GLOBAL RESEARCH INSTITUTE

DWS

DIGITALISATION

April 2018

WHAT DISTRIBUTED LEDGERS MEAN FOR ASSET MANAGEMENT

Compared with some industries, asset management does not have many of the problems for which distributed ledger technologies are the only solution. But there still are plenty of exciting opportunities.

SUMMARY

Distributed ledger technologies (DLTs or blockchains) were invented to fix many problems that financial service companies do not share to the same extent as other industries – namely around trust and central coordination. Still, asset managers should be optimistic.

Benefits could manifest themselves in three main ways: First, in how asset managers organise themselves. Second, in the structure of the market ecosystem. Third, in the underlying investments themselves – what an asset manager can buy for the benefit of its clients.

Improvements to business models include negating the need for parallel record keeping and reconciliations, as well as mitigating operational risks. For the asset management industry, certain information needs to be public, from regulatory reporting to trade pricing, and so-called public registers provide proofs that can be verified by others. Likewise many of the inputs used by analysts could run entirely on blockchains, from land registry data or company information. Or regulators may decide to manage a know-your-client register on a public blockchain.

Distribution is another area of focus where DLT could lead to better service for clients. The most radical approach would be a tokenisation of shares in investment vehicles, that is putting an entire fund on a blockchain. This would allow for efficient subscription and redemption mechanisms and facilitate the secondary trading of units. It could also lower costs by disintermediating distributors.

Meanwhile, everyday asset management processes such as onboarding, document management, trade execution and settlement, ownership transfer, voting, and receiving dividends could be done through so-called smart contracts. These allow even advanced pieces of business logic to be automated. In addition, activities such as regulatory reporting and investor relations could be made more efficient this way.

In terms of the market econsystem, DLT could have a profound influence on the way trading in underlying investments is organised. This could change important areas such as settlement speed, collateral management, trade reconciliation or asset life-cycle management.

Another rarely spoken about opportunity for asset managers is how blockchain can potentially open up and facilitate new business in frontier markets. Indeed, blockchain is most valuable in countries with radically different legal systems and local conventions.

Finally, exploring new blockchain-based solutions is an opportunity for asset managers to refresh old technologies with a newer code built on widely tested systems created by a large pool of external talent. The review process itself should lead to long-term improvements that benefit clients.

Adam Iley
Head of User Technologies,
DWS Digital & Innovation
adm.iley@dws.com

Roland Guenther
Vice Presiden
DWS Digital & Innovation
roland.guenther@dws.com

Stuart Kirk
Head of Global
Research Institute
stuart.kirk@dws.com

Introduction

Bitcoin[1] was developed to solve the problem of how a group of people who do not trust or even know each other can agree on matters of value without a central coordinator and without the issue of "double spending" – that is, fraudulently transferring the same money several times to several counterparties unbeknownst to each other.

Bitcoin solved these problems using a structure known as a blockchain in which transactions were grouped into blocks and blocks were linked to previous blocks. For more details on the blockchain structure, see the Appendix.

The term blockchain is now often used as an umbrella term describing many different systems that are similar or improve on the original bitcoin system. This usage is occasionally confusing as not all technologies that fall under this umbrella use a chain of blocks. We will use the term blockchain to refer to the block structure and distributed ledger technologies (DLT) to refer to the field more generally.

Although cryptocurrencies[2] such as bitcoin were the first and most visible, they are just one application of a technology that brings together cryptography and distributed data. As well as tracking ownership of cryptographic assets, the same approach can be used in a number of other ways. For example Ethereum has created smart contracts that are programmes running in the ledger that cannot be tampered with.

A distributed ledger is a way of storing data, such as ownership information, with maintenance not done centrally, but distributed between a group of peers. The data can vary, the information can be public or private, and maintainance rights can be equally shared or limited to a sub-group of participants. In the case of smart contracts, they go one step further than maintaining data – doing something to and with the data automatically.

Depending on which characteristics are emphasised, this technology has many advantages such as transparency and resistance to manipulation. But it also has disadvantages compared to a centralised ledger, including speed (it takes longer to add data), scalability (recording of entire history) and, for public ledgers, consumption of energy (mining consumes vast amounts of computing power and in turn substantial amounts of energy). It is therefore not suited to every problem. However, when distributed ledgers are applied to certain issues they have the potential to be transformative for value chains in many industries as an enabling technology.

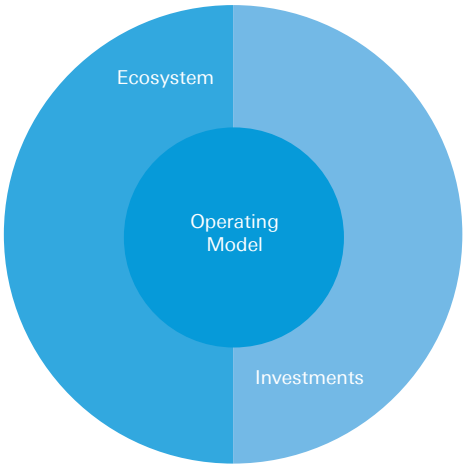
Players in the asset management space and fintech entrants have tried to outdo each other with announcements on how they are going to use DLT. So far there are limited actual examples. Potential uses should be evaluated according to their risk/reward and cost profile. What counts are the innovations clients can look forward to. As fiduciaries, it is important asset management firms chose and drive their agenda, rather than wait for other participants along the value chain (banks, custodians etc.) to adopt their own solutions first .

The aim of this paper is to understand the possible impact the advent of DLT might have on the asset management industry, particularly from a client perspective. Once the hype has settled down, there are lots of reasons to be optimistic. Potential impacts could manifest themselves in three main ways, each of which receives a section in the paper. They are:

1. In the way the asset managers organise themselves and their investment vehicles – for example, how processes are designed to reduce costs and risks or improve customer service
2. In the structure of the market ecosystem – how investments are traded and with whom
3. In the underlying investments themselves – what an asset manager can buy for the benefit of its clients

For readers interested in the technological aspects, the appendix contains further explanations and examples.

Chart 1: Blockchain Spheres of Influence for AM



[1] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, downloadable at https://bitcoin.org/bitcoin.pdf
[2] As just one example, see https://www.bloomberg.com/news/articles/2018_02_02/roubini-says-bitcoin-is-the-biggest-bubble-in-human-history.

DLT and asset management operating models

Distributed ledger technologies can potentially mean huge changes to asset management operating models. But it needs to be acknowledged from the start that blockchains were invented to fix many problems that financial service companies do not share to the same extent as other industries – namely around trust and central coordination.

Banks and asset managers have always run on trust and despite various crises continute to do so today. The finance industry is heavily regulated and accountable to central authorities. It is required by law to be honourable, trustworthy, and to deal only with clients it knows.

This means there is already a long history of interaction between financial companies, where efficient, centralised repositories of information have been shared – think of exchanges, custodian services, and so on. Indeed, many problems that blockchain solutions purport to solve would be sorted out more efficiently by using a centralised database.

For example, supply chains are often cited as examples of where blockchains could be useful to the industry. However, if asset managers, their providers and customers can agree to use a decentralised solution such as a blockchain, they should be able to coordinate themselves to use a more efficient centralised approach.

Nor does the double spending problem (see appendix), a key issue DLT was invented to solve, apply in many situations where physical assets are being tracked on a distributed ledger. A simple arrangement where at each link in the chain a certificate indicating transfer of ownership is signed by both parties is sufficient.

And perhaps the biggest drawback with blockchain for asset managers is the need to keep many client transactions private. There is a solution to the transparancy problem, however. Create a private ledger where only those with permission are allowed to connect. This is the approach taken by some of the DLT projects aimed at banks, such as R3 Corda[3] and hyperledger[4].

That said, the likely efficiency gains to asset managers from DLT are huge – also allowing clients to save on costs. The main areas of potential gains are describted below, starting with the fact that distributed public ledgers are perfect places to store public information cheaply.

Public registers

Public registers negate the need for parallel record keeping and reconciliations, as well as mitigating operational risks. They provide proofs that can be verified by others. For example it is possible to write a transaction that proves ownership of a document or image at a particular time without revealing what the document contains. This is perfect for things such as trademarks or claims of copyright.

For the asset management industry, certain information needs to be public, from regulatory reporting to trade pricing. Likewise many of the inputs used by analysts could run entirely on blockchains, from land registry data or company information, thereby providing a greater level of transparency and the ability for smart contracts to operate against the data directly.

Or regulators may decide to manage a know-your-client register on a public blockchain, keeping encrypted documents that prove that particular addresses belong to particular individuals. Such a register could be a point of coordination for further services and applications.

On this topic, the EU's new General Data Protection Regulation[5] right to forget personal data stored on an immutable medium is potentially in conflict with the blockchain's immutable history. Whilst not relevant for most use cases of a more institutional nature, it could be an issue with regards to storing personal data in the area of distribution or a unit ownership ledger for retail.

Distribution

Distribution is another area of focus where DLT could lead to more efficient and swifter service for clients. The most radical approach would be a tokenisation of shares in investment vehicles that is putting the entire "fund"/pooled vehicle on the blockchain. This would allow for efficient subscription/redemption mechanisms and facilitate secondary trading of units, and could also lower costs by disintermediating distributors. Less radical is a shared ledger of units, establishing a clear ownership record in countries where there is no centralised register.

A first step in that direction has been made by IBM Hyperledger, Northern Trust and Unigestion, allowing secondary trading in the latter's Private Equity funds on the blockchain[6]. Another example is the cooperation between Nasdaq and SEB on a platform for Swedish mutal funds to establish a unit ledger[7].

[3] https://www.r3.com/
[4] https://www.hyperledger.org/
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council
[6] http://www-03.ibm.com/press/us/en/pressrelease/51655.wss
[7] https://m.nasdaq.com/article/seb-and-nasdaq-to-build-blockchain-for-swedish-fund-market-cm852832

FundsDLT, KPMG and Natixis are trying to test a blockchain enabled new distribution channel in Luxemburg[8]. IZNES has been established to allow direct distribution of units from fund managers to clients[9]. Calastone are endeavouring to build a distributed market infrastructure for the mutal funds industry and have announced they will move onto blockchain 2019, with an estimated £2bn in cost savings to the industry[10].

Furthermore, client reporting could also be facilitated by a move to DLT, with regards to sharing data.

Technology refresh

If nothing else the arrival of blockchain is a good reason for asset managers to undergo a technology refresh – an opportunity to move old systems to a newer code built on widely tested systems created by a large pool of external talent.

Although many uses of blockchain could instead be provided by a sufficiently advanced scheme using modern cryptography and traditional databases, the fact is that there are many systems that would benefit from the use of modern cryptographic techniques but cannot easily do so.

It is a common adage in software engineering that you should never write custom cryptography code yourself – it needs extensive study, testing and deployment across an industry to achieve safe acceptance. While asset managers could create new systems using a modern approach to cryptography, it may be easier and less risky to leverage the talent already working on blockchain technologies.

DLT and ecosystem

Depending on efforts by market counterparties such as banks, DLT could have profound effects on the way trading in underlying investments is organised. This could change important areas such as settlement speed, collateral management, trade reconciliation or asset life-cycle management. This has also piqued regulatory interest. Useful overviews of potential applications can be found in an ESMA paper[11] and the Financial Conduct Authority's recent feedback statement[12].

One example is syndicated loan settlement, where a group of companies (Credit Suisse, Ipreo, Symbiont and R3 together with buy-side firms AllianceBernstein, Eaton Vance Management, KKR and Oak Hill Advisors) have delivered a proof of concept to help speed up syndicated loan settlement via a loan data ledger eliminating the need for manual record keeping and reconciliation[13].

Smart contracts

Large organisations often have an enormous number of manual processes, many of which could be executed more efficiently. So-called smart contracts allow even advanced pieces of business logic to be automated. For asset managers, everyday processes such as onboarding, document management, trade execution and settlement, ownership transfer, voting, and receiving dividends could be done through smart contracts. Even activities such as regulatory reporting and investor relations should be made more efficient this way.

Cutting manual and paper processes could increase speed while reducing errors and staff needed significantly. Smart contracts can be thought of as a form of cloud computing where computations happen against a state that is stored and tracked in the ledger. For example there are more than 12,000 smart contracts running on the Ethereum blockchain right now. Many of these are simple pieces of code tracking the owners of newly issued tokens or other coins, but some are much more complex.

Many asset management processes could run entirely on a blockchain with little or no human involvement at all. A smart contract for an ETF could allow instance purchasing and settling, provide a public certificate of ownership if required, and pay out a dividend agreed by multiple companies within the security.

In fact, the original Ethereum DAO (Distributed Autonomous Organisation) was intended to operate like an investment fund. It had an initial accumulation phase that distributed tokens representing shares to investors, an automated investment phase where the investors were able to vote on the projects to invest in, and finally automated payouts of any proceeds.

Another possibility for companies such as asset managers would be to move internal project management processes and budget tracking to smart contracts running on a private blockchain. The benefits would again be increased transparency, security and automation.

[8] https://home.kpmg.com/lu/en/home/insights/2017/06/natixis-asset-management-test-blockchain-fundsdlt.html
[9] http://www.iznes.io/img/cplznesEn.pdf
[10] http://www.calastone.com/news/calastone-forecasts-over-1-9bn-savings-for-the-mutual-funds-market-in-move-to-blockchain/
[11] https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf
[12] https://www.fca.org.uk/publication/feedback/fs17-04.pdf, particularly pp. 17-19
[13] https://www.credit-suisse.com/corporate/en/articles/media-releases/blockchain-demonstration-shows-potential-loan-market-improvements-201609.html

Selling services on blockchains

The asset management industry is already exploring many uses for smart contracts, with fund distribution a particular focus among European managers. Less explored is the need for trusted institutions to publish financial and economic data to the various public blockchains. It is possible to generate revenues for this service and costs would be minimal as companies including asset managers are already collecting this data.

What is driving this demand for data? Those writing smart contracts often want to connect them to the real world, having contracts react to events or use information from outside the blockchain in decision-making processes. That is because smart contracts can only make use of information that has been published into the blockchain.

The problem is there is a dearth of trust in the ecosystem. Many smart contracts rely on small, potentially untrustworthy companies to provide information such as live stock prices or forex rates. Likewise in theory asset managers could charge for know-your-client information on a blockchain.

DLT and investments

With regards to underlying investments, the first example is the potential of buying crypto assets. While certainly highly speculative and to a degree questionable, irrespective of where one stands with regards to such investments, as a simple fact crypto funds last year were the fasted growing hedge fund segment[14].

By establishing trust through irrevocable proof, DLT also has the potential to make certain market segments more accessible (some emerging market assets, say).

Frontier markets with weak institutions

Another rarely spoken about opportunity for asset managers is how blockchain can potentially open up and facilitate new business in frontier markets. Indeed, blockchain is most valuable in countries with radically different legal systems and local conventions.

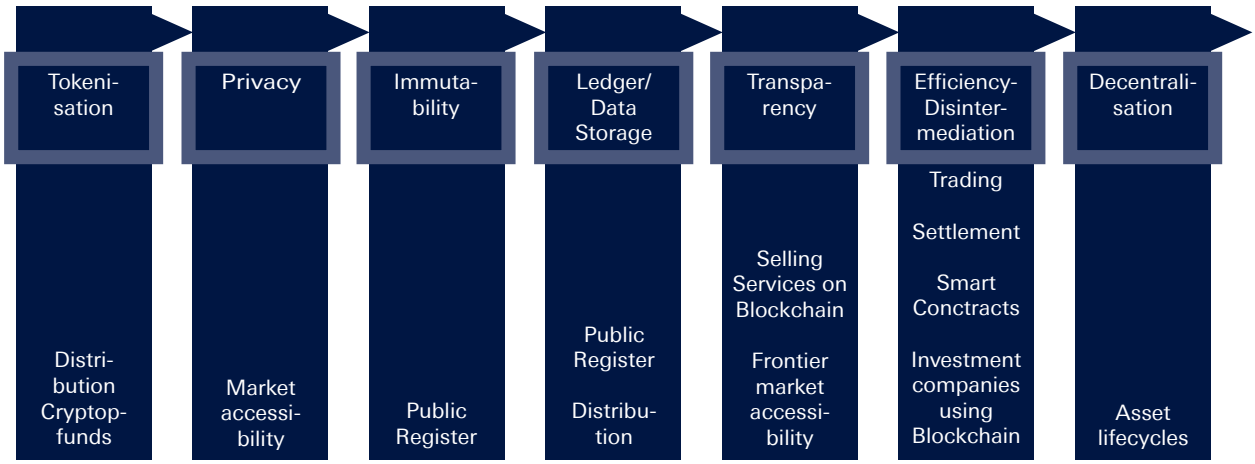
For example, it can be difficult to do business in markets that have problems with corruption. But using modern cryptography to certify transfers, and the transparency gained by tracking assets on a blockchain, could bring into scope revenue opportunities previously deemed too risky.

The use of blockchain in countries with weak institutions is already happening. The UN's World Food Programme has been experimenting with a blockchain for providing aid in Pakistan, and is planning a larger roll out. Already more than 10,000 Syrian refugees are purchasing goods with eye scans and having these transactions recorded on a blockchain.

Less speculative, but with potentially much more benefit for clients is focusing on investments in securities that benefit from the propagation or adoption of DLT by their issuers. This means early-stage investments in DLT companies, or simply analysing which companies/industry sectors or potentially even countries will potentially post additional revenue streams or efficiency gains in a DLT environment, irrespective of whether that investment is being made via active/passive or alternative styles.

Finally, DLT could be used to extract value more efficiently out of underlying investments as they go through their lifecyle (examples might lie in management of real assets such as real estate or infrastructure investments, or more efficient interest rate/dividend payments for different types of securities through smart contract applications).

Chart 2: Transmission Mechanism: Blockchain and Related AM Products/Services



[14] Bitcoin Rise Ignites Crypto Fund Explosion – Hedge Fund Alert 15-11-2017

APPENDIX

A beginners guide to blockchain

A block is just a bundle of data. It could theoretically store anything, but in a distributed ledger blocks usually store transactions that record transfers of value – just like the lines in a ledger book.

A blockchain is a data structure where subsequent blocks depend on all of the blocks previous to them. They do this by recording the hash of the block immediately prior to them in the chain, which in turn includes its own hash of the block immediately preceding it. In this way a blockchain has a level of tamper resistance, since to modify a historical transaction would require not just changing that transaction but also the block it was recorded in and all the blocks that came after.

> *Hashing* is a way of taking potentially lots of data and describing them in a single piece of data – the hash. It is like a summary or a fingerprint of something bigger. For cryptographic hashes it is easy to take some data and find a hash, but it is very hard to do this in reverse – to start with a hash and generate some data that matches it. This is because changing any of the data, even only a little, results in a completely different hash.

Consensus and nodes

To be useful as a ledger, a chain of blocks needs a mechanism for adding new blocks onto its end. When a blockchain is designed to serve mutually distrusting individuals, it needs to be sure that when someone suggests a new block, the transactions in it are all legal – that is, they do not contradict earlier transactions. If lots of different people are suggesting new blocks to add to the chain, everyone needs a way of agreeing which ones should be added and which ones should not.

This process of many different parties coming to agreement about something (in this case which blocks should be accepted as containing transactions that change the ledger) is called consensus. Two famous consensus algorithms are Paxos[15] and Raft[16]. These algorithms and others like them are commonly used in distributed databases to ensure that all the database replicas agree, without losing any data. A big problem is knowing in advance which computers will be part of the network and trusting that these nodes are behaving honestly. There are similar algorithms that can cope with some malicious actors, such as Practical Byzantine Fault Tolerance[17], which are used by some private blockchains to control which users are permissioned to access them.

> *The double spend problem* is where someone sends 10 coins to someone else and then tricks a network into thinking they are still allowed to send the same 10 coins to someone else. It is the central problem that cryptocurrencies needed to solve. Old fashioned cryptography was enough to prove that someone had legitimately acquired some coins – provided every transaction was signed by the originator – but until Bitcoin, there was no known way for a decentralised system of mutually distrusting parties to know they had not transferred them on already.

Therefore, people working to create money that could be used on the internet with similar characteristics to cash needed a system that could result in consensus, even if some individuals were behaving badly. And if someone went offline they needed to come back later and work out which transactions had happened. Another requirement was new participants should be able to join a network whenever they wanted without having to get permission from everyone else.

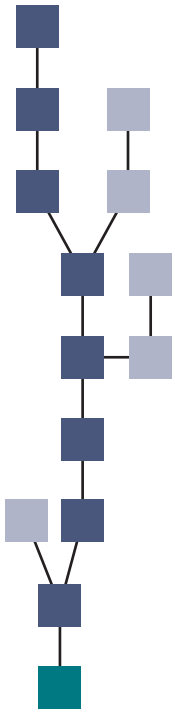
> Bitcoin nodes that are trying to get their suggested blocks accepted by the rest of the Bitcoin network are called *miners*. They compete to be the first to make a block with a hash that meets the network difficulty. The difficulty is recalculated every 2016 blocks (approximately every two weeks) with the target of having a new block found by the network every 10 minutes. Since a node only receives transaction fees and the reward in chains that contain its block, miners are highly incentivised to add blocks to the longest chain.

Mining and proof of work

In 2008, an individual or individuals calling themselves Satoshi Nakamoto[18] finally came up with a plan that had the characteristics needed to solve the problems outlined above. The scheme was based on blockchains but required that adding blocks must be a difficult thing to do and that whichever chain had the most

[15] http://lamport.azurewebsites.net/pubs/paxos-simple.pdf
[16] https://raft.github.io/raft.pdf
[17] http://pmg.csail.mit.edu/papers/osdi99.pdf
[18] https://bitcoin.org/bitcoin.pdf

valid blocks was the true chain. So if two people wanted different valid blocks to be the next one, although temporarily no one may not know which is the right one, after a few more blocks have been added it should be easy to see which is part of the longest chain, and so that is the block ultimately be accepted by everyone.



For this to work, adding blocks must be difficult otherwise people could build on any block and the network would keep switching between the different possible chains – there would be no consensus. The process that makes adding blocks difficult is called *proof of work* and involves the hashes mentioned above. With cryptographic hash algorithms, it is difficult to modify data in order to get a specific hash, so everyone taking part agrees that the hash of each block needs to be smaller than some value.

It does not matter what the hash is, but everyone has to guess the change needed to make to their suggested block arrive at a hash that meets the requirement. There is a special value called a nonce that is included in the data specifically so it can be tweaked in order to get a different hash. The process of guessing a nonce and checking until you find a good hash requires lots of computational effort and time. As people add new hardware to do this work, the network recalibrates. Everyone agrees to reduce the number that hashes must be below, making it harder to find a suitable one.

If the *mining* computers verifying transactions start going offline, then the number increases and the difficulty decreases again. And as the chain lengthens more computing power is needed to modify something in a blockchains history. This is why transactions in the latest mined block are susceptible to being cancelled if a competing chain becomes longer, but also why transactions in a block that has had multiple blocks on top of it is very secure.

Incentives

In order to incentivise people to go to the effort required to have a block accepted, every block found grants the finder some coins as a reward. They also receive fees from any transactions included in the block. Reward coins are freshly created for a block. For many other cryptocurrencies, the size of reward minted in each new block is on a reducing schedule and eventually stops. Bitcoin will grant 21m coins in total. Many of the early cryptocurrency pioneers had a libertarian dislike of government and in particular inflation, so most cryptocurrencies have a capped supply such that miners will be entirely reliant on transaction fees. This is also considered to be good for early adopters as a limited supply of coins is hoped to result in their value appreciating.

Chart 3: Miners revenue (USD)[19]

[19] Source: https://blockchain.info/charts/miners-revenue

Altcoins

Once the basic scheme behind Bitcoin was shown to be workable, it spawned many imitators and innovators, often called altcoins. Some are straightforward clones, some are simple tokens running as smart contracts on other platforms. Others innovate in various ways. The box below lists a few of the interesting larger altcoins targeting the general public.

Ethereum	Blockchain as a platform	Along with transactions, Ethereum allows bytecode programs to be stored on a blockchain, which are then executed by the miners whenever someone sends a transaction to their address. This allows all kinds of advanced business logic to be run automatically and makes it easy to create new currencies, tokens and smart contract. The Ethereum network is configured to find blocks every 15 seconds rather than the ten minutes of the Bitcoin network, enabling faster confirmations.
Ripple	A semi-centralised, regulator friendly, cross network payments competing with SWIFT	Ripple aims to enable current payment networks to interconnect with low fees and automatic conversions where necessary. It is targeted mainly at banks and requires a trusted, known set of validators.
Bitcoin Cash	Bitcoin with bigger blocks.	Bitcoin has become more expensive as more transactions compete to get into the blocks. Bitcoin cash is a 'fork' of Bitcoin that allows bigger blocks. Combined with the fact that it is less popular than Bitcoin, its fees are currently around a fiftieth of the transaction fees on Bitcoin.
IOTA	A different datastructure: 'the tangle'.	IOTA uses a directed acyclic graph structure instead of a blockchain for its ledger. This has many potential benefits: no transaction fees, offline transactions, and scalability. But there are serious questions around whether consensus will happen in a reasonable period of time if it were under attack and its centralised coordinator was not running.
Monero	Privacy focused built on the CryptoNote protocol.	Bitcoin and many other distributed ledgers are public. All balances are known and transactions visible. The only privacy most cryptocurrencies provide is pseudonymity – transactions are made under an address/account number/public key rather than the real name of transactors. There are a few cryptocurrencies such as Monero that make it their aim to make transactions as private as possible, using cryptography to disguise the accounts taking part in a transaction and the amounts transferred. Unsurprisingly these cryptocurrencies are being increasingly preferred for grey and illegal transactions.

Problems and risks with blockchain

Resource usage

The system of spending a huge amount of energy to guess values in order to derive a good hash is currently using about 40 terrawatt hours of electricity for Bitcoin alone – approximately the annual energy consumption of Peru. This is unsustainable. Blockchains grow continuously as full nodes need all historical transactions in order to prove they have a legitimate history.

There are a few different ideas for how resource usage could be reduced. Most of these involve less energy intensive ways of making sure participants are incentivised to add to the longest chain or punished for bad behaviour.

Perhaps the leading solution so far is called proof of stake. Nodes take it in turns to suggest blocks but they must first put up a stake that they can lose if they are later found to have misbehaved by proposing conflicting blocks. Current proof of stake cryptocurrencies use a variant called delegated proof of stake. Some worry this increases centralisation too much, but there are other proof of stake algorithms. Ethereum for example is experimenting with an algorithm called Caspar, a proof of stake algorithm planned for the end of 2018.

Scalability

Another question mark hovering over Blockchain is whether it is scalable enough for ubiquitous use. By way of comparison Visa processes an average of 1,600 transactions per second and at peaks double that. Bitcoin on the other hand has a maximum blocksize that restricts the number of transaction on a block to around 2,000. Since new blocks are found every ten minutes, Bitcoin's typical transaction rate is around four per second.

Maybe it can manage seven transactions a second, which means it needs to improve by three orders of magnitude before it can be taken seriously as a global payments network. Other cryptocurrencies have boosted their throughputs and confirmation times by finding blocks faster and allowing blocks to contain more transactions. But they remain far short of Visa or PayPal, resulting in rising transaction costs on popular coins. Bitcoin transactions attract an average fee of 22 dollars.

And higher transaction fees are not the only repercussion of a lack of scale. The fact that blockchain networks are congested leads to financial risk too. For example, during market sell-offs transactions can take a very long time to be executed. Indeed its not unusual for exchanges to stop taking orders during periods of high volume.

To be fair, the process of achieving a decentralised consensus is inherently more difficult and slower than operating a centralised database as a leger. The networks that are the most scalable tend to have significant centralised aspects, such as Ripple and Stellar, or are entirely private. Finding a way to scale-up is essential for true distributed blockchains to have a future. There are a number of proposed solutions but they are still experimental and must prove that they do not compromise the security of the system.

Technology risk

The recent experience with cryptocurrencies shows that blockchain has some attractive security features, but is still exposed to a number of technology risks. Of primary concern is vulnerability to attack. In a so-called 51 percent attack, someone controlling a sufficiently large amount of the hashing power would eventually be able to create a new history that reverses transactions that were previously considered settled. Since their new chain would be the longest, the modified chain would be considered legitimate by other clients.

The name comes from the assumption that one would need a majority of all hash power on the network, although this is not strictly true. Even with less than half of the hash power an attacker may be successful. Luckily 51 per cent attacks remain theoretical. The main reason why is because they would probably require about $6bn dollars in hardware and nearly $11m per day in running costs. And such an attack would be visible and most likely result in a huge loss of confidence and hence a collapse in value of the cryptocurrency.

Furthermore, blockchain communities are aware of the dangers of centralising too much of the mining power and hence there is social pressure discouraging any one mining pool becoming too large. Of course a nation state may be prepared to lose money on damaging a network. Some worry there is a lot of the hash power in China that may be susceptible to malign influence.

Another type of potential attack is called transaction censorship. It is assumed that miners are incentivised by transaction fees to include all valid transactions

they receive. If some miners refused to add transactions involving particular parties into a block, those transactions would have increased confirmation times. Eventually they would be included by a miner that was not part of the attack, depending on what proportion of miners were part of the conspiracy. A wide distribution of miners is therefore key to avoiding this problem. There is also research into ways a transactor could prove they are being censored that would allow a network to take action.

There are also concerns around key management with stories of people losing keys with balances of hundreds of thousands of dollars. In order to transact on a cryptocurrency network, an individual needs a private key and a corresponding public key. If a private key is not backed up then money is essentially gone forever. Keys are typically stored in software called wallets, which if inadequately secured, provide another point of attack. One potential fix are threshold signatures that allow a form of multifactor authentication for wallet access. Since key management is difficult, many people rely on addresses controlled by an exchange. Some of the biggest losses have come when exchanges have been hacked or had employees run off with customers' money. Many exchanges are operating with little or no oversight.

A final technology risk worth mentioning involves smart contracts – a means of having business logic run automatically on blockchains. A bug in the smart contract code could allow an attacker to steal money from the contract or exploit it in other ways. There have already been a number of high-profile attacks with a significant amount of money stolen due to bugs in smart contract code. The most famous was a so-called re-entry bug in the Ethereum platform that allowed an attacker to steal around $50M. Luckily the funds were recovered. There are now tools to help write secure smart contract code but it is still a developing field.

In conclusion, while the Bitcoin platform has now had enough scrutiny and value passing through it to be fundamentally secure, innovations in alternative coins (Altcoins) that try to replace the basic structure with something more efficient or scalable are less proven. Weaknesses may be found that could potentially result in those networks breaking entirely.

Fraud and crime

Related to technology risk above is blockchain's vulnerability to basic forms of fraud and other crimes. This should not be a surprise as such risks always follow the money. For example, companies seeking alternative financing have begun issuing tokens on blockchains that they sell before they have started making money themselves, promising future rights to income. These so-called initial coin offerings (ICO) enabled companies to raise more than $4bn last year[20], outstripping early stage venture capital funding. The market has grown so quickly that there is little regulation and many offerings are fraudulent. According to Ernst & Young, more than a tenth of the money raised through ICOs has been lost or stolen[21].

Bitcoin is often used to extort, with WannaCry for example hitting more than 230,000 computers in 2017. WannaCry encrypted files on a user's hard disk and demanded a payment in Bitcoins to unencrypt them. It was blamed on North Korea, a country that is struggling to acquire foreign currency. Cryptocurrencies are being used to evade sanctions and capital controls as well as for extortion and ransom. At least all transactions and accounts on the Bitcoin ledger are public, so investigators and courts have more information than with cash-based crimes. But already more private cryptocurrencies such as Monero are emerging.

Regulatory risk

As with any financial activity there are risks around regulation. The oversight of cryptocurrencies is still in its early days with many regulators taking a light touch for now. But over the next year or so the regulatory environment is likely to crystallise, with some countries banning or heavily restricting exchanges.

For example, the Securities and Exchange Commission in America has made it clear that many of the ways smart contracts are being used – particularly where a company issues tokens to raise money – amounts to a securities issue and hence will be regulated as such[22]. The SEC has already begun acting against some of the most obviously fraudulent examples. Likewise China and South Korea have issued bans on raising money using cryptocurrency.

Volatility

Most cryptocurrencies are incredibly volatile, which creates risk for anyone holding them for any length of time. High volatility also makes it hard to predict in advance how much is needed to be paid in fees for any transaction. Gains and falls of 20 per cent over short periods are not uncommon. Combined with the slowness of transactions, speculators are often stuck trying to react to market movements.

[20] https://www.coinschedule.com/stats.html?year=2017
[21] https://www.reuters.com/article/us-ico-ernst-young/more-than-10-percent-of-3-7-billion-raised-in-icos-has-been-stolen-ernst-young-idUSKBN1FB1MZ

Volatility is a big issue if cryptocurrencies wish to become mediums of exchange. There are a few different attempts to address this. Tether for example has issued coins based on dollar reserves that have maintained a reasonable degree of stability. This despite Tether's relationship to an exchange that has been hacked numerous times and rumours[23] that its reserves do not match the stock of coins issued.

Meanwhile the Ethereum platform is approaching the volatility problem with something called a stablecoin[24]. This attempts to maintain a peg to the dollar using reserves. So far, stablecoin has performed quite well, despite the volatility in the overall market. But some concerns remain that it could fail in sufficiently adverse conditions.

Chart 4: Market Price (USD)[25]

Acknowledgements

Thanks to Joshua Evans, Sylvain Faucherand, David Wragg, and Samuel Williams for providing feedback on earlier versions of this paper.

[22] https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
[23] https://bitcoinexchangeguide.com/bitfinex-tether-scam/
[24] https://makerdao.com/
[25] Source: Thomson Reuters Datastream

IMPORTANT INFORMATION

The brand DWS (formerly known as Deutsche Asset Management) represents DWS Group GmbH & Co. KGaA and any of its subsidiaries, such as DWS Distributors, Inc., which offers investment products, or Deutsche Investment Management Americas Inc. and RREEF America L.L.C., which offer advisory services.

Investors will be provided with DWS' products or services by one or more legal entities that will be identified to (potential) investors pursuant to the contracts, agreements, offering materials or other documentation relevant to such products or services.

This document has been prepared without consideration of the investment needs, objectives or financial circumstances of any investor. Before making an investment decision, investors need to consider, with or without the assistance of an investment adviser, whether the investments and strategies described or provided by DWS, are appropriate, in light of their particular investment needs, objectives and financial circumstances. Furthermore, this document is for information/discussion purposes only and does not constitute an offer, recommendation or solicitation to conclude a transaction and should not be treated as giving investment advice.

DWS does not give tax or legal advice. Investors should seek advice from their own tax experts and lawyers, in considering investments and strategies suggested by DWS. Investments with DWS are not guaranteed, unless specified. Unless notified to the contrary in a particular case, investment instruments are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental entity, and are not guaranteed by or obligations of DWS or its affiliates

Investments are subject to various risks, including market fluctuations, regulatory change, counterparty risk, possible delays in repayment and loss of income and principal invested. The value of investments can fall as well as rise and you may not recover the amount originally invested at any point in time. Furthermore, substantial fluctuations of the value of the investment are possible even over short periods of time.

Past performance is no guarantee of future results; nothing contained herein shall constitute any representation or warranty as to future performance.

This publication contains forward looking statements. Forward looking statements include, but are not limited to assumptions, estimates, projections, opinions, models and hypothetical performance analysis. The forward looking statements expressed constitute the author's judgment as of the date of this material. Forward looking statements involve significant elements of subjective judgments and analyses and changes thereto and/or consideration of different or additional factors could have a material impact on the results indicated. Therefore, actual results may vary, perhaps materially, from the results contained herein. No representation or warranty is made by DWS as to the reasonableness or completeness of such forward looking statements or to any other financial information contained herein. The terms of any investment will be exclusively subject to the detailed provisions, including risk considerations, contained in the Offering Documents. When making an investment decision, you should rely on the final documentation relating to the transaction and not the summary contained herein.

IMPORTANT INFORMATION – UK

FOR PROFESSIONAL CLIENTS ONLY

Issued in the UK by Deutsche Asset Management (UK) Limited. Deutsche Asset Management (UK) Limited is authorised and regulated by the Financial Conduct Authority.

This document is a "non-retail communication" within the meaning of the FCA's Rules and is directed only at persons satisfying the FCA's client categorisation criteria for an eligible counterparty or a professional client. This document is not intended for and should not be relied upon by a retail client.

This document is intended for discussion purposes only and does not create any legally binding obligations on the part of DWS Group GmbH & Co. KGaA and/or its affiliates ("DWS"). Without limitation, this document does not constitute an offer, an invitation to offer or a recommendation to enter into any transaction. When making an investment decision, you should rely solely on the final documentation relating to the transaction and not the summary contained herein. DWS is not acting as your financial adviser or in any other fiduciary capacity in relation to this Paper. The transaction(s) or products(s) mentioned herein may not be appropriate for all investors and before entering into any transaction you should take steps to ensure that you fully understand the transaction and have made an independent assessment of the appropriateness of the transaction in the light of your own objectives and circumstances, including the possible risks and benefits of entering into such transaction. For general information regarding the nature and risks of the proposed transaction and types of financial instruments please go to https://www.db.com/company/en/risk-disclosures.htm. You should also consider seeking advice from your own advisers in making this assessment. If you decide to enter into a transaction with DWS, you do so in reliance on your own judgment.

Although information in this document has been obtained from sources believed to be reliable, we do not guarantee its accuracy, completeness or fairness, and it should not be relied upon as such. All opinions and estimates herein, including forecast returns, reflect our judgment on the date of this report and are subject to change without notice and involve a number of assumptions which may not prove valid.

Any projections are based on a number of assumptions as to market conditions and there can be no guarantee that any projected results will be achieved. Past performance is not a guarantee of future results. Any opinions expressed herein may differ from the opinions expressed by other DWS departments. DWS may engage in transactions in a manner inconsistent with the views discussed herein. DWS trades or may trade as principal in the instruments (or related derivatives), and may have proprietary positions in the instruments (or related derivatives) discussed herein. DWS may make a market in the instruments (or related derivatives) discussed herein. You may not distribute this document, in whole or in part, without our express written permission.

DWS SPECIFICALLY DISCLAIMS ALL LIABILITY FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL OR OTHER LOSSES OR DAMAGES INCLUDING LOSS OF PROFITS INCURRED BY YOU OR ANY THIRD PARTY THAT MAY ARISE FROM ANY RELIANCE ON THIS DOCUMENT OR FOR THE RELIABILITY, ACCURACY, COMPLETENESS OR TIMELINESS THEREOF.

Any reference to "DWS", "Deutsche Asset Management" or "Deutsche AM" shall, unless otherwise required by the context, be understood as a reference to Deutsche Asset Management (UK) Limited including any of its parent companies, any of its or its parents affiliates or subsidiaries and, as the case may be, any investment companies promoted or managed by any of those entities.

This document may not be reproduced or circulated without our written authority. The manner of circulation and distribution of this document may be restricted by law or regulation in certain countries. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction, where such distribution, publication, availability or use would be contrary to law or regulation or which would subject DWS to any registration or licensing requirement within such jurisdiction not currently met within such jurisdiction. Persons into whose possession this document may come are required to inform themselves of, and to observe, such restrictions.

IMPORTANT INFORMATION – GERMANY

The information contained in this document does not constitute investment advice.

The terms of any investment will be exclusively subject to the detailed provisions, including risk considerations, contained in the Offering Documents. When making an investment decision, you should rely on the final documentation relating to the transaction and not the summary contained herein.

This document may not be reproduced or circulated without our written authority. The manner of circulation and distribution of this document may be restricted by law or regulation in certain countries.

IMPORTANT INFORMATION – EMEA

Kingdom of Bahrain

For Residents of the Kingdom of Bahrain: This document does not constitute an offer for sale of, or participation in, securities, derivatives or funds marketed in Bahrain within the meaning of Bahrain Monetary Agency Regulations. All applications for investment should be received and any allotments should be made, in each case from outside of Bahrain. This document has been prepared for private information purposes of intended investors only who will be institutions. No invitation shall be made to the public in the Kingdom of Bahrain and this document will not be issued, passed to, or made available to the public generally. The Central Bank (CBB) has not reviewed, nor has it approved, this document or the marketing of such securities, derivatives or funds in the Kingdom of Bahrain. Accordingly, the securities, derivatives or funds may not be offered or sold in Bahrain or to residents thereof except as permitted by Bahrain law. The CBB is not responsible for performance of the securities, derivatives or funds.

State of Kuwait

This document has been sent to you at your own request. This presentation is not for general circulation to the public in Kuwait. The Interests have not been licensed for offering in Kuwait by the Kuwait Capital Markets Authority or any other relevant Kuwaiti government agency. The offering of the Interests in Kuwait on the basis a private placement or public offering is, therefore, restricted in accordance with Decree Law No. 31 of 1990 and the implementing regulations thereto (as amended) and Law No. 7 of 2010 and the bylaws thereto (as amended). No private or public offering of the Interests is being made in Kuwait, and no agreement relating to the sale of the Interests will be concluded in Kuwait. No marketing or solicitation or inducement activities are being used to offer or market the Interests in Kuwait.

United Arab Emirates

Deutsche Bank AG in the Dubai International Financial Centre (registered no. 00045) is regulated by the Dubai Financial Services Authority. Deutsche Bank AG - DIFC Branch may only undertake the financial services activities that fall within the scope of its existing DFSA license. Principal place of business in the DIFC: Dubai International Financial Centre, The Gate Village, Building 5, PO Box 504902, Dubai, U.A.E. This information has been distributed by Deutsche Bank AG. Related financial products or services are only available to Professional Clients, as defined by the Dubai Financial Services Authority.

State of Qatar

Deutsche Bank AG in the Qatar Financial Centre (registered no. 00032) is regulated by the Qatar Financial Centre Regulatory Authority. Deutsche Bank AG – QFC Branch may only undertake the financial services activities that fall within the scope of its existing QFCRA license. Principal place of business in the QFC: Qatar Financial Centre, Tower, West Bay, Level 5, PO Box 14928, Doha, Qatar. This information has been distributed by Deutsche Bank AG. Related financial products or services are only available to Business Customers, as defined by the Qatar Financial Centre Regulatory Authority.

Kingdom of Saudi Arabia

Deutsche Securities Saudi Arabia LLC Company, (registered no. 07073-37) is regulated by the Capital Market Authority. Deutsche Securities Saudi Arabia may only undertake the financial services activities that fall within the scope of its existing CMA license. Principal place of business in Saudi Arabia: King Fahad Road, Al Olaya District, P.O. Box 301809, Faisaliah Tower - 17th Floor, 11372 Riyadh, Saudi Arabia.

IMPORTANT INFORMATION – APAC

Although the information herein has been obtained from sources believed to be reliable, we do not guarantee its accuracy, completeness or fairness. Opinions and estimates may be changed without notice and involve a number of assumptions which may not prove valid. We or our affiliates or persons associated with us or such affiliates. ("Associated Persons") may (i) maintain a long or short position in securities referred to herein, or in related futures or options, and (ii) purchase or sell, make a market in, or engage in any other transaction involving such securities, and earn brokerage or other compensation.

The document was not produced, reviewed or edited by any research department within Deutsche Bank and is not investment research. Therefore, laws and regulations relating to investment research do not apply to it. Any opinions expressed herein may differ from the opinions expressed by other Deutsche Bank departments including research departments. This document may contain forward looking statements. Forward looking statements include, but are not limited to assumptions, estimates, projections, opinions, models and hypothetical performance analysis.

This document may not be reproduced or circulated without our written authority. The manner of circulation and distribution of this document may be restricted by law or regulation in certain countries

This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction, , where such distribution, publication, availability or use would be contrary to law or regulation or which would subject Deutsche Bank to any registration or licensing requirement within such jurisdiction not currently met within such jurisdiction. Persons into whose possession this document may come are required to inform themselves of, and to observe, such restrictions.

Unless notified to the contrary in a particular case, investment instruments are not insured by the Federal Deposit Insurance Corporation ("FDIC") or any other governmental entity, and are not guaranteed by or obligations of Deutsche Bank AG or its affiliates.

IMPORTANT INFORMATION – UNITED STATES

For purposes of ERISA and the Department of Labor's fiduciary rule, we are relying on the sophisticated fiduciary exception in marketing our services and products through intermediary institutions, and nothing herein is intended as fiduciary or impartial investment advice.

IMPORTANT INFORMATION – SWITZERLAND

This material is intended for information purposes only and does not constitute investment advice or a personal recommendation. This document should not be construed as an offer to sell any investment or service. Furthermore, this document does not constitute the solicitation of an offer to purchase or subscribe for any investment or service in any jurisdiction where, or from any person in respect of whom, such a solicitation of an offer is unlawful. Neither Deutsche Bank AG nor any of its affiliates, gives any warranty as to the accuracy, reliability or completeness of information which is contained in this document. Past performance or any prediction or forecast is not indicative of future results. The views expressed in this document constitute Deutsche Bank AG or its affiliates' judgment at the time of issue and are subject to change. Deutsche Bank has no obligation to update, modify or amend this letter or to otherwise notify a reader thereof in the event that any matter stated herein, or any opinion, projection, forecast or estimate set forth herein, changes or subsequently becomes inaccurate, or if research on the subject company is withdrawn. Prices and availability of financial instruments also are subject to change without notice.(to Article 10 paragraph 3 of the Swiss Federal Act on Collective Investment Schemes (CISA) and Article 6 of the Ordinance on Collective Investment Schemes. This document is not a prospectus within the meaning of Articles 1156 and 652a of the Swiss Code of Obligations and may not comply with the information standards required thereunder. This document may not be copied, reproduced or distributed or passed on to others without the prior written consent of Deutsche Bank AG or its affiliates.

IMPORTANT INFORMATION – NORDICS

Deutsche Bank AG is authorized under German banking law (competent authority: European Central Bank and the BaFin, Germany's Federal Financial Supervisory Authority. Deutsche Bank Branches operates within the EEA on the back of the legal entity (Deutsche Bank AG) EU Passports within the European Economic Area ("EEA"). Reference is made to European Union Regulatory Background and Corporate and Regulatory Disclosures at https://www.db.com/en/content/eu_disclosures_uk.htm. Details about the extent of our authorization and regulation by BaFin are available from us on request." This presentation is for information purposes only and is not intended to be an offer or an advice or recommendation or solicitation, or the basis for any contract to purchase or sell.