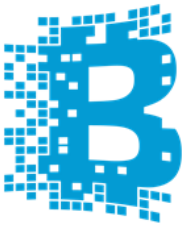
WHITE PAPER
May 2016
For professional investors

ROBECO
The Investment Engineers

Distributed ledger technology for the financial industry

Blockchain administration 3.0

ethereum



BLOCKCHAIN

HYPERLEDGER PROJECT

Jeroen van Oerle
Patrick lemmens

TABLE OF CONTENTS

Executive summary

Distributed ledger technology, also known as blockchain, has been gaining a lot of attention lately. This technology forms the underlying infrastructure of a cryptocurrency called Bitcoin. Thanks to the open architecture of blockchain's programming code, many alternative use cases are being developed rapidly. Within the financial sector we see most resources being invested by banks, which have formed a consortium in R3CEV. We view this technology as an enabler of efficiency gains and dubbed it 'administration 3.0'. Although disruptive use cases are theoretically possible, we think an evolutionary sustaining innovation trajectory is the most likely path of development for blockchain. As with other technology, a pre-condition for survival of incumbents is technological competence and a proactive attitude.

Hyped, but here to stay

We think the technology is currently being hyped, as witnessed by large investment flows from private investors. At the same time, we are convinced that this technology is here to stay in the long run. The technology is currently in its infancy stage and there are several challenges to overcome before mass adoption is possible. Regulatory and technical issues are most decisive. In this report we argue there is a need for standardization to overcome hurdles, which we believe is best accomplished through the creation of consortia that include all relevant stakeholders.

Evolutionary, not revolutionary

In this report we lay out the idea behind distributed ledger technology and the powerful combination of blockchain with smart contracts. After having established what the technology is and how it can be used, we dig deeper into use cases within banking, insurance and asset management. We think blockchain technology will have a large impact on the financial sector. Still, we believe the rollout will be evolutionary rather than disruptive given the high level of regulation in the financial sector. We think this allows incumbents to react to the new technology and find ways to incorporate it into their current IT systems. We don't think there will be only one version of blockchain, which allows for customization within specific industries.

Winners and losers

We believe it is too early to identify clear winners. A comparison can be made to the music industry where Napster was the first company that enabled large scale online distribution of music, but Spotify emerged as leader. We argue the same can hold true for blockchain. Focus should be on distributed ledger technology in our view. Who will eventually offer this distributed ledger technology is of lesser importance for now. In terms of losers, we argue that companies in the 'quick win' areas are most at risk. Blockchain technology can make quick wins in labor intensive, costly and lengthy processes. Companies operating in such environments should be pragmatic with regard to blockchain implementation.

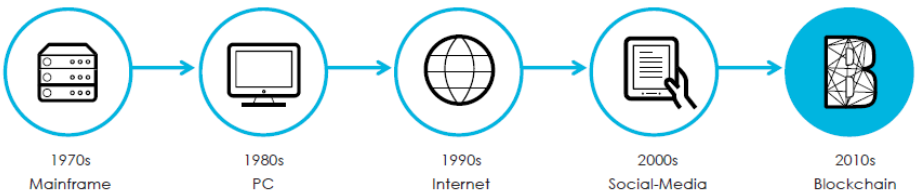
Introduction

Distributed ledger technology is gaining popularity fast. Blockchain, the best known example of a distributed ledger, might be highest on people's swear-jar list due to its daily cheerleading in all kinds of news outlets, while to others it is still a vague or unknown concept. The actual path of development is best summarized by Amara's law: "We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run." Perhaps it is hyped now, but potentially efficiency-disruptive in the long run.

Administration 3.0

We view the developments in distributed ledger technology as important efficiency gains and therefore dubbed it 'administration 3.0'. We think of administration 1.0 as paper format ledgers. Administration 2.0 is in our view the transition from paper to digital ledgers. Thanks to new technology we are now moving to administration 3.0, which is a decentralized distributed ledger. This decentralized feature is an extremely important concept and is in our view going to fuel a new wave of efficiency innovations. Although this might be disruptive to some, we think the overall impact of this new technology will be positive to incumbents. Banks, insurance companies and asset managers have the ability to reduce their cost-base substantially by using blockchain technology. Although we will focus on the implications of distributed legers for the financial industry, the use cases for other industries are growing by the day. Technical challenges and regulation form barriers to implementation though, which is why we expect an evolutionary development path.

In this paper we describe the distributed ledger technology and applications. We then take a closer look at the impact on banking, insurance and asset management. When talking about distributed ledgers, we often automatically use the word blockchain. There are two important points to remember for the rest of this paper. Firstly, the real innovation is distributed ledger technology and the applications that are being developed around it (smart contracts). Blockchain is an example of a distributed ledger, but not necessarily the only one nor the final surviving one. Throughout this paper we will use both words interchangeably, though. Secondly, blockchain technology was developed as the underlying technology of a cryptocurrency concept named Bitcoin, but meanwhile has developed far beyond its initial use. In its current form, Bitcoin is one of many applications of blockchain. We will focus on distributed ledger technology and not on cryptocurrencies.



Distributed ledger technology

Distributed ledgers allow for decentralized databases

A distributed ledger is a database that keeps track of who owns a specific asset. This asset can be physical or electronic. Examples are diamonds, real estate, land, shares, currency, etc. Up until this point there is no difference to an electronic centralized ledger that might already be used by companies. An essential feature of the new technology is that it is distributed. Every participant can keep a copy of the ledger which is updated automatically when new transactions occur. The best known example of such a distributed ledger technology is blockchain. Block chain is the underlying ledger technology behind Bitcoin, a cryptocurrency. All Bitcoin transactions are processed and recorded on the Block chain. Literally every Bitcoin transaction ever made is recorded and can be traced. Not necessarily traced to people, but traced to accounts. A more detailed description of a typical Bitcoin transaction can be found in appendix A.

Trustless system that overcomes two key issues with digital asset transfers

The blockchain has become such an important feature of Bitcoin because it stands as a trustless proof mechanism. An issue with digital currency (or the digital transfer of assets in general) is that of 'double spending', which can result from the fact that centralized ledgers have not been updated on time. Instead of transferring the asset, a worthless copy is transferred while the original asset is maintained in the own account. The traditional way to mitigate this risk is to use trusted third parties (e.g. a bank) to act as centralized authority, or use cash. Blockchain technology, however, has shifted this trusted third party role to the whole network instead of a centralized party.

A related computing challenge is the 'Byzantine General's problem', which occurs when several stand-alone decision makers need to cooperate in a trustless communication system. It could happen that one node in the system makes a false claim to approve a transaction, after which the other nodes react to that false claim by also approving the transaction. The ground-breaking solution to these key issues comes from cryptography. Through a process called 'mining', or 'proof of work', mathematical puzzles need to be solved in order to come to a consensus about the state of the underlying data. Only if there is consensus, is the transaction added to the network. As this transaction cannot be changed, nor canceled, blockchain is permanent and immutable.

Main properties of distributed ledger technology

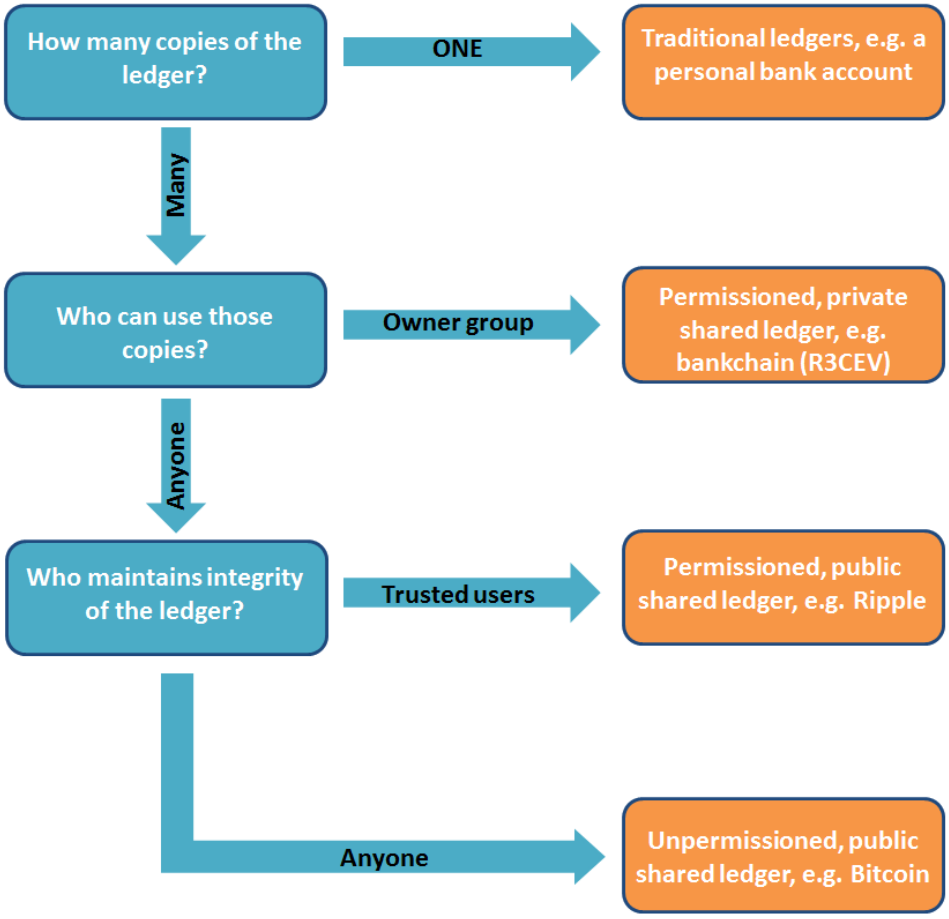
There are four important properties of distributed ledger technology:

1) Reconciliation through cryptography
2) Availability of many copies
3) Granular access control (view keys for regulators and validating keys for miners)
4) Irreversibility; to prevent tampering with previous transactions

Permissioned versus unpermissioned and public versus private

Whereas Bitcoin is an unpermissioned, public distribution method there are alternatives that only allow certain groups to enter the blockchain data. These are called private ledgers as can be seen in figure 1. In addition to the right to actually see copies of the ledger information, a validation overlay can also be used. In Blockchain everyone can become a validator by means of installing enough computing power to participate in the proof of work process. Alternatively, only permissioned parties are allowed to validate. We think the most likely application for the financial sector will be a permissioned blockchain. We think consortiums within banking, insurance and asset management will maintain the ledger and, in cooperation with regulators, allow members to participate.

Figure 1. Public versus private and permissioned versus permissionless systems



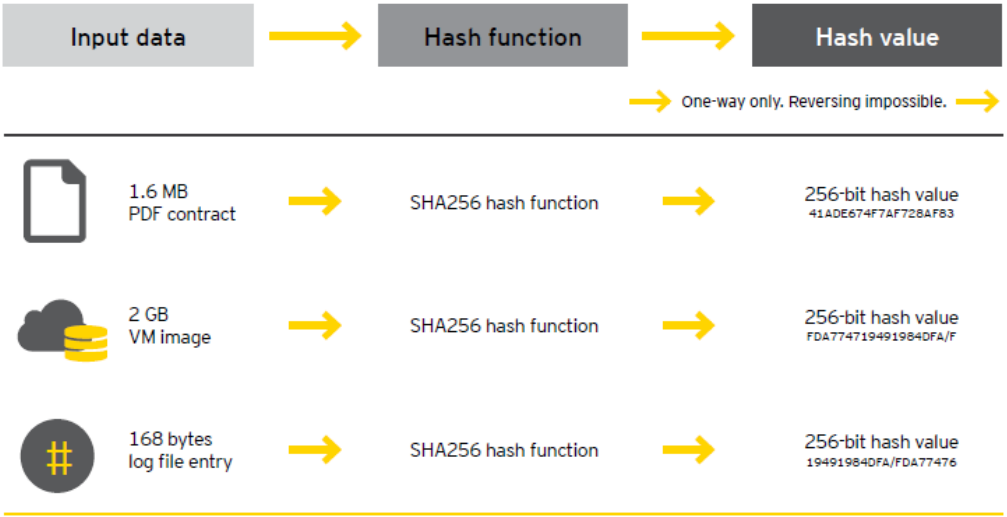
Source: Dave Birch (2015), Robeco

Hashing is an essential feature of blockchain

Hashing and timestamping are key functions of blockchain technology. Hashing is the process of running a computer algorithm over content in order to create an alphanumeric character that cannot be back-computed into the original content. It allows validating a claim and determining sequential priority. A hash is always the same if the underlying asset has not changed. Hashing only works one-way. This implies it is not possible to trace back what the hash represents from validating the transaction. A miner can only validate the transaction and ownership of the asset, without knowing what the asset actually represents (could be 1 USD but also a diamond or a car insurance document). As can be seen in figure 2, hashing can be done with documents of all sizes. This is important

because the size of the underlying document does not impact the ability to be added to the blockchain. When using the SHA256 protocol for hashing, as in Bitcoin, the size of the hash code that is added to the blockchain is only 32 bytes. Hashing is also used to validate blocks in the blockchain using a so called 'Merkle tree' validation pattern. If a previous block is altered, the hash changes and does not match anymore with the latest available hash value. This way, it is avoided that previous blocks are tampered with.

Figure 2. Hashing function in blockchain



Source: EY, 2016

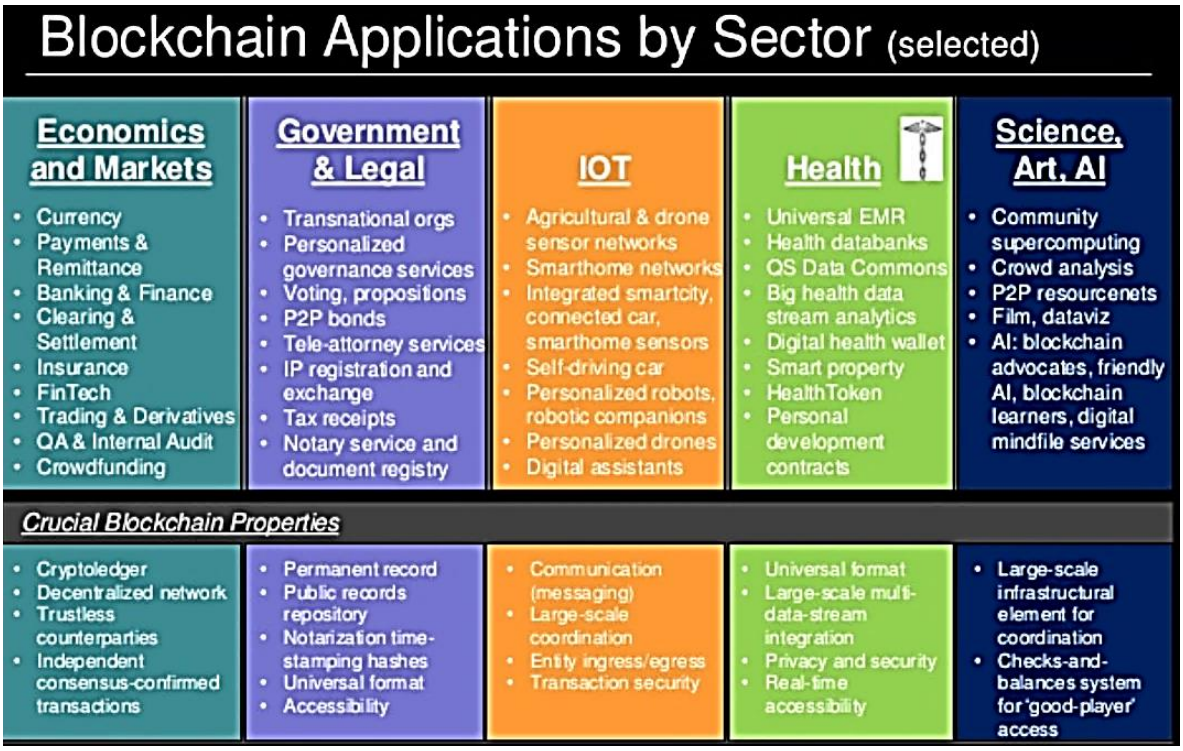
Blockchain 1.0, 2.0 and 3.0

The literature discusses three versions of blockchain[1]:

- Blockchain 1.0 is currency and refers to the deployment of cryptocurrencies in applications related to cash such as digital payments and remittance. The best known example of blockchain 1.0 is Bitcoin, but there are over two hundred cryptocurrencies. This number grows exponentially as governments are exploring the concept. Poland has issued its own cryptocurrency, which is backed by the zloty and the regulator[2].
- Blockchain 2.0 is contracts and refers to all the financial applications that are being built on the blockchain technology other than the transfer of currency. Examples are stock or bond transactions and mortgages. This is where most attention goes to at the moment.
- Blockchain 3.0 is applications beyond currency and finance. Blockchain 3.0 refers to a very diverse set of use cases, of which a selection is shown in figure 3.

[1] Swan, 2015
[2] Billon, 2016

Figure 3. Blockchain applications by sector



Source: USF, 2015

Blockchain is neither Bitcoin nor one single version

It is important to understand that blockchain technology was first used to run the Bitcoin application on top of it, but is not necessarily linked to the cryptocurrency. Blockchain technology can indeed work with a version that relies on the features of Bitcoin (blockchain 1.0), but there are many alternative methods to use blockchain technology.

Bitcoin has received negative attention because of the link to criminal activities. Due to its anonymity the technology is a preferred method of payment for illegal transactions. Although this is indeed true, we would like to use an analogy to nuclear power. The process of splitting atoms can be used to create nuclear power, but also to create a nuclear bomb. This does not make the process of splitting atoms a criminal invention, but what you do with the technology determines its impact. For a long time, blockchain and Bitcoin were intertwined, but now that the two concepts are separated, it is possible to create alternative use cases. Another important thing to remember is that there is not one single blockchain. There are many blockchain applications and it is not likely we will ever end up with a single blockchain.

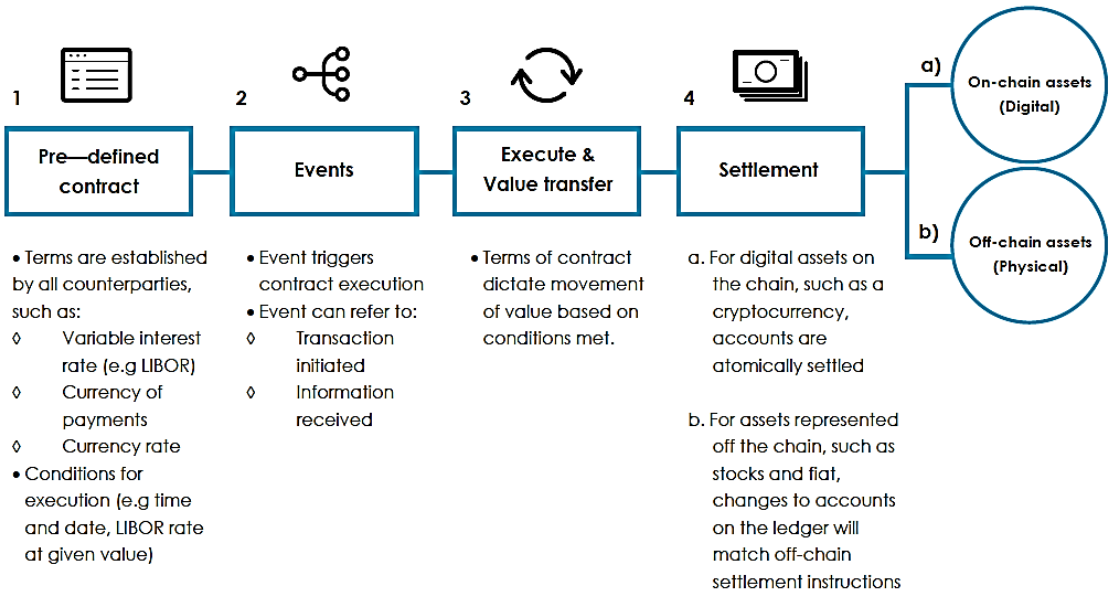
Smart contracts open up a whole new range of opportunities

Although blockchain 1.0 could lead to efficiency gains related to the transfer of money, blockchain 2.0 (and 3.0) is the truly big efficiency gain promise. A vital piece of this efficiency gain puzzle is provided by a concept called smart contracts. A smart contract is a method of using cryptocurrency to form agreements with people (or machines) via the blockchain. The contract is autonomous. Once it is specified and running there is no need for anyone to still routinely check that process. Next to being autonomous, smart contracts are self-sufficient, which implies they do not depend on funding from their originator. Thirdly, smart contracts are decentralized thanks to the blockchain because they are no longer stored on one central database.

Simplified example of a smart contract

Most smart contracts currently run on Ethereum, which is an alternative to the Bitcoin blockchain. Figure 4 shows the process of creating a smart contract. In order to make smart contracts less abstract we use the simplified example of mini-bonds as currently tested by UBS[3]. The issuer of the bond makes up a smart contract (or has a law firm make up a smart contract) that specifies at what dates coupon payments are made, for what amounts and how/when repayments occur. This smart contract is connected to the blockchain and buyers can allocate money to the bond by paying cryptocurrency to the address of the bond (which is separate from the issuer address). The bond keeps this money in escrow and when completely filled, the smart contract with all its terms is activated. If the bond is oversubscribed or undersubscribed, rules will determine how the money is redistributed. After the bond goes live, the smart contract triggers payments of coupons on all coupon dates without the need for manual inputs and the value of the bond is transferred to the issuer. The bond has rights to withdraw money from the issuer's bank account in order to fulfil the coupon payments. Because the contract is on blockchain, the validity of the bond's authority to request a withdrawal from the issuer's bank account is guaranteed.

Figure 4. Smart contracts on Ethereum



Source: Evry labs, 2015

Large cost savings potential

The impact of execution automation should not be underestimated. This could lead to substantial cost savings on personnel and administration. In most cases, this is exactly the reason for investigating the possibilities of blockchain: the potential cost savings rather than the technology.

Dapps, DAOs, DACs, DASs: autonomous smart contracts

The first use cases of smart contracts are simple. We expect to see a couple of implementations using smart contracts in the coming years in order to test how they hold up in the 'real world' and how they must be regulated. Technological development,

[3] Batlin, 2016

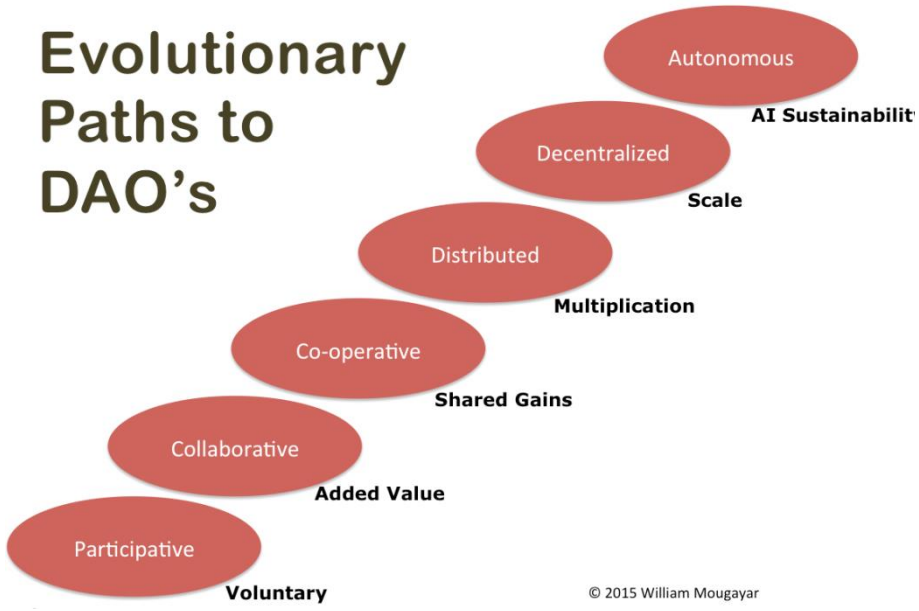
however, is not waiting for this to happen and has already moved on to the next step. Over time, smart contracts could become very complex and autonomous.

Dapps, DAOs, DACs and DASs are all abbreviations of decentralized operations. Dapp is an application that runs on a network in a distributed way with a decentralized operating model via smart contracts. One can think of the decentralized Twitter (Twister and Gems) where information is not stored centrally, but maintained (in encrypted form) on a distributed ledger. DAO, DAC and DAS stand for decentralized autonomous organization, corporation and society respectively. They allows applications to become corporations and run fully autonomously. Examples are vending machines that have their own bank account and order new drinks if the machine runs out of inventory. Because the soft-drink machine is a verified entity on the blockchain and the cryptocurrency it holds in the wallet is verified, the ordering of the soft-drink as well as the actual delivery can refer back to the machine's status on the blockchain. In a theoretical example, once the soft drink machine has enough money on its bank account for inventory, it could order another soft drink machine and deploy that machine in a place where there is demand for soft-drinks.

The start of an autonomous world?

That same line of thinking has been applied to taxi services (combined with autonomous driving) and many more possible decentralized autonomous business models that now have a tool for trusted transactions in a trustless payment environment. Although a deeper discussion goes beyond the scope of this paper, it is a good example of how transformative this technology really is and how powerful the combination of a smart contract and the blockchain can be, in theory. We think these kinds of applications will only become reality in the long run. We think the focus should be on the implementation of simple smart contracts for now in order to realize cost savings.

Figure 5. DAO's evolutionary path boosted by blockchain



Source: William Mougayar, 2015

Distributed ledgers in banking

Now that we know what distributed ledger technology is, we will discuss the impact on banking, insurance and asset management. We argue banks are currently most advanced in their exploration of blockchain technology. R3CEV is a consortium which currently exists of 42 members[4] from different parts of the world. This consortium is testing blockchain applications for banking and aims to create a blockchain standard. Cooperation with national regulators is also high on the agenda. We see opportunities for banks in the areas of trade, (international) payments, regulatory compliance (KYC/AML) and structured investment products.

Figure 6. R3CEV participants

Source: R3CEV

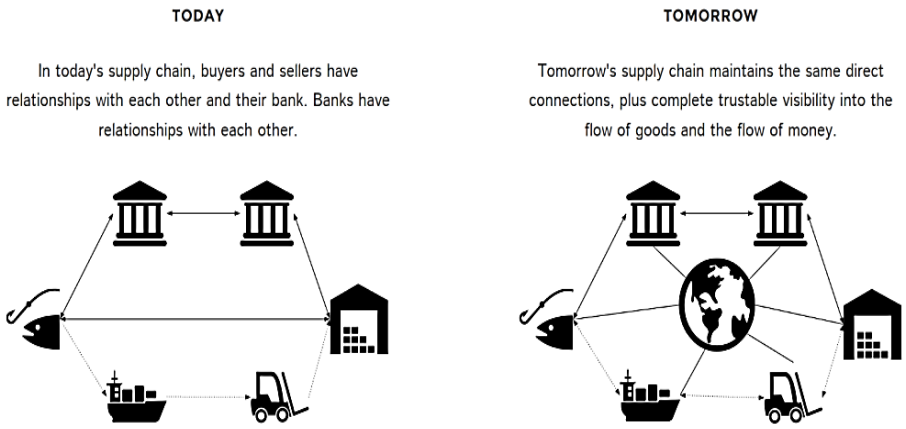
Large efficiency gains in trade

There are three ways to settle a payment. Either through an open account, a letter of credit or through supply chain financing. Open accounts are used in eighty percent of all payments. Typically the buyer settles the amount within a 30 to 60 day period. The level of trust must be high in these transactions. Of the other twenty percent of payments, about half is done through a letter of credit. This service is typically used for the trade of very valuable assets. A lot of parties are involved and every participant has to use its own ledger and reporting processes to initiate the next step in the process. The same goes for supply chain financing, which makes up the other half of non-direct payments. Here, the bank is replaced by companies within the supply chain. In sum: the current process is very lengthy, takes a lot of paperwork and man-hours and does not directly generate profit to banks (especially when taking into account capital requirements by regulators).

[4] As of December 2015

Alternatively, by means of using the blockchain in combination with smart contracts, all the issues around paperwork and centralized ledgers can be solved. Also the issue of trust is solved because the blockchain acts as escrow service. The buyer pays money into the smart contract and this money is transferred to the seller if it is established that the buyer indeed received the goods. The European Commission is working on a mandatory e-invoicing law, which requires the documents in the trade process to be electronic by 2018. At the moment only about ten percent of invoices are electronic. This is estimated to reduce the trade process to ten days and will be a substantial efficiency gain. However, when combined with distributed ledger technology, the benefits can potentially be bigger. The combination with IOT (internet of things) is also often mentioned. Once a container is loaded on a boat, the smart contract can initiate (partial) payment to the seller. A startup that is using blockchain to make a letter of credit is Skuchain (named after SKU stock keeping unit). Estimated cost savings are USD 20 billion per year by 2022[5].

Figure 7. Trade before and after distributed ledger technology



Source: Skuchain.com

Payments only partially impacted by blockchain

The large efficiency gains as described under the trade applications of blockchain are only partially possible in payments. The payment processes in developed markets are very efficient and fast. Often, it is regulation rather than technology that reduces speed and efficiency. Although we do not think the current payment systems will be impacted by blockchain developments in the coming years, we would like to indicate the theoretical applicability.

A payment consists of two separate functions. One is a message (usually transferred via SWIFT) and one is the transfer of money. Messages sent via SWIFT are very fast, but they are one-way only. Often, manual input mistakes result in wrong messages which require a lot of administrative work to correct. In a separate transaction, the money is transferred from one bank to another. If this is done within a country, the central bank deposits of both banks will be debited and credited accordingly. If the transfer is done internationally, the correspondent banking process is used, which is shown in figure 8.

[5] Santander, 2015

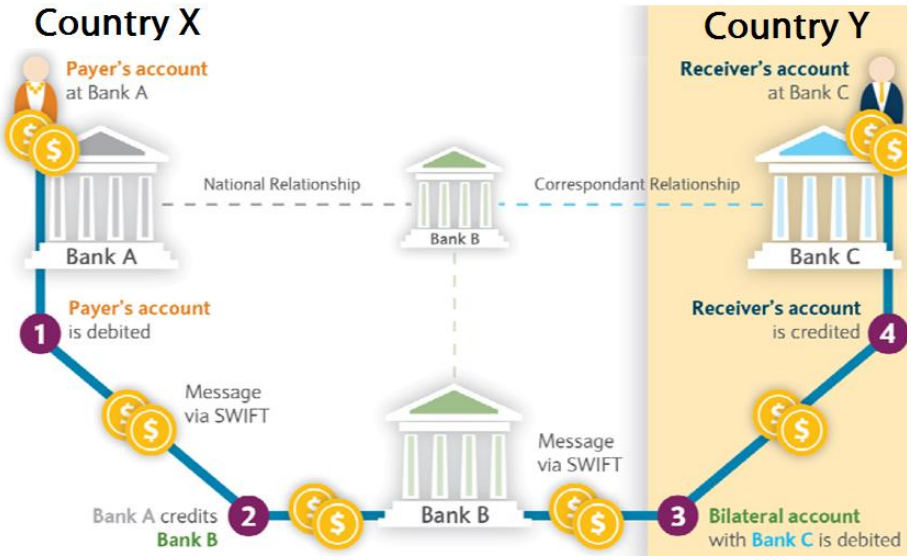
Several countries have initiated faster payments. Fedwire and Target2 are used for gross settlement in dollars and euros respectively. Banks need to hold enough capital to enable these real time payments. As a result, this technique is only used for high transaction volumes. Low value, high volume transactions are batched and netted through networks like ACH. This usually takes between one and two days. Blockchain combines messaging and transfer of money. The real gain is therefore not speed (because it can be done through gross settlement), but the added value would be in reducing administration costs, administration mistakes and counterparty risk, which potentially leads to a reduction in capital requirements. Blockchain in payments is therefore more about cost benefits than technical improvements.

Blockchain has the potential to disrupt correspondent banking

Although inter-country payments are currently very efficient, international payments are less so. Due to a lack of trust and high costs to be compliant with local regulation, correspondent banking has become an important tool for cross-country settlement. This tool is an expensive one though for customers, but also for Tier-3 banks that deal with international payments on a less frequent basis. Blockchain can combine messaging and transfer of money as explained above, but for international transactions this would require an international cryptocurrency. Bitcoin is an example, but it is a rather poor idea to use it for international settlement from a stability perspective. There is no guaranteed fiat conversion rate yet within Bitcoin. Ripple is the most advanced startup in this field.

National central banks could launch an international cryptocurrency which is backed by local currency. Although that seems far away, Polish banks have launched a cryptocurrency (in cooperation with Billon) that is backed by the zloty. The UK and Australian regulators are also well advanced in researching the possibilities of cryptocurrency. We expect to see examples of international cooperation on this topic soon.

Figure 8. Current correspondent banking system



Source: Barclays, 2016

KYC and AML via the blockchain

Money laundering and the financing of terrorist activities are high on the agenda of governments. In order to curb illegal money transfers, banks have to comply with an increasingly extensive set of rules. Know your customer (KYC) and anti-money laundering

(AML) compliance was estimated to cost around 10 billion US dollars in 2014[6]. In addition to the costs, the KYC process is also very lengthy. KYC requests can take between 30 and 50 days to complete at a satisfactory level and involve a lot of double work at different organizations.

Blockchain enables customers (either retail or corporate) to create a verified profile. Every time KYC information is required, the document on the blockchain can be used as a confirmation of identity. Although SWIFT has already launched a program that entails centralizing KYC information by means of aggregating data from participating banks, it is not in the same safe format as blockchain. Fraudsters only need to concentrate on breaching this centralized database in order to change the required documents, a process that is not possible on blockchain. Well known start-ups in this area are Tradle and Factom, but there are many more examples of companies working on this. Having a decentralized KYC document is better for customers (because they don't need to fill out the same information over and over again) as well as banks (because of cost reductions). This can make the continuous AML process a lot more cost efficient.

Investment banking products on blockchain

Recently a group including Bank of America Merrill Lynch, Citi, Credit Suisse, Markit and DTCC completed their first trial of a credit default swap that was fully traded via the blockchain. This CDS got its own wallet address, just as with the mini-bond example on page 8, and a smart contract written on top dictated the conditions for payment. A company that is concentrating on investment banking applications and post-trade financial services is Digital Asset Holdings, which is run by Blythe Masters, a former executive at JPMorgan Chase. It is clear that the efficiency gains on the investment banking operations are very large. New products that were previously not profitable due to the large amount of administrative costs relative to the revenue potential are currently becoming available, opening up for mass market consumption.

Blockchain technology requires business model adaptation

The introduction of blockchain technology can also have an impact on business models. Currently, a lot of banks offer a complete range of products and are sometimes vertically integrated in order to manage the process better. We think the modular nature of blockchain technology allows banks to look critically at their service offering and spin-off unprofitable business units, without the risk of losing other parts of their service offering . Administration, KYC and AML are examples of critical inputs in the current process, but can become modular inputs once standardized blockchain applications have been developed. There is less risk of IT legacy issues in this new environment. A pre-condition is a high level of standardization though. It will be interesting to see how incumbents deal with this business model change, as it will become even easier for new companies to start banking services once regulatory approval is granted.

[6] Deloitte, 2016

Distributed ledgers in insurance

The opinion on distributed ledger technology in insurance can be summarized into three classes. One group believes there is no impact of blockchain technology because the industry can already make use of the latest technology (like telematics) in order to make the process more efficient and does not need blockchain. Another group sees blockchain as efficiency increasing and the third group looks at blockchain as an opportunity to completely disrupt business models for the insurance sector. The theoretical possibilities for blockchain within the sector are large. An example of a company that uses this technology is Everledger (in cooperation with Allianz and Aviva), which registers diamonds to trace ownership. We see developments in the range of fraud reduction by means of using IOT in digital claims handling and P2P insurance. We will discuss these topics in more detail below. We think administration 3.0 is much needed in the insurance industry and expect cost reducing implementations first, with the more exotic applications (and perhaps disruption) being developed at a later stage.

Cost efficiency and fraud reduction needed in insurance

Administrative cost leakage is high in the insurance sector. It is estimated that for every unit of premium, 25 percent is spent on distribution and administration, with another 5 percent on costs of handling claims[7]. This implies only 65 percent of premiums actually goes to the funding of claims. Of these claims, a significant percentage is fraudulent. Especially within healthcare insurance, fraud is big. In a report by the World Health Organization, global health care insurance fraud was estimated to be USD 260 billion in 2015. In the US alone, USD 80 billion is lost on fraudulent Medicare claims per year[8]. Most of the fraud starts with the creation of fake IDs. Insurance fraud includes more than just healthcare though. Diamonds, expensive paintings, car insurance and casualty insurance are key targets of fraudsters.

Reducing fraud via blockchain and smart contracts

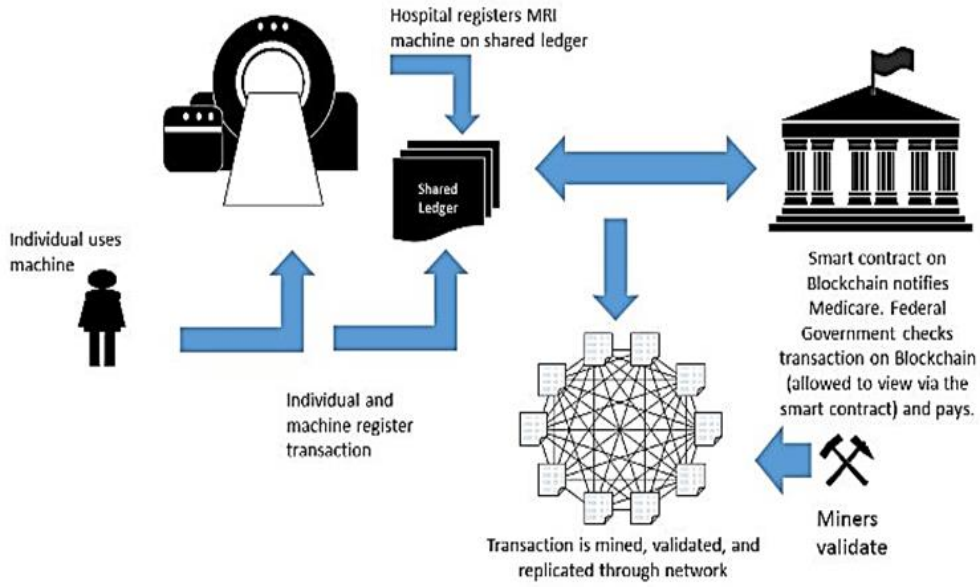
Blockchain enables the decrease in fraud because fake IDs, 'stolen' property and many other tricks in the books of fraudsters now need to be validated not only by an insurance agent, but also by the community of blockchain users. Trying to create a false insurance claim using a false ID is virtually impossible, because that fake ID will not be accepted by the blockchain participants. And if it were accepted, the claim would also need to be accepted in a separate validation process. By means of combing smart contracts and IOT technology, it is much easier to check those claims, as shown in figure 9.

If a patient claims he has gone through a scanner, the scanner (as well as a doctor) has to validate that transaction on blockchain. Only if all parties agree, is it put in the shared ledger, after which the insurance pays out the costs to the relevant parties. If a hospital claims a patient went through the scanner without the verification from that patient, it is simply not added to the ledger. Also, if the patient claims he went through the scanner, without the machine actually validating that action, it is not added to the ledger and there is no pay-out. We think that having the optionality to trace asset transactions and ownership via blockchain will revolutionize insurance.

[7] Barclays, 2016

[8] Coalition Against Insurance Fraud, US 2015

Figure 9. Health insurance application via blockchain



Source: Adams, 2015

P2P insurance; disruption via blockchain

A more radical thought is to apply blockchain technology in P2P insurance. The first protocols have already been developed and are in the proof of concept phase. The idea is that via smart contracts, people form their own insurance consortium (a DAO) and all become shareholders next to being policy holders. There is a clear separation between people who can accept new policy holders and people who can approve claims, and IOT technology is used as validation input.

The first applications that are tested are based on the simplest form of insurance; delayed flights. Delayed flights are publicly recorded, so no judgment or individual assessment is required when a claim comes in. Upon the event, a smart contract is triggered and the pay-out to the policyholder is made. This is fully automated and no claim processing costs with expensive manual back office labor are required.

Another example is car windshields. The costs of replacing a windshield are about 350 dollars, irrespective of car brand. Policyholders validate a windshield that needs to be replaced by means of chips in the window of the car and combine ledger information from the garage holder to validate the windshield was indeed replaced. Once the windshield has been replaced, the smart contract transfers money to the policyholder. No intermediaries are needed in the back office of the insurance consortium.

This type of insurance will work on all policies whose pay-out conditions are objective and can be captured in a smart contract. When insurance becomes more complex, pricing risks become higher and subjective claim assessment becomes more important. This reduces the technology's applicability. We think P2P insurance DAOs have the potential to become reality, but only for easy to understand and highly commoditized insurances. We do not think P2P insurance is able to price more complex insurance products and the risk of plan-wipeout due to a mega-claim will hold back regulators. Examples of P2P insurance are Friendsurance in Germany (where moral hazard is reduced by forming groups of friends instead of anonymous policy holders), Lemonade (US), Guevara (UK) and Inspeer (France).

Distributed ledgers in asset management

We see very clear use cases for blockchain technology in asset management, but just as with payments, a distinction needs to be made between processes that are already very efficient and processes that need improvement. Within the asset management industry trading in publicly listed companies works very efficiently and fast with the current technology. The post-trade process and private company trading are totally different though. The post-trade process currently takes about two days to complete. Distributed ledger technology enables a large efficiency gain in the after-trade process. We argue it makes little sense to go after actual trading process innovations at this point in time.

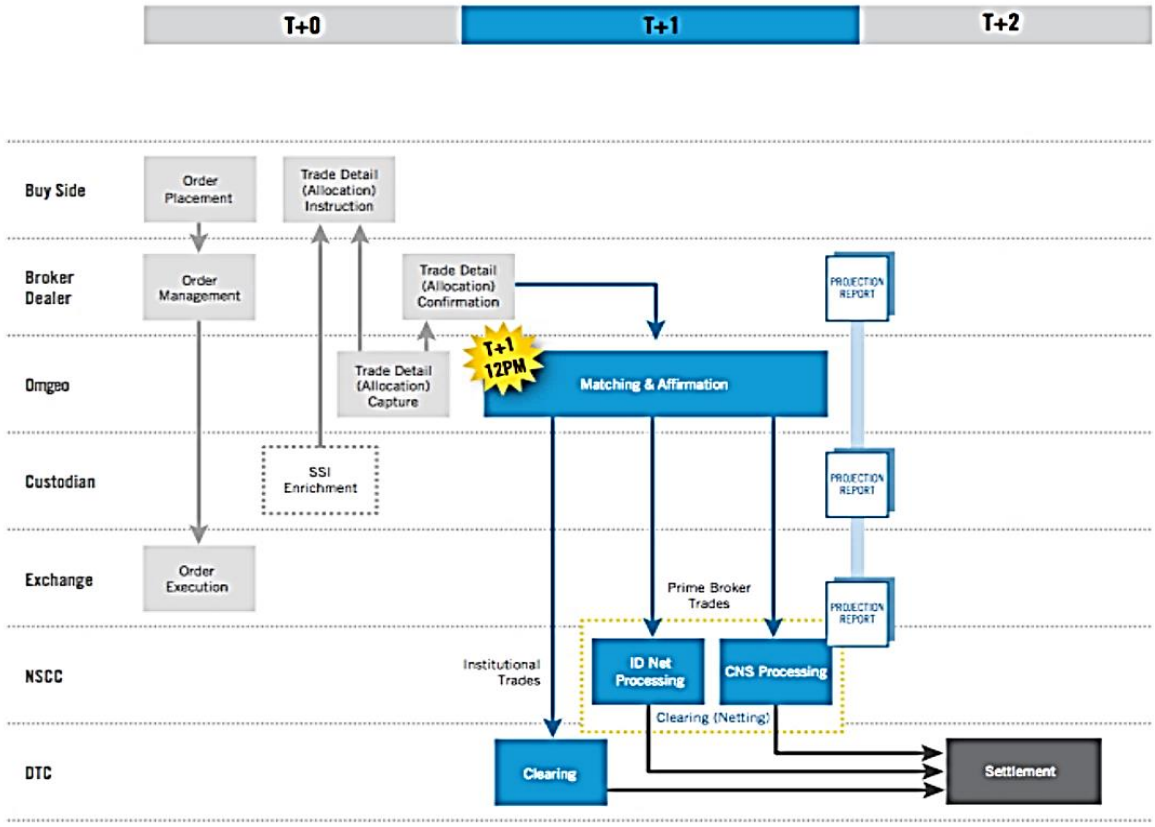
Asset management industry needs a consortium

The consortium structure within the banking industry (R3CEV) is important for standard-setting. The sooner there is a standard, the more focused new developments will be. Within the asset management industry, there is no such consortium yet. There is a risk that multiple projects will eventually not be compatible and that the lack of standards will hold back innovation. Service providers (like the exchanges and custodians) are already working on distributed ledger technology, but it would make sense (also from a strategic perspective) to form a consortium including asset managers and service providers.

T+2 settlement results from pure administrative delay

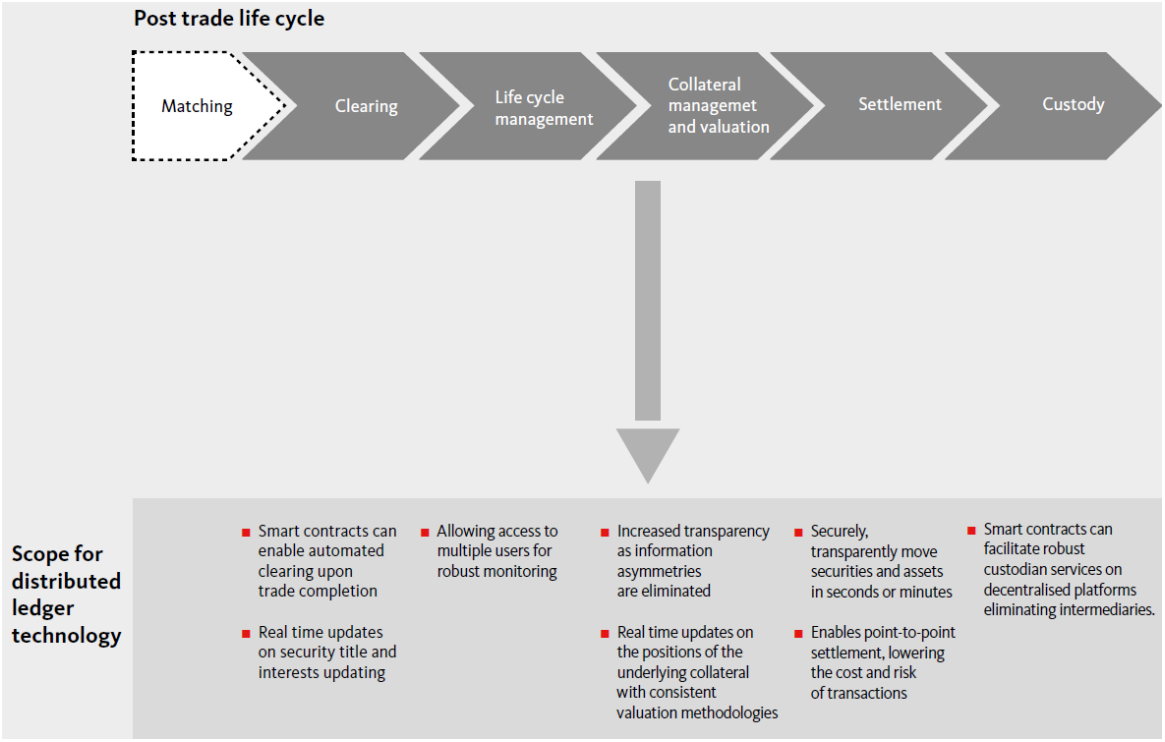
As can be seen in figure 10, the post-trade process involves a lot of steps with different parties involved. All of these intermediaries keep their own records. Updating the entire ledger and sending that information back to the buyer of the asset takes two days at best, but in some countries it takes longer. This does not only create annoyance due to the fact that records are not up-to-date, it is also very costly. As figure 11 shows, blockchain technology can take all the intermediaries with their centralized ledgers to one common ledger which speeds up the process dramatically. When placing smart contracts on top of the decentralized distributed ledger though, the process can both be shortened, and made less labo- intensive. Given the fact that back-offices are costly while fees are under pressure, integrating this technology can give the sector its well needed breathing room. A company specializing in direct settlement for stocks is t0.com, but the regulatory hurdles for mainstream adoption are large still.

Figure 10. T+2 after trade settlement process



Source: Bitsonblocks, 2015

Figure 11. Post-trade life cycle security settlement with blockchain



Source: fintech 2.0, 2015

Private shares issued on blockchain

The pre-IPO market has been increasing during the past couple of years. The lively start-up scene sponsored by central banks' policies that keep interest rates low is enjoying the benefits of being private. Blockchain has now introduced the benefits of being listed for investors in those companies. The transparency and tradability of private stocks has improved because of distributed ledger technology. One of the most advanced applications on that front is offered by Linq, which is a distributed ledger product created by Nasdaq. It is part of the Nasdaq private market and is tailored to entrepreneurs and venture capitalists. Currently only a limited number of companies are registered via Linq, but this is expected to grow fast, as regulatory approval has not been an issue.

Overstock.com is working on similar technology. They have started with the issuance of a private bond via blockchain. The regulator has not officially approved it, but they have not tried to prevent the transaction either. If private markets become more attractive for entrepreneurs as well as private investors, there could be implications for the number of listed stocks. Private company listing requirements are much less costly than for public companies. If the owners of private shares find a liquid and transparent market to trade their holdings via blockchain, there is less incentive for an initial public offering.

Blockchain disintermediation in asset management?

Distributed ledger technology combined with smart contracts makes the entire process very efficient. The obvious question that arises is if this has the potential to disintermediate existing participants in the value chain. We do not think this will be the direct result. An important reason is that with blockchain technology rubbish in also leads to rubbish out. In other words: there needs to be validation of assets and flows. We expect certain companies in the value chain to develop the required technological capabilities to do this. This implies the task of, for instance, custodians will change from record keeping and administrative processes to validating records. They also have a good position to validate off-chain transactions that come on the chain and vice versa. Consequently, the threat of disintermediation becomes lower, but the pre-conditions are technology investments and IT architecture readiness.

Certain processes will change though. Smart contracts will pay out coupons and dividends without the need to manually check that process. That could impact the margins for custodial services in the long run. Two of the biggest custodians, State Street and BNY Mellon, are working on blockchain technology services.

Current state of distributed ledger technology

The hypothetical applications of distributed ledger technology are numerous. For the powerful combination of distributed ledger technology with smart contracts, those applications are even broader, have more impact and potentially lead to completely new business models and value chain participants. However, it is important not to be carried away by all these theoretical possibilities and to focus on what is likely to happen from a practical perspective. Two important considerations are regulation and the current state of technological developments.

Regulation and blockchain started off on the wrong foot

Blockchain 1.0 (as in cryptocurrency) has been a heavily debated topic and the outcome of that debate in terms of practical rules varies widely from one country to another. Some regulate Bitcoin as a commodity, others as a currency, yet others don't allow it to be used at all. It does not help that many of the Bitcoin believers have outspoken anti-government ideas either. This caused regulators to prepare for a reaction to an invention that was perceived to be an attack to the current monetary policy instead of an opportunity to reduce risks in the financial system and create large efficiency gains as demonstrated by the creation of blockchain 2.0 applications.

Regulation in a system that doesn't need to be regulated

Although the Bitcoin system does not require local governments to regulate the platform in order for it to function, it does need the regulator to allow for the legal usage of the technology. Although, theoretically, the network makes sure that participants obey the rules of the game, it makes sense to have central points of contact on which customers can fall back. International trade rules, anti-money laundering and know-your-customer are examples of essential regulation in order to preserve social and ethical boundaries on the flow of money that exist in the current system and have to be adopted in the new system as well.

It is highly unlikely that the regulator will change opinions with regard to these topics because of the introduction of new technology. Cooperation is therefore required and an essential step in the roll-out of blockchain technology. Bank consortium R3 CEV works very closely together with the UK regulator on blockchain 2.0 technology. Although this slows down the speed of technological progress, it creates a much stronger base from which an evolutionary roll-out can be established.

Blockchain benefits for regulators

The introduction of blockchain technology also creates a lot of advantages for regulators. Instead of having to go through a large set of centralized ledgers, the regulator has a good overview of asset exposure with the push on the button. Implementing blockchain technology and smart contracts also allows for efficiency gains within the regulatory process itself. However, we think it will take several years for the regulator to have sufficient trust in this new technology in order to replace current systems. In the meantime, most regulators have been supportive and in some countries (such as the UK and Australia) the regulator is advancing quickly.

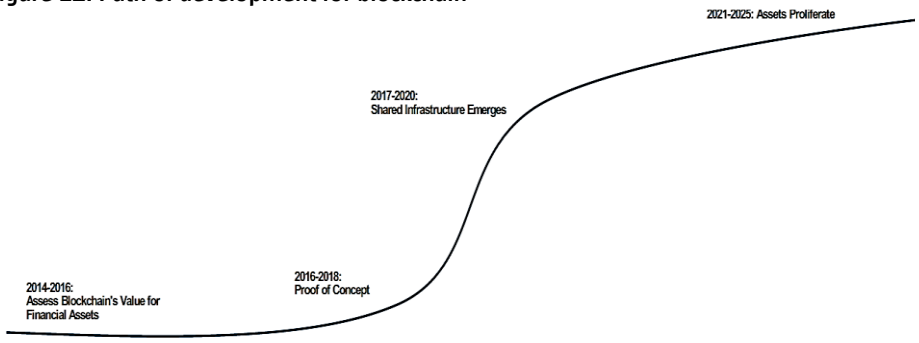
Blockchain technology still in its infancy stage

Although everything we have written before might give the impression that distributed ledger technology is ready for implementation, the opposite is true. Blockchain technology is only in its infancy stage and a lot of 'laboratory' testing will need to verify real life applicability. Regulators and existing companies will want to investigate ways to implement and oversee this new technology, which takes time.

The costs of implementing this new technology can be large. The benefit is not in reduced IT costs (these will likely increase), but rather in the ability to do the same amount of work with fewer people. We expect the coming two years to be a continuous flow of successful as well as failed experiments with the implementation of distributed ledgers.

We expect to see use cases in the 'quick win' areas first, such as trade and international remittance flows. The preconditions are that the current process is very inefficient (as in, labor-intensive), lengthy and costly. In other areas (like payments), the current processes are technically efficient, and the biggest gain would be in making the process more efficient. We think these will be the use cases for distributed ledger technology once the technology has matured. This is also the case with new business models, like distributed autonomous companies (DAOs). Morgan Stanley predicts the latter scenario to come into play after 2020. This is shown in figure12.

Figure 12. Path of development for blockchain



Source: Morgan Stanley, 2016

Technical issues to overcome

As explained above, the blockchain methodology behind Bitcoin uses proof of work in order to validate transactions. This technology requires a lot of processing power to solve mathematical puzzles. There are two main technical issues with this technology. The first one is the most obvious; it uses a lot of energy. At this point in time, mining is estimated to cost USD 15 million per day in energy consumption. In 2013 Bitcoin mining consumed 982 megawatt hours a day, which is enough to power 31,000 homes in the US[9]. These numbers vary a lot though and depend on the global hash rate (which is the speed of completing a crypto puzzle). In the most optimistic scenario of using only 0.1 watt per giga-hash, the energy usage would be 7.3 gigawatt hours per year. And those scenarios use the current usage of Bitcoin, not to mention the hypothetical applications discussed above.

Another issue, besides energy usage, is speed. In the original Bitcoin protocol, a maximum speed of 7 transactions per second could be reached (versus 2.000 transactions by Visa). This is set to increase to 1,000 transactions per second, but this is still too low when

[9] Swan, 2016

comparing it with current payment volumes, let alone what happens if blockchain 2.0 and 3.0 become operational and machines start to transact with each other as well. A possible solution will come at the end of 2016, when a new version of the Bitcoin protocol will be published. This protocol hypothetically allows for a limitless number of real time transactions, but might sacrifice on security.

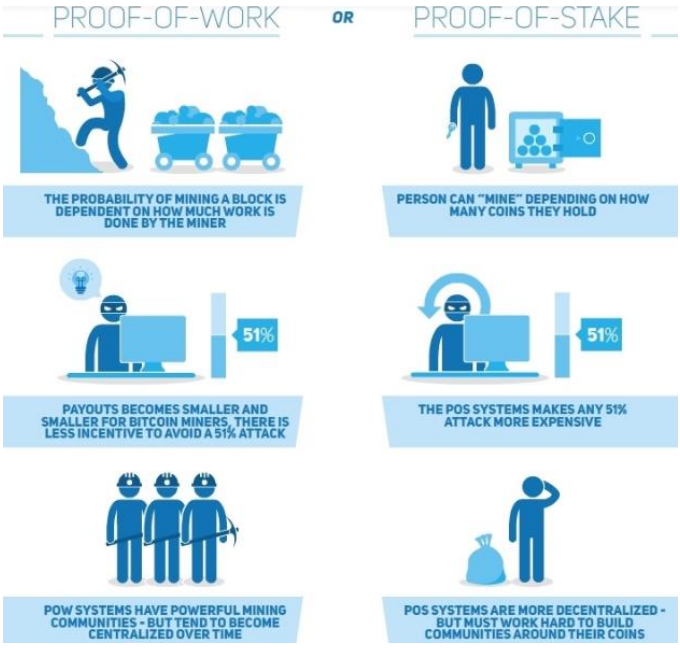
One standard required

At this point in time, there is not yet a common standard for distributed ledger technology. If this technology is going to function as the foundation on which numerous other applications are built, a standard needs to be agreed upon. Another feature that is required is the usage of open source technology. From the latter perspective, distributed ledger technology is doing the right thing because most applications are fully open source. The standard has not yet been agreed upon though. Testing results and momentum will be important drivers of the standards adoption. We do not expect regulatory selection of standards.

Proof of X instead of proof of work

In the current testing of distributed ledger technology most attention goes to solving the Bitcoin blockchain issues described above. A solution to the large size of proof of work could be smaller side chains that 'hook onto' the big blockchain on a regular basis. Alternatives to proof of work have been suggested and are being tested. Proof of burn, proof of ownership and proof of stake are examples of alternative validation methods. Especially the latter, proof of stake, has caught developers' attention. As shown in figure 13, proof of stake does not require the heavy processing power, but works on the idea that an attack can only be validated by the one who owns most (has the highest stake), which automatically hurts the one who owns most. Alternatives are being researched whereby the regulator plays an important role as well. We have no doubt the technical challenges can be solved in the future, but it will take time to develop and test these new applications.

Figure 13: Proof of work versus proof of stake



Source: Cointelegraph.com, 2015

Winners and losers

Expect evolutionary implementation

We are of the opinion that the blockchain rollout will be evolutionary rather than revolutionary. This implies we think in terms of sustaining innovation rather than disruptive innovation[10] within the financial sector. A lot of money and attention goes to distributed ledger technology at the moment. We think it is over-hyped and the short-term impact is overestimated. However, we are convinced blockchain technology is here to stay.

There are a lot of start-ups in this space, and just as with fintech in general, too many companies are involved at the moment, as shown in Appendix B. Only time will tell which companies will survive and it is very hard to predict clear winners at this stage. A lot of these companies are private, which implies we either have to wait until they become public, or we have to look for investible venture capitalists with a focus on blockchain. Although we cannot yet identify clear winners, we do see challenged business models.

Not only look at the financial industry for challenged companies

In the financial sector, there is an increasing influence of technology. Good examples of companies that are providing services for the financial sector are IBM, Accenture and Cognizant. Their main products and services focus on transforming legacy IT infrastructure. It can be questioned if there will still be demand for these services in a blockchain eco-system. Many technology companies are working on their own blockchain solutions, but we think it is wise to consider the consequences for the suppliers of 'old' technology as well as for the financial companies themselves.

Challenged business plans with inefficient value chains

In our opinion, companies involved in the 'quick win' areas (costly, labor intensive and lengthy processes) are most at risk if they do not react to this new technology. The 'middle man' who is not able to provide value for his customers is expected to be disintermediated by distributed ledger technology. Key incumbents are likely to be investing in the technology in order to transition their current business model.

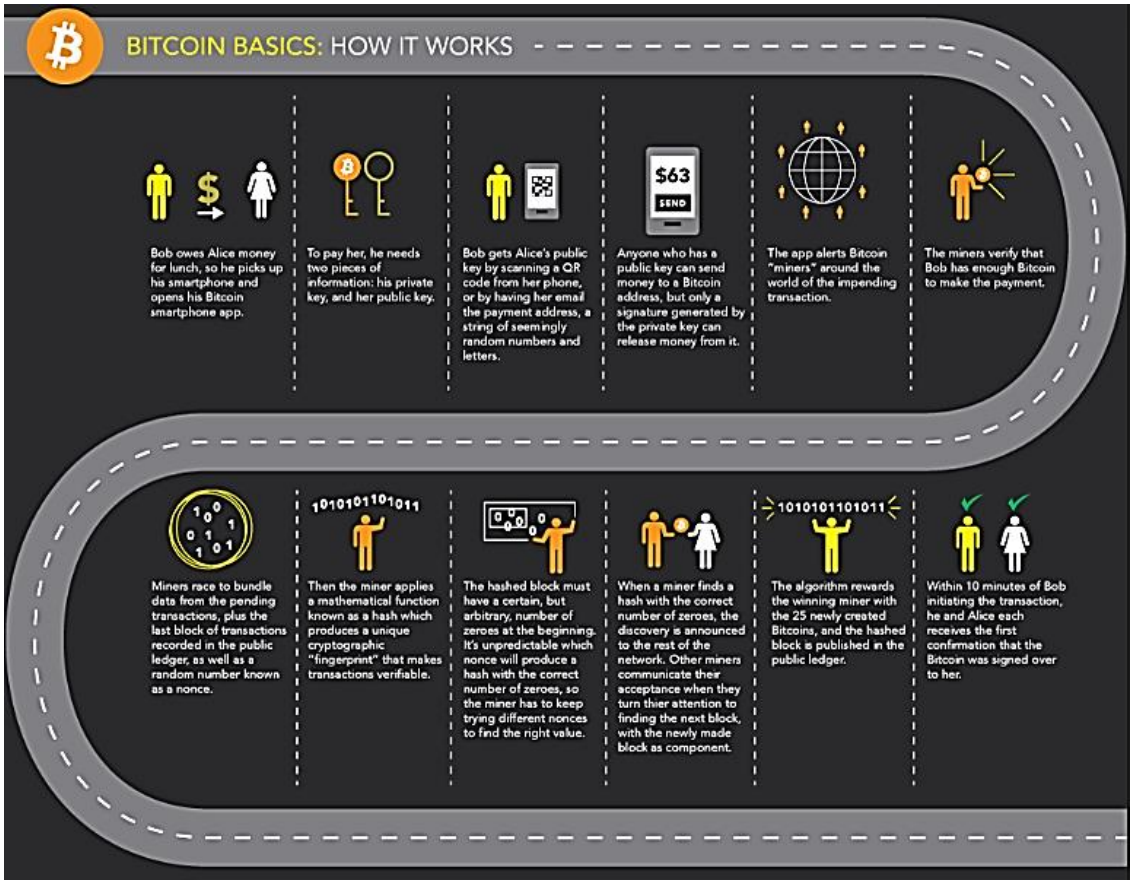
Within banking we think of three quick win use cases for blockchain. Correspondent banking, trade settlement and remittance services are areas where a large efficiency gain can be made by implementing distributed ledger technology in combination with smart contracts. We expect to see pressure on existing business models as a consequence.

Within the asset management value chain we expect to see competition emerge between exchanges and custodians in order to become the validator-hub for blockchain transactions. We believe the efficiency gain will, in the meantime, put pressure on the margins of their current business models. We do not expect disintermediation.

Quick win use cases in insurance are further away, but when they come, they are likely to enter via the personal lines Property & Casualty side of insurance. We expect insurance products with the most programmable/objective pay-out schemes (like flight insurance and weather insurance) to be challenged first. We would be cautious with insurers that have a large exposure to these products.

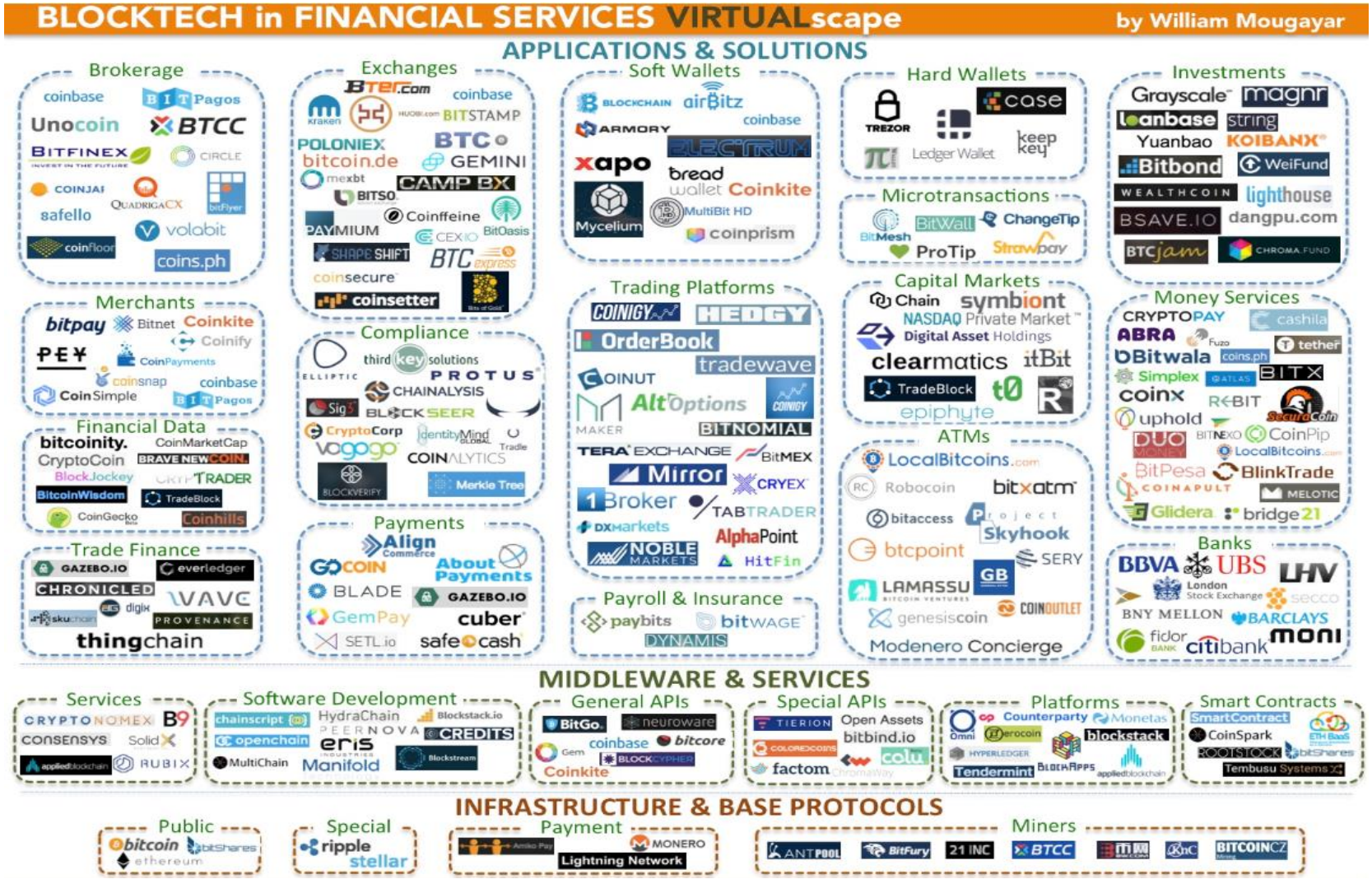
[10] C. Christensen, disruptive technology innovation framework

Appendix A: Bitcoin transaction flow



Step 1: Type the transaction amount in the bitcoin app
Step 2: To pay, person 1 needs person 2's public key, and his own private key
Step 3: Via the public key of person 2, person 1 can transfer the money if he uses his own private key
Step 4: Once the transaction request has been approved, miners start verifying the transaction
Step 5: Miners first verify that person 1 has enough money in his account to make the payment, after which miners race to bundle transactions in order to solve a mathematical puzzle that makes the transaction valid
Step 6: When solving the hash, the discovery is communicated to the rest of the mining network, after which other miners quickly move onto the next puzzle to solve
Step 7: The miner who solved the puzzle receives Bitcoins as a reward for using his computing power
Step 8: The transaction is placed on the distributed ledger and everyone can see the flow of money

Appendix B: Blockchain eco-system



Source: Mougayar, 2015

Glossary

Bitcoin	Cryptocurrency invented in 2009, based on cryptography to operate in a trustless environment.
Block chain	Protocol behind cryptocurrency Bitcoin specifically, see blockchain
Blockchain	A blockchain is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called blocks (rather like collating them onto a single sheet of paper). Each block is 'chained' to the next block, using a cryptographic signature. This allows block chains to be used like a ledger, which can be shared and accessed by anyone with the appropriate permissions.
Cryptocurrency	A digital currency in which encryption techniques are used to regulate the generation of units of currency (so there is a maximum of units created) and verify the transfer of funds.
DAO	Distributed automated organization. This is an organization that exists on the blockchain, but without the usual ownership structure. A DAO can have shareholders, but does not necessarily require any. DAOs have authorization that allows for transactional flows. Combined with artificial intelligence and IOT a DAO hypothetically has the potential to exist without the need for human intervention in any part of the process.
Double spend	Scenario in the Bitcoin network, where someone tries to send a Bitcoin transaction to two different recipients at the same time. However, once a Bitcoin transaction is confirmed, it makes it nearly impossible to double spend it. The more confirmations a particular transaction has, the harder it becomes to double spend the Bitcoins.
Hash rate	The number of hashes that can be performed by a Bitcoin miner in a given period of time (usually a second).
Hashing	The process of running a computer algorithm over content in order to create an alphanumeric character that cannot be back-computed into the original content.
IOT	Internet of Things. It is a broad concept used to describe the creation of a 'Smart' product or system where 'Things' are inter-connected via wireless and/or wired networks. The 'Things' are physical devices, equipment, machines, computers or screens – of any size – that are embedded with software applications, sensors and electronics. The embedded components enable 'Things' to connect and exchange data that monitors, analyzes and controls the Smart product or community of products.
Merkle Tree	Tree-structured process where every non-leaf node is labeled with the hash of the values of its child nodes. An example is the hash of block 2 that depends on the hash of block 1.
Mining	The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.

Permissioned ledger	A permissioned ledger is a ledger where actors must have permission to access the ledger. Permissioned ledgers may have one or many owners. When a new record is added, the ledger's integrity is checked by a limited consensus process. This is carried out by trusted actors — government departments or banks, for example — which makes maintaining a shared record much simpler than the consensus process used by unpermissioned ledgers. Permissioned blockchains provide highly verifiable data sets because the consensus process creates a digital signature, which can be seen by all parties. A permissioned ledger is usually faster than an unpermissioned ledger.
Proof of stake	An alternative to the proof-of-work system, in which your existing stake in a cryptocurrency (the amount of that currency that you hold) is used to calculate the amount of that currency that you can mine.
Proof of work	A system that ties mining capability to computational power. Blocks must be hashed, which is in itself an easy computational process, but an additional variable is added to the hashing process to make it more difficult. When a block is successfully hashed, the hashing must have taken some time and computational effort. Thus, a hashed block is considered proof of work.
SHA256	The cryptographic function used as the basis for Bitcoin's proof of work system.
Smart contract	Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system. There is, however, also a possibility to manually go through contract terms if required.
Unpermissioned ledger	Unpermissioned ledgers such as Bitcoin have no single owner - indeed, they cannot be owned. The purpose of an unpermissioned ledger is to allow anyone to contribute data to the ledger and for everyone in possession of the ledger to have identical copies. This creates censorship resistance, which means that no actor can prevent a transaction from being added to the ledger. Participants maintain the integrity of the ledger by reaching a consensus about its state.

Jeroen van Oerle
Trend analyst at Robeco
Trends Investing

Patrick lemmens
Portfolio Manager Robeco
New World Financial Equities

(Cth) pursuant to ASIC Class Order 03/1103. Robeco is regulated by the Securities and Futures Commission under the laws of Hong Kong and those laws may differ from Australian laws. This document is distributed only to wholesale clients as that term is defined under the Corporations Act 2001 (Cth). This document is not for distribution or dissemination, directly or indirectly, to any other class of persons. It is being supplied to you solely for your information and may not be reproduced, forwarded to any other person or published, in whole or in part, for any purpose.

Additional Information for investors with residence or seat in the United Arab Emirates

Robeco Institutional Asset Management B.V. (Dubai Office), Office 209, Level 2, Gate Village Building 7, Dubai International Financial Centre, Dubai, PO Box 482060, UAE. Robeco Institutional Asset Management B.V. (Dubai office) is regulated by the Dubai Financial Services Authority ("DFSA") and only deals with Professional Clients and does not deal with Retail Clients as defined by the DFSA.

Additional Information for investors with residence or seat in France

In remuneration for its advisory and distribution activities in respect of the group's UCITS, the parent company will pay the entity in France a fee, in application of all the rules laid down by the Robeco Group with regard to transfer pricing:

- equivalent to 1/3 of the management fees applied to institutional-type units that do not give rise to a distribution fee (which distributor "clients" such as private banks would receive, for example).
- equivalent to 2/3 of the management fees applied to "all investors" units that may, provided there is an agreement in place, give rise to payment of a distribution fee (which distributor "clients" such as private banks would receive, for example) up to a maximum 50% of the management fees of the underlying UCIT. RIAM is a Dutch asset management company approved by the AFM (Netherlands financial markets authority), having the freedom to provide services in France. Robeco France has been approved by the French prudential control and resolution authority (formerly ACP, now the ACPR) as an investment firm since 28 September 2012.

Additional Information for investors with residence or seat in Spain

The Spanish branch Robeco Institutional Asset Management BV, Sucursal en España, having its registered office at Paseo de la Castellana 42, 28046 Madrid, is registered with the Spanish Authority for the Financial Markets (CNMV) in Spain under registry number 24.

Additional Information for investors with residence or seat in Switzerland

RobecoSAM AG has been authorized by the FINMA as Swiss representative of the Fund, and UBS AG as paying agent. The prospectus, the articles, the annual and semi-annual reports of the Fund, as well as the list of the purchases and sales which the Fund has undertaken during the financial year, may be obtained, on simple request and free of charge, at the head office of the Swiss representative RobecoSAM AG, Josefstrasse 218, CH-8005 Zurich. If the currency in which the past performance is displayed differs from the currency of the country in which you reside, then you should be aware that due to exchange rate fluctuations the performance shown may increase or decrease if converted into your local currency. The value of the investments may fluctuate. Past performance is no guarantee of future results. The prices used for the performance figures of the Luxembourg-based funds are the end-of-month transaction prices net of fees up to 4 August 2010. From 4 August 2010, the transaction prices net of fees will be those of the first business day of the month. Return figures versus the benchmark show the investment management result before management and/or performance fees; the fund returns are with dividends reinvested and based on net asset values with prices and exchange rates of the valuation moment of the benchmark. Please refer to the prospectus of the funds for further details. The prospectus is available at the company's offices or via the www.robeco.ch website. Performance is quoted net of investment management fees. The ongoing charges mentioned in this publication is the one stated in the fund's latest annual report at closing date of the last calendar year.