and forth between hot and cold storage is crucial.

Exchanges are a tempting target for hackers

When a customer transfers their assets to an exchange, they are added to the exchange's pool of assets. The customer's ownership is registered in their own sub-account but any transactions carried out on the exchange are off-chain (ie ledger entries between sub-accounts). Only when the customer withdraws assets are the transactions recorded on-chain. The pool of assets held by exchanges is therefore an attractive target for hackers or unscrupulous exchange owners or employees. The large exchanges keep at least 95% of customer digital assets in cold storage, with the remainder in hot storage to maintain liquidity.

As a result of the large number of asset thefts from exchanges, secure digital asset custody services are emerging, many with a focus on the future institutional market. These can be standalone companies or part of cryptocurrency exchanges. Traditional custodians such as banks are also entering the market. Several of the larger exchanges have acquired specialist crypto custodians, such as Coinbase's acquisition of Xapo's institutional business in August 2019 for US$55m.

We discuss below the key features of each type of storage in more detail, the technology being developed to improve security and liquidity and the main market players focused on the institutional market.

Cold storage exploits high-value physical asset security techniques

In its most basic form, cold storage involves an asset owner's private key being stored on a hardware device isolated from the internet. This can be as simple as writing the code on a piece of paper and locking it away, but more commonly involves the use of a USB-type device. For the retail market, hardware wallets have been specifically developed for cold storage by companies such as Ledger (www.ledger.com) and Trezor (www.trezor.io). For the institutional market, hardware security modules (HSMs) are used – these are physical computing devices that safeguard and manage digital keys.

Hardware wallets usually offer the ability to **back up** the assets with a 'recovery seed'. If the wallet is lost, stolen or damaged, the recovery seed can be used to restore access to the assets. The recovery seed is essentially the private key translated into a series of words (12–24 words long). The asset owner needs to keep this safe offline (in much the same way they have to secure the private key) but it can be useful way to access assets for either the asset owner or the asset owner's estate. It does raise the issue of an endless loop of security – securing the various copies of the recovery seed too. Another back-up tool is the Shamir Secret Sharing Scheme. This takes the secret (ie the private key) and divides it into x parts. The user distributes the parts to other people or devices. When the key needs to be recovered, it needs x-1 parts recombined to get access to the secret.

While individuals usually store their hardware wallets at home, institutional investors need a secure venue for their cold storage. To provide additional security, custodians store the HSMs in much the same way as high-value physical assets such as artwork or gold bullion, locking the HSMs in safes or vaults that have high levels of security (eg biometric ID, armed guards, CCTV) and protection against fire, flooding or power outages. Again, as with high-value physical assets, custodians are putting in place insurance, with companies such as Aon, Lloyds of London and MunichRe active in the space.

Custodians typically use HSMs that are certified to **FIPS[6] 140-2 Level 2 or 3**. FIPS 140-2 is the benchmark for validating the effectiveness of cryptographic hardware. Level 1 requires production-grade equipment and externally tested algorithms. Level 2 adds requirements for physical tamper-evidence and role-based authentication. Software implementations must run on an operating system approved to Common Criteria[7] at EAL2.[8] Level 3 adds requirements for physical tamper resistance and identity-based authentication. There must also be physical or logical separation between the interfaces by which 'critical security parameters' enter and leave the module. Private keys can only enter or leave in encrypted form.

Cold storage typically combines high physical security to protect HSMs, backups in different physical locations, and processes to ensure that only legitimate customer orders are processed.

Those keeping assets in cold storage need to be aware of the time it takes to undertake withdrawals. Depending on where they are stored, it can take from two hours to more than a day to withdraw assets from cold storage, reducing the ability to react quickly to price changes. This is particularly the case where multiple signatures are required.

Hot storage requires good cybersecurity habits

Hot storage describes wallets that are connected to the internet, whether on an exchange or on a user's device. Any connected wallet runs the risk of being hacked, although to trade assets, at some point a hot wallet must be used. Methods to improve the security of hot wallets include backing up the contents, using two-factor authentication and exercising good cybersecurity hygiene (eg keeping anti-virus software up to date, using a password manager). To further secure the wallet, users can add whitelisting (cryptocurrency can only be sent to a user-approved list), set limits (eg to number of log ins) and use data encryption at rest and in transit.

Warm storage attempts a compromise between hot and cold storage

To try to provide the best of both worlds, warm storage solutions have been developed. These provide a bridge between cold storage and fully online wallets by using secure HSMs and adding additional logical steps to transactions. For example, although Bakkt's warm wallet is network connected, all withdrawal requests are verified and processed by staff located in multiple geographies and requests are validated, both manually and systematically, against rules that set controls over the amount, destination and velocity of transactions. Each transaction requires multiple individuals across multiple teams and locations to be involved.

[6] Federal Information Processing Standard

[7] Common Criteria is an international standard for computer security developed through the combined efforts of Canada, France, Germany, the Netherlands, the UK and the US.

[8] Evaluation Assurance Level 2

Exhibit 10: Range of storage options

	DIGIVAULT KELVIN		DIGIVAULT HELIOS	
	Deep Cold Custody	Cold Custody	Warm Custody	Hot Custody
Security	Highest	High	High	Medium
Accessibility	Low - manual operations required	Low – manual operations required but no third-party involved	High – accessible online	High – accessible online
Protection of Private Key	• Keys stored offline with air gap • Physical protection against key duplication and/or theft • Extremely secure storage operated by a third-party, reduces collusion risk	• Keys stored offline, possibly no air gap • Minimal physical protection against key duplication and/or theft • Keys stored by custodian	• Logical protection against key duplication and/or theft • Hardware protection of network • Secure server location operated by third-party provider	• Key stored in raw format on server and not within a protected hardware device
Insurability	• Highest	• High	• High	• Low

Accessibility →

← Security

Source: Diginex

Techniques to improve security

One technique commonly used to add another layer of security is **multi-signature technology (multi-sig)**. This replaces the use of one private key to authenticate a transaction with the requirement for m out of n signatories to sign a transaction (for example, two out of three signatories). While this improves security, it can slow down processing speeds and needs to be customised for each ledger used. It also results in higher block processing costs.

Another technology in use is **multi-party computation (MPC)**. In this case, independently generated shares of cryptographic material are used instead of private keys. Each share is distributed to a different party. Like multi-sig, this is an m out of n technology, where the investor selects m and n. When an investor wants to transfer a digital asset, shares are provided by m out of n holders and never combined in order to authenticate the transaction. No share holds enough useful information on its own, so if it is lost, the asset cannot be stolen. As holders of the shares need to communicate with each other, this can create scaling issues, particularly as the size of m increases. It can also be complicated to create back-ups of private keys using MPC. Examples of companies offering MPC as an alternative or enhancement to cold and hot storage include Curv (with US$50m insurance from Munich Re), Fireblocks and Unbound Tech.

Features offered by custodians

As well as providing a secure environment to store digital assets, custodians are increasingly adding functionality to enhance the security and appeal of their service. Features include:

- **Insurance**: to cover the loss of assets. Some custodians will provide detail on the types of losses covered, such as theft, hacking, the financial limit on the insurance and the broker used.
- **Staking:** for PoS-based currencies, investors can earn digital assets by staking their assets to win the right to process transactions. As this would usually require the investor to hand over their assets during the staking process, it is difficult if the assets are held by a custodian. Several custodians have developed methods to allow asset owners to stake their assets while in custody.
- **Governance:** in some blockchains, asset owners participate in blockchain governance (eg voting on protocol measures) based on the level of assets they hold. Similar to the staking feature, some custodians have developed methods to allow investors take part in governance while assets are in storage.

The table below shows the main custodians targeting institutional investors and the features offered. We also note which custodians hold regulatory licences. Factors that investors should consider when selecting a custodian include the location of the cold storage (as it will have a bearing on speed of withdrawal and regulation), customer service, regulatory position, the availability of insurance (and the specifics of what is covered), and the physical, operational and logical controls put in place to secure the assets.

Exhibit 11: Digital asset custodians with institutional focus

Company (HQ)	Custody service	Hot storage	Warm storage	Cold storage	Insurance	Staking/ governance	Assets supported	Regulation/ oversight	Details
Anchorage (US)	Anchorage Trust Company	Unclear – details not provided on website. Claims not to be cold storage.				S/G	22	Approved as custodian by South Dakota Division of Banking	Offers option to trade direct from custody.
Archax (UK)				x			Security tokens	Seeking FCA licence	Using Unbound Tech's Crypto Asset Security Platform, based on MPC.
Bakkt (US)	Bakkt Trust Company		x	x	Up to US$125m		Bitcoin	NYFDS qualified custodian	Partnered with BNY Mellon for secure storage. Cold wallet keys are sharded.
BitGo (US)	BitGo Trust Company	x		x	Up to US$100m, provided by Lloyds of London	S	100+ coins and tokens	Approved as custodian by South Dakota Division of Banking; applying for approval in Germany; member of VQF in Switzerland (overseen by FINMA)	Offers the ability to trade out of cold storage via Genesis Global Trading partnership. Uses multi-sig. Use of trust company is optional.
Coinbase (US)	Coinbase Custody (US); Coinbase Custody International (Dublin)			x	Syndicate of insurers; max US$255m per incident & overall	S	35 (90% by market cap)	NYFDS qualified custodian	Two-hour withdrawal from cold storage within business hours, 24 hours outside of these hours.
Copper (UK)				x					Provides Walled Garden approach – whitelisted exchanges; uses multi-sig.
Diginex (HK)	Digivault		Launching Helios in H120	Kelvin	Insurance policy with Lloyd's of London syndicate		Bitcoin, Ether, ERC-20, ERC-1400	UK: planning to seek FCA AML authorisation for exchange tokens, aiming to join FCA Sandbox for security tokens & in parallel apply for a licence. Jersey: seeking to register as a trust company. Singapore: plans to apply for CMSL.	Uses Malca-Amit vaults and logistics globally.
Fidelity (US)	Fidelity Digital Assets			x			Bitcoin	NYFDS qualified custodian	Offers option to trade direct from cold storage
Finoa (DE)	Custody		x				Bitcoin, Ether, ERC-20	Preliminary BaFin approval	
Gemini (US)	Gemini Custody			x	Captive insurer 'Nakamoto', up to US$200m		18	NYFDS qualified custodian	Instant trading from cold storage on Gemini Exchange. Same day withdrawal. Uses multi-sig.
Nomura	Komainu Digital			x				Jersey custody licence	JV with Ledger & Global Advisors.
Paxos (US)	Paxos Trust			x				NYFDS qualified custodian	
Kingdom Trust (US)	Kingdom Trust	Unclear - details not provided online			Lloyds of London			Approved as custodian by South Dakota Division of Banking	
Prime Trust (US)	Prime Trust	Unclear - details not provided online			Yes – provider/amount not disclosed		Bitcoin, Ether, ERC-20	NYFDS qualified custodian	
Trustology (US)	TrustVault	x			Bespoke cover available		Bitcoin, Ether, ERC-20		Uses Secure Enclave on mobile device (iOS only). Uses multi-sig.
Vo1t (UK)			x	x	Aon	S	>19		30 to 120-minute withdrawal time. Has a partnership with Curv.

Source: Company websites, Edison Investment Research

Demonstrating cybersecurity credentials

As well as using secure custody services, digital asset businesses need to show their customers they are taking security seriously. Audit and cybersecurity companies are using existing standards and adapting them to this sector. We highlight the main audit and certification tools used to assess cybersecurity in this sector:

- **ISO27001** is the international standard that provides the specification for an information security management system. Companies that achieve ISO27001 certification have implemented a framework through which they are able to identify, analyse and address information risks.
- **Service organisation control (SOC) audits: SOC 2** is an auditing procedure designed to ensure third-party service providers or service organisations can securely manage data to protect the interests and privacy of their clients. An SOC 2 report confirms a service organisation has put in place certain controls to meet some or all of the trust service principles (availability, confidentiality, processing integrity, privacy and security). There are two SOC 2 report types: Type I, which describes the systems of a vendor and assesses whether it is capable of meeting relevant trust principles as of a specified date, and Type II, which details the operational effectiveness of the systems throughout a specified period of time. Companies that have received SOC 2 certification include Bakkt (Type II), BitGo (Type I and II), Coinbase (Type 1) and Gemini (Type I and II). A **SOC 1** report reviews the internal controls over financial reporting. Fidelity Digital Assets has SOC 1 Type I certification.
- **Cyber Essentials:** in the UK, the government has developed the Cyber Essentials certification, which specifies requirements for IT infrastructure and covers five risk areas: firewalls, secure configuration, user access control, malware protection and patch management. Digivault has received Cyber Essentials Plus accreditation.

To help provide advice on crypto-specific security, specialist crypto-focused cybersecurity companies are emerging, such as Coinnect and Hacken. At the same time, traditional cybersecurity companies are building out crypto practices.

CryptoCompare regularly publishes its Exchange Benchmark report,[9] which ranks the top 100 cryptocurrency exchanges based on a number of factors, including security. Making this kind of information available to the public should be a crucial motivator to exchanges to up their game when it comes to the security of customer assets.

Private blockchains not immune from security issues

While the security of private blockchains is likely to be helped by the fact each node is a known, trusted participant, this does not remove traditional cybersecurity risks. Issues such as the ability of third parties or internal bad actors to access nodes, errors in software code and business continuity still need to be addressed.

Data privacy concerns to be addressed

The EU introduced strict data privacy regulations with GDPR in 2018 and other territories have introduced, or are introducing, similar regulations (eg the California Consumer Privacy Act). These regulations give data subjects the rights to compel data controllers to correct or delete personally identifiable information about themselves. Participants in a blockchain will need to consider how these privacy requirements can be met bearing in mind all information on a public blockchain is visible to all participants in the network. Fully anonymised data on a blockchain would fall outside the scope of data privacy laws, but as we have discussed on page 28, AML/KYC rules mean full

[9] CrytptoCompare Exchange Benchmark Q3 2019

anonymisation of data is unlikely if businesses are to be able to establish customers' identities. If a data subject asks for their data to be corrected or deleted, even if all nodes agreed to make the change, this would change the block that contains the data and break the links to the next block. Additional problems arise in identifying who is a data controller or data processor – does a node count as a data controller? Who decides whether to correct or delete data? Who would the regulator pursue in the event of a suspected breach?

One solution would be to store personal data off-chain, separately encrypted, so it could be amended without affecting the blockchain. However, this would have its own security issues – the data could be hacked and as it is not on-chain, it would be harder to guarantee it had not been accessed or tampered with.

A recent Europa study[10] discusses the difficulties in applying GDPR on the blockchain. While the report did not provide any concrete answers on how to deal with the contradictions, it suggests further regulatory guidance is required to ascertain how the concepts within GDPR should be applied, particularly for anonymisation and data controllers. It also suggests that compliance will be considered on a case-by-case basis, as the structure of each blockchain is different.

These issues mainly relate to public blockchains. In the case of private blockchains, it is easier to agree on who controls the data and how to prevent access to data outside of the network members.

[10] The Blockchain and the General Data Protection Regulation; EPRS July 2019

Glossary

5MLD: fifth anti-money laundering direction (EU)

ACPR: Autorité de contrôle prudentiel et de resolution (France)

AMF: Autorité des marchés financiers (France)

AML: anti-money laundering

ATS: alternative trading system (US)

BaFin: federal financial supervisory authority (Germany)

CBDC: central bank digital currency

CFTC: commodity futures trading commission (US)

CTF: countering the financing of terrorism

DPoS: delegated proof of stake

DSE: digital securities exchange

DLT: distributed ledger technology

FATF: financial action task force (global)

FCA: financial conduct authority (UK)

FinCEN: financial crimes enforcement network (US)

FSA: financial services authority (Japan)

GDF: global digital finance

GDPR: general data protection regulation (EU)

HKMA: Hong Kong monetary authority

HSM: hardware security module

ICO: initial coin offering

JFSC: Jersey financial services commission

KYC: know your customer

MAS: monetary authority of Singapore

MPC: multi party computation

NYDFS: New York State Department of Financial Services (US)

OTC: over the counter

PoS: proof of stake

PoW: proof of work

SEC: US securities and exchanges commission

SFC: securities and futures commission (HK)

SOC: service organisation control

SSSS: Shamir's secret sharing scheme

STO: security token offering

SWIFT: global secure financial messaging service

VCE: virtual currency exchange

General disclaimer and copyright

This report has been commissioned by Diginex and prepared and issued by Edison, in consideration of a fee payable by Diginex. Edison Investment Research standard fees are £49,500 pa for the production and broad dissemination of a detailed note (Outlook) following by regular (typically quarterly) update notes. Fees are paid upfront in cash without recourse. Edison may seek additional fees for the provision of roadshows and related IR services for the client but does not get remunerated for any investment banking services. We never take payment in stock, options or warrants for any of our services.

Accuracy of content: All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report and have not sought for this information to be independently verified. Opinions contained in this report represent those of the research department of Edison at the time of publication. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

Exclusion of Liability: To the fullest extent allowed by law, Edison shall not be liable for any direct, indirect or consequential losses, loss of profits, damages, costs or expenses incurred or suffered by you arising out or in connection with the access to, use of or reliance on any information contained on this note.

No personalised advice: The information that we provide should not be construed in any manner whatsoever as, personalised advice. Also, the information provided by us should not be construed by any subscriber or prospective subscriber as Edison's solicitation to effect, or attempt to effect, any transaction in a security. The securities described in the report may not be eligible for sale in all jurisdictions or to certain categories of investors.

Investment in securities mentioned: Edison has a restrictive policy relating to personal dealing and conflicts of interest. Edison Group does not conduct any investment business and, accordingly, does not itself hold any positions in the securities mentioned in this report. However, the respective directors, officers, employees and contractors of Edison may have a position in any or related securities mentioned in this report, subject to Edison's policies on personal dealing and conflicts of interest.

Copyright: Copyright 2020 Edison Investment Research Limited (Edison). All rights reserved FTSE International Limited ("FTSE") © FTSE 2020. "FTSE®" is a trade mark of the London Stock Exchange Group companies and is used by FTSE International Limited under license. All rights in the FTSE indices and/or FTSE ratings vest in FTSE and/or its licensors. Neither FTSE nor its licensors accept any liability for any errors or omissions in the FTSE indices and/or FTSE ratings or underlying data. No further distribution of FTSE Data is permitted without FTSE's express written consent.

Australia

Edison Investment Research Pty Ltd (Edison AU) is the Australian subsidiary of Edison. Edison AU is a Corporate Authorised Representative (1252501) of Crown Wealth Group Pty Ltd who holds an Australian Financial Services Licence (Number: 494274). This research is issued in Australia by Edison AU and any access to it, is intended only for "wholesale clients" within the meaning of the Corporations Act 2001 of Australia. Any advice given by Edison AU is general advice only and does not take into account your personal circumstances, needs or objectives. You should, before acting on this advice, consider the appropriateness of the advice, having regard to your objectives, financial situation and needs. If our advice relates to the acquisition, or possible acquisition, of a particular financial product you should read any relevant Product Disclosure Statement or like instrument.

New Zealand

The research in this document is intended for New Zealand resident professional financial advisers or brokers (for use in their roles as financial advisers or brokers) and habitual investors who are "wholesale clients" for the purpose of the Financial Advisers Act 2008 (FAA) (as described in sections 5(c) (1)(a), (b) and (c) of the FAA). This is not a solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned or in the topic of this document. For the purpose of the FAA, the content of this report is of a general nature, is intended as a source of general information only and is not intended to constitute a recommendation or opinion in relation to acquiring or disposing (including refraining from acquiring or disposing) of securities. The distribution of this document is not a "personalised service" and, to the extent that it contains any financial advice, is intended only as a "class service" provided by Edison within the meaning of the FAA (i.e. without taking into account the particular financial situation or goals of any person). As such, it should not be relied upon in making an investment decision.

United Kingdom

This document is prepared and provided by Edison for information purposes only and should not be construed as an offer or solicitation for investment in any securities mentioned or in the topic of this document. A marketing communication under FCA Rules, this document has not been prepared in accordance with the legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research.

This Communication is being distributed in the United Kingdom and is directed only at (i) persons having professional experience in matters relating to investments, i.e. investment professionals within the meaning of Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005, as amended (the "FPO") (ii) high net-worth companies, unincorporated associations or other bodies within the meaning of Article 49 of the FPO and (iii) persons to whom it is otherwise lawful to distribute it. The investment or investment activity to which this document relates is available only to such persons. It is not intended that this document be distributed or passed on, directly or indirectly, to any other class of persons and in any event and under no circumstances should persons of any other description rely on or act upon the contents of this document.

This Communication is being supplied to you solely for your information and may not be reproduced by, further distributed to or published in whole or in part by, any other person.

United States

Edison relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Investment Advisers Act of 1940 and corresponding state securities laws. This report is a bona fide publication of general and regular circulation offering impersonal investment-related advice, not tailored to a specific investment portfolio or the needs of current and/or prospective subscribers. As such, Edison does not offer or provide personal advice and the research provided is for informational purposes only. No mention of a particular security in this report constitutes a recommendation to buy, sell or hold that or any security, or that any particular security, portfolio of securities, transaction or investment strategy is suitable for any specific person.

Frankfurt +49 (0)69 78 8076 960
Schumannstrasse 34b
60325 Frankfurt
Germany

London +44 (0)20 3077 5700
280 High Holborn
London, WC1V 7EE
United Kingdom

New York +1 646 653 7026
1,185 Avenue of the Americas
3rd Floor, New York, NY 10036
United States of America

Sydney +61 (0)2 8249 8342
Level 4, Office 1205
95 Pitt Street, Sydney
NSW 2000, Australia