Capgemini

Distributed Ledger Technology

A conceptual and contextual Introduction[1]

Dr. Jan-Willem Burgers

April 2018

1 Introduction

Distributed ledger technology, also commonly referred to as "blockchain technology," has been making headlines in the financial services industry for several years. Many of the world's financial institutions have invested in learning and experimenting with the technology, and many believe it will have a significant impact on the future of financial services. Since 2016, the enthusiasm for distributed ledger technology has also spread to government and industry. Since the fall of 2016, for example, a great number of pilots have been initiated in the Dutch public sector.[2]

But what is distributed ledger technology exactly? And what is the relationship with Bitcoin? In this paper, I offer an in-depth conceptual and contextual introduction to Bitcoin and distributed ledger technology. The paper begins in Sections 2 and 3 with a brief history of digital cash systems and why Bitcoin was a watershed moment in this long history of initiatives. Sections 4 and 5 provide insight into how Bitcoin works and how Bitcoin differs from the various rivals which have sprung up after its inception. In Section 6, I use the knowledge on Bitcoin and its history to describe and understand the recent popularity of permissioned ledger platforms, the types of distributed ledger platforms generally preferred by financial institutions. Section 7 briefly discusses the applications for Bitcoin and permissioned ledger systems. Section 8 concludes.

2 Centralized digital cash

All of us are familiar with **physical cash**. It generally refers to the Central Bank issued paper notes and coins most of us carry around in our wallets in the form of euros, dollars, yens, and many other types of national currencies. Historically, coins and paper notes used on a large scale would have also been issued by other types of institutions than central banks, such as commercial banks or other types of state institutions. Additionally, it would have been common to have numerous currencies in circulation. Standardization efforts by states in the last few centuries, however, have significantly reduced this heterogeneity in our monetary environment.[3] Generally, the only forms of physical, non-central-bank-issued cash one might by chance run into in modern times are those based on local or regional initiatives, such as the Brixton Pound or the Makkie in Amsterdam's Indonesian district. But even such local or regional cash systems are often pegged to national currencies.

Physical cash in the form of notes and coins is by the far the most common type of **physical money** in modern times. Historically, physical money also came in other forms. In the early 18th century in North America, for example, a great number of physical money substitutes were used. The most popular was "wampum," shell money used by Native Americans, but other commodities such as corn, bullets, animal skins, tobacco, and pork were also employed as physical money substitutes.[4] And though issued coins, usually made of silver or gold, were already popular in Ancient Greece and Rome (having first arisen in Lydia in the sixth century BC), paper notes really only became widely accepted in the nineteenth century. In modern times, alternative forms of physical money still sometimes arise when there is an acute absence of usable notes and coins: cigarettes, for example, sometimes assume the role of money in prisons.

Perhaps the most central property to the concept of physical cash is that it is by default a **bearer financial instrument**: whomever holds a certain amount of physical cash in their possession is generally entitled to enjoy its value in economic exchange. Typically physical cash transactions also (1) do not require third parties to intermediate, (2) are relatively anonymous, and (3) are difficult to censor. The nature of a cash transaction, thus, differs quite substantially from, say, a money

[1] Please note that the views expressed within this paper are entirely my own and not Capgemini's.

[2] For an overview, see www.blockchainpilots.nl.

[3] See, for example, Mujagic 2016.

[4] Breckenridge 1903, pp. 53–4. See also, for example, Graeber 2011.

transfer from your current account to another one. You cannot transfer the money on your own, you need your financial institution as an intermediary. The registered value in your current account is coupled to your identity and, therefore, such a transaction is typically much less anonymous. Finally, your financial institution could quite easily censor your activities if desired by, say, the authorities.

A **cryptographic cash system or digital cash system** is a digital payment system in which the payments resemble physical cash transactions. Though we do not frequently encounter digital cash systems, fare cards and gift cards are the most familiar examples of products that sometimes fall into the category. With many of these types of cards, value is actually loaded onto them, so that transactions do not require an intermediary. Furthermore, these cards are frequently not coupled to an identity, so that anyone who holds them can generally enjoy their value in economic exchange. Hence, unless there is a strong link to an identity, these types of cards are also bearer financial instruments with no need for an intermediary and with a reasonable level of anonymity.

The most common modern methods for digital payments such as credit card transactions and credit transfers have little resemblance to physical cash transactions. Yet, there is a long history of projects that have sought to bring digital cash systems to the public. The Dutch company Digicash, active in the 1990s, is a noteworthy example. It was founded by the American cryptographer David Chaum in 1990. Its main product was the Ecash system, a digital cash system based on scientific papers written by Chaum and others in the 1980s (see, e.g., Chaum 1983 and Chaum, Fiat, and Naor 1988).

The Ecash system worked as follows. Members could purchase an amount of Ecash from Digicash. They could then use this Ecash to pay one of the other members in the network for goods and services without the need for intermediation by DigiCash. Hence, unlike with standard online credit card transactions or credit transfers, no intermediary was needed for an Ecash transaction. As with physical cash transactions, Ecash transactions could in principle provide a strong assurance of anonymity to those buying goods and services, at least given enough participants in the system (a much stronger assurance of anonymity, in fact, than is provided with current bitcoin transactions). As the number of participants in the Ecash system was limited, however, in practice the system offered little anonymity to those buying goods and services. Unlike physical cash transactions, however, the Ecash system offered little anonymity to anyone on the receiving end of an exchange, regardless of the number of participants in the network. Any merchant or individual that received Ecash in the system, namely, needed to exchange it again with Digicash for security purposes. They could not, in other words, take the Ecash they had received and use it in a new transaction with another member in the network.

Systems such as Ecash are referred to as **centralized digital cash systems**: even though they offer participants a money-like digital bearer instrument, they have a central party that plays a crucial role, usually by issuing the money and controlling transaction flows for security purposes. Before Bitcoin, every digital cash system was centralized to prevent what is known as **double spending**: using the same digital cash twice (or even more times). The double spending problem is particularly relevant in the design of digital cash systems. In the physical world, central-bank-issued cash, at least in many modern societies, is very difficult and costly to copy exactly. In this way, spending the same amount of cash twice, by making a copy, is difficult to do. In the digital world, however, we face a completely different scenario. Think of how easy it is to copy a music file. We can make hundreds or thousands of copies of the same music file, and there is practically no way to prove that any copy was the original or authentic copy. Any digital cash system, therefore, needs to prevent its users from making copies of their digital cash and using it multiple times. Before Bitcoin, all digital cash systems solved this double spending problem by allowing a strong role for a central authority.

3 Decentralized Digital Cash

Before the Bitcoin system, there had long been discussions about the possibility of **decentralized digital cash** within the cryptographic community: a digital cash system open to anyone, which did not require centralized coordination and control (particularly, to help avoid the double spending problem). Many within the cryptographic community had thought such a decentralized system was impossible. In fact, when the Bitcoin white paper was released on a forum for cryptographers in November 2008, most of those who read it did not seem to believe the system would work!

There were probably two main motivations behind the interest in building a decentralized digital cash system among certain segments of the cryptographic community. First, decentralized digital cash presented a formidable technical problem. The double spending problem is really a specific case of achieving **distributed consensus in an open network**. When a network is open to anyone and does not have registered identities, how can we get everyone to come to valid agreements on the state of that network? Say, the total amount of money that is in the system, how much is owned by each participant, and the transactions that have occurred?

Furthermore, many with an interest in decentralized digital cash had strong political motivations. An open system would, for instance, open the world of finance to anyone, without fear of censorship by central authorities. It was also thought such a system could give people more control over their money, which now rests primarily with commercial banks and states. Many of the individuals interested in decentralized digital cash were sympathetic to Libertarian and Anarchist political philosophies, and to ideas from the Austrian School of Economics. Specifically, ideas about decentralized digital cash were discussed among a group of cryptographers who called themselves **cypherpunks** and who sought to empower individuals and promote political and economic freedom through cryptography.[5]

4 Bitcoin

The distributed consensus problem in an open network, and the double spending problem which is a specific case of it in financial cryptographic systems, was thought by many to be an insurmountable challenge.[6] Why was distributed consensus thought to be impossible in such a system? There were basically two kinds of obstacles. First, in an open network there would be many imperfections, such as nodes crashing and lag time in communication. Second, and even more importantly, without having verified identities in such an open network, there would be no good way of preventing bad actors from trying to manipulate the system in harmful ways, particularly in the form of sybil attacks.

The **Bitcoin Network** solves the problem of double spending in a decentralized financial cryptographic system, and thus the distributed consensus problem in an open network for a specific case (it does not solve the problem in a more general sense). It is difficult to understate what an achievement that is from a computer science perspective. It is the culmination of decades of discussions, debates, and research.

The Bitcoin Network was launched in 2009, invented by a person or group of persons operating under the pseudonym **Satoshi Nakamoto**.[7] The primary basic functionality of the Bitcoin Network is that participants can transfer

[5] See, for example, Rid 2016.

[6] In closed systems with verified identities, the problem is much less pernicious. A famous result from Lamport, Shostak, and Pease (1982) shows, for example, that such a system can be reliable if more than two-thirds of the nodes are honest, a reasonable assumption in a well-organized, closed environment.

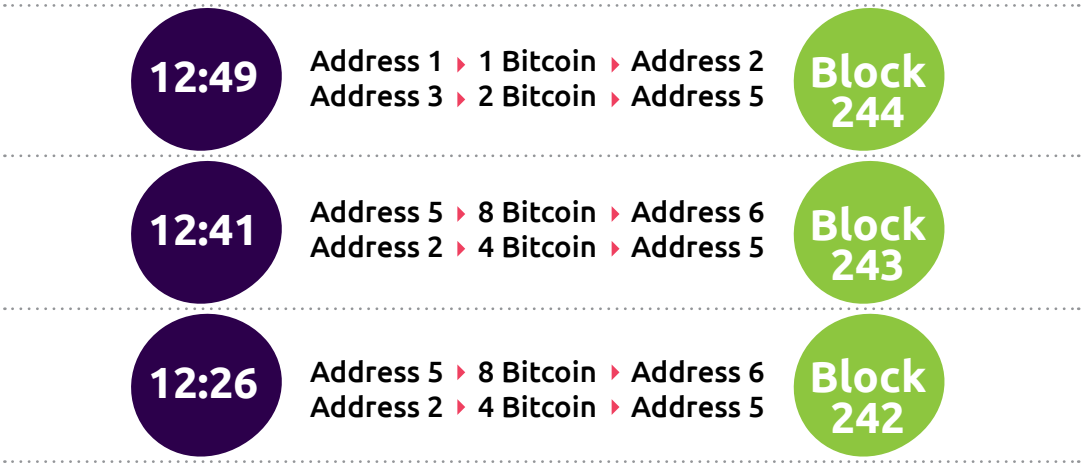
[7] For an overview of the Bitcoin system, see Nakamoto 2008, Antonopoulos 2014, and Narayanan et al. 2016

the cryptocurrency **bitcoin** to one another without the need for any intermediary; hence, why Bitcoin is called a **peer to peer digital cash system**.[8] These bitcoins are not issued by a centralized authority, but in a decentralized fashion through **proof-of-work mining** according to a fixed production schedule. Currently, 12.5 new bitcoins are introduced to the Bitcoin system with every new block of transactions, on average every ten minutes. Anyone can join this network by downloading a **wallet application** such as Electrum or Samourai Wallet, or by opening a wallet with a third-party provider such as Xapo or Coinbase.[9] These wallets allow a user to generate bitcoin addresses from which to receive and send money. In many countries, the digital currency is nowadays easily obtained with fiat money through exchange platforms. In the Netherlands, for example, you could acquire bitcoins with euros via Bitonic, Bitmymoney, Coinbase, Kraken, LocalBitcoins, and numerous other channels.

The Bitcoin Network, though still small, has grown significantly in the number and dollar volume of transactions.[10] It is also very much in development still. One active area of research and development is the **Bitcoin Protocol**, the core protocol which governs the Bitcoin system. An intense public discussion has surrounded, for example, the introduction of **Segregated Witness** (Segwit); originally intended to fix a bug in the code known as transaction malleability, Segregated Witness has a number of additional significant benefits for the Bitcoin Network. Another area of research focuses on higher-level protocols, applications, and services which can be layered on top of the basic the Bitcoin Network. An exciting project is the **Lightning Network**, a network that will sits on top of the basic Bitcoin Network, which has grown substantially in recent months. Its realization could help significantly increase the number of bitcoin transactions that can be made. Some believe innovations such as these will eventually allow Bitcoin to scale to the size of sophisticated payment networks such as Visa or MasterCard.

Despite all this active development, however, the Bitcoin system is secure really only for the technologically adept. Bitcoin is not (yet) a consumer-friendly product. For instance, using Bitcoin securely currently requires private key management and protecting yourself from theft and loss; the average consumer is not familiar with the measures that need to be taken in order to use bitcoin in a secure way. If Bitcoin is ever to become a widespread system, one of the largest challenges will be to find ways to make participation in the system more consumer-friendly.

In a nutshell, Bitcoin works as follows. At the heart of Bitcoin is a ledger which is stored and maintained by thousands of computers around the world called **full nodes**; anyone is free to run such a full node on their computer. This distributed ledger is not like a standard bank ledger with account balances that are coupled to individual identities. Instead it contains a series of sequentially time-stamped blocks stacked on top of each other and cryptographically linked. Such a block is added every ten minutes on average to the ledger. Although blocks contain different important data types, most importantly they contain a list of bitcoin transactions that are considered by the system to have occurred at the same time. Each transaction has information on the amount transferred and on the Bitcoin addresses involved, but it does not provide any direct information on the identities of the parties involved. A high-level impression of Bitcoin ledger is given below.



[8] Note that we normally distinguish the network from the currency by using upper- and lower-case letters respec-tively. That is, Bitcoin refers to the network and bitcoin refers to the currency.

[9] Note that both these options each come with their own security issues. You can learn more about securely using the Bitcoin system from Antonopolous (2014) and Narayanan et al. (2016).

[10] For network statistics, there are numerous sites such as Blockchain.info.

How does Bitcoin ensure that all full nodes have the same copy of the ledger? To be exact, Bitcoin does not give a 100% guarantee that all full nodes have a completely consistent view all the time. Instead, it guarantees for all practical purposes that they have a consistent view once you move several blocks down into the ledger. Different views with regards to the top blocks commonly arise, but these are eventually resolved through Bitcoin's consensus protocol. This is why it is generally recommended to wait **six confirmations** before accepting as secure any bitcoins that you have received (that is, until five new blocks have been stacked on the top of the block containing your transaction). For all practical purposes, you may consider all the transactions in the Bitcoin ledger and the relative order they have occurred in from six blocks down into ledger as the official history of the Bitcoin system. From this information you can, of course, calculate the confirmed address balances for any point in time in the history of Bitcoin.

The Bitcoin ledger seems to have at least two crucial properties, which ensures that the system works: **tamper-resistance** and **rule rigidity**. First, once a transaction has been included in a block that is added to the ledger, it is already highly unlikely that it is reversed or changed in some relevant way by a small group of actors. But the chance of any such alteration to the transaction by a small group of actors decreases drastically as even more blocks are added on top of the block which contains the transaction. After a few blocks have been added, the chance of reversal or alteration of a transaction by any small group of actors is practically negligible.

To be sure, transactions can be reversed or altered in the Bitcoin system if there is widespread consent in the system. In the end, Bitcoin is also a social system that relies on the actions of people to function. Bitcoin's ledger is often described as **immutable**, meaning that once a transaction is added to the ledger it can no longer be altered or reversed. But this description is not entirely accurate. First of all, immutability seems to suggest the ledger cannot be changed at all in any way. This is clearly not the case as at the very least transactions are continuously being added. One might, then, suggest that what "immutability" means here is that transactions cannot be reversed or altered once they are in the ledger. If this were true, then it would be more accurate to say that Bitcoin has an **append-only ledger**. But even this description of Bitcoin's ledger is too strong: only the chance of being reversed or altered decreases as transactions move down in the chain of blocks. The transactions in the latest few blocks a full node has stored are sometimes still changed, as required by the consensus protocol. Finally, and crucial in understanding Bitcoin, transactions could be reversed or altered, even in the more distant past, if the community agreed to reset the system from a historical point. An essential element in Bitcoin is precisely that such an agreement is very unlikely to occur within the community, not in the least because of the incentives built into the system.

A better way to describe the relevant property of Bitcoin's ledger here is as **tamper-resistant**: it is unlikely that any small group of actors could reverse or alter a transaction, once it is included in the chain of blocks, and this likelihood decreases as the transaction moves down the chain. This tamper-resistance is the result of a complex interaction between the technical aspects of Bitcoin's design, the incentives created by this design, and certain social norms that permeate the Bitcoin community. If this rigidity were not the case in Bitcoin, then participants could never be sure a payment was settled. A merchant would then, for example, have less certainty when sending a customer her goods after a bitcoin payment.

A second crucial property of the Bitcoin ledger is that it seems to have what might be termed **rule rigidity:** it is highly unlikely that one or a few participants in the system can change the basic rules of the ledger, and community consensus for such changes generally takes substantial time to build, if that is even possible. By the basic rules of the Bitcoin system, I have mind, for example, the following: the production schedule for bitcoins, that transferring bitcoins requires a valid digital signature based on a particular elliptic curve scheme, that miners have a fixed block reward in the coinbase transaction, and so on. These basic rules are important in setting certain expectations for participants in the Bitcoin system. Take the example that only actors who can make the correct digital signature for an account can move the funds in that account. As a consequence of rule rigidity, it would be nearly impossible, for instance, for any actor or small group of actors to push through a financial haircut for bitcoin account holders for some common end.

The Bitcoin ledger has generally come to be known as the **Bitcoin Block Chain**. There is much discussion and debate as to why this ledger is called the Block Chain. Some people believe it is because the ledger consists of a series of blocks that are cryptographically linked. This conceptualization, however, misses the thicker meaning of the term "chain." Additionally, if you use the term Block Chain in this way, then there does not appear to be anything substantially new about the Bitcoin Block Chain, as the idea of databases constructed in the form of cryptographically linked blocks existed long before Bitcoin, even for the purposes of relative time-stamping (see, e.g., Haber and Stornetta 1991).

Instead, we should understand the term Block Chain as indicating something more. For the purposes of our discussion, we might understand the ledger as the Block Chain because it has the aspects we just discussed: (1) tamper-resistance, and (2) rule rigidity. It should be noted that there is quite a bit of discussion about what exactly is meant by terms like tamper-resistance in the Bitcoin community. For instance, some believe that idea of tamper-resistance requires that data is never lost, while others believe that permanent data storage is not inherent to the idea of the remembrance of certain shared facts. Nevertheless, despite such discussions, most agree that the term Block Chain needs to be more specific than the idea of cryptographically linked blocks to capture its innovativeness, and the aspects of tamper-resistance and rule rigidity as I have described them above at least go some way towards understanding what is innovative about this ledger.

Importantly, I have suggested that transaction alterations and reversals, and basic rule changes can only feasibly be executed with widespread consent. Many would argue that power is, in fact, much more concentrated in the Bitcoin system; specifically, many people argue that a few Bitcoin mining pools and large miners hold a disproportionate share of influence. I believe that for a number of reasons these concerns are misguided. However, if power were indeed much more concentrated as claimed by these detractors, then Bitcoin's ledger would not enjoy the tamper-resistance and rule rigidity as described above, and indeed the ledger would seem much less innovative than is commonly suggested.

Note that you might have similar types of guarantees for tamper-resistance and rule rigidity from a bank with regards to the ledgers they keep: a bank cannot, for instance, just change the balance in your account at their discretion. Importantly, however, these guarantees come from trust in the reputation of the bank, and legal and institutional measures. In Bitcoin, at least in large part due to its technical design, you have to place less trust in one or a few parties to enjoy these types of guarantees. A common refrain in the Bitcoin community is that the system does not require trust. This I would argue is not exactly the case. It is just that the system is much less reliant on central actors in the core system and instead this trust is more widespread across a community.

How does the Bitcoin system ensure that its ledger has these two properties of tamper-resistance and rule rigidity? It depends, in fact, on a number of factors. At least for tamper-resistance, one main driver is what is known as proof of work mining. This is both one of the key aspects of the Bitcoin system as well as the most difficult part to explain to laymen. In a nutshell, Bitcoin has basically made the ability to alter the ledger a question of computer power and energy consumption. Any attacker or group of attackers that wants to make alterations to the Block Chain would need to have a large amount of customized computer equipment (known as application specific integrated circuits) and expend significant energy to do so. How much computer power and energy is a matter of debate and depends also on what exactly the attacker is trying to do. But to give an idea, the Bitcoin Network currently has about several million times more mining power than the world's largest supercomputer, the Sunway Taihulight.[11] Why would Bitcoin miners contribute all this computer power to ensure that the Bitcoin Network runs smoothly? It is because they are rewarded in bitcoins for every block they add to the Block Chain as well as for the transactions in those blocks through fees. The Bitcoin system, in general, works because the participants are incentivized in the right way. In fact, all the

[11] You can find an expression of the network's hash rate in petaflops at www.bitcoinwatch.com.

techniques used in Bitcoin are well-known and familiar. What makes Bitcoin innovative is, at least partially, from a design perspective: how existing techniques were combined to create a system which gives the participants the right incentives for it to work. Hence, Bitcoin is arguably much more interesting from a game-theoretical perspective than a technical perspective.

Although Bitcoin is at its basis best described as a payment network, it is important to realize that this basic network may support other types of applications. For a straightforward example, by adding some metadata to particular bitcoins we could change the meanings of what those bitcoins represent: instead of money, these bitcoins might then represent shares, bonds, or some other kind of (financial) asset. For another example, the OpenTimestamps Protocol verifies that data exists at a certain point in time, which have may have various applications including for financial institutions. It is matter of debate which kinds of applications could successfully be built on top of the Bitcoin Network, but ideas range from stock exchanges and bond markets to decentralized storage applications and notary services.

5 Other block chain networks

Given the (financial) success of Bitcoin and that the source code is open to anyone, we should hardly be surprised that people have tried to create similar networks. Starting such a network is incredibly easy to do. We could do it in a few minutes. And unsurprisingly there probably are 1000 active alternative networks at the moment. Most of these networks simply use the Bitcoin source code with minor tweaks, such as Dogecoin, Litecoin, and Blackcoin, though some networks were created from the ground up, such as Nxt and Ethereum. Many, in fact I would say most, of these networks were set up purely from the motivation for financial gain. Some have genuinely tried to create monetary and technical innovations on Bitcoin. Perhaps best-known is Ethereum: whereas Bitcoin was primarily designed to be a decentralized digital cash system, Ethereum's purpose is much broader, namely to serve as a distributed, open network for more general applications. Other well-known examples are Monero, a currency which focuses on privacy features, and Litecoin, a currency which intends to be the "silver to Bitcoin's gold." It is a matter of fierce debate within the community whether these or any of the other alternative networks offer any tangible benefits over Bitcoin.

As easy as it is to start such a decentralized network based on the Bitcoin protocol, so difficult it is to create one that is actually secure and reliable. Every other open network that has tried to emulate Bitcoin is substantially less secure from attackers. This is so even for well-known open networks such as Ethereum and Litecoin. And we should be skeptical of any such network eventually being able to provide the same degree of security as Bitcoin. The Bitcoin Network was, with some luck, able to overcome a bootstrapping problem, so that it now enjoys a triad of security, value, and mining power. It is by no means a sure thing. But no other public network seems to have overcome this bootstrapping problem anywhere near the same degree. Unless an alternative method for securing such open networks other than by proof of work mining is found, it will be difficult for alternative networks to be able to offer similar standards of security (many claim that proof of stake can do this, but this method faces serious problems and has yet to be tested in practice for networks of significant value).[12]

6 Permissioned ledger technologies

Many products that commonly fall under the heading of "blockchain technologies" are better classified as **permissioned ledger technologies**. Ripple, Fabric, Corda, Eris, and BigchainDB are all well-known examples of such products. Although there are dozens of such products, they all are based around Bitcoin's idea of a shared ledger but in a **closed environment**. Given the similar idea of a shared ledger, it is clear why these permissioned ledger products often fall under the heading of "blockchain platforms" or "blockchain technologies." Yet, these platforms really should be carefully distinguished from Bitcoin.

To start, permissioned ledger platforms have a very different purpose than Bitcoin. One main purpose of the Bitcoin Network is to solve the double spending problem on an open, permissionless network without known identities. As the defining feature of permissioned ledgers is that they work in a closed system, they clearly cannot have the same primary purpose as the Bitcoin system. Given these different purposes, the architectural details are also signifcantly different. For instance, whereas the Bitcoin system absolutely requires the existence of a cryptocurrency and a proof of work mining process to incentivize the participants to secure it, permissioned systems do not require a cryptocurrency (or, at least not for the same reasons) and can draw on a number of practical consensus protocols not feasible for Bitcoin.

These technical differences between Bitcoin and permissioned ledgers result in vastly different properties with regards to the ledger as well. In Section 4, I suggested that the Bitcoin Block Chain has the properties of tamper-resistance and rule rigidity. By tamper-resistance, I meant to convey that the chance of transaction reversal or change becomes very small as a transaction moves down the Block Chain.

[12] For a good discussion, see Poelstra 2015.

By rule rigidity, I meant to convey that the basic rules of the Bitcoin system are either unlikely to change or, at least, take a long time to change, due to the need for community consensus. The Block Chain has these features in large part for technical reasons, but also due to particular norms which govern the Bitcoin community. Though terms such as tamper-resistance are often used to describe permissioned ledger systems, we should at least acknowledge that these terms do not apply in the same way as to Bitcoin. First, permissioned ledger systems generally only include selected institutions, so that control over a ledger is not spread throughout a community as with Bitcoin. Rule changes, even fundamental rule changes, could be implemented in a much easier way. Second, the energy expended in the Bitcoin Network provides a signficant incentive and protection against transaction alteration and reversal. This incentive does not exist in closed systems.

There are many existing products, which enable consensus on distributed database systems, such as Cassandra, Couchbase, and Aerospike. The idea of a shared ledger in a closed system was, therefore, certainly possible before Bitcoin. Nevertheless, we might say there are still two reasons why permissioned ledger products are innovative compared to these traditional distributed database platforms. First, the idea of having a shared ledger has caught on with many businesses and organizations, as in many contexts such a shared ledger seems to offer substantial value. Even if such shared ledgers were possible with previous technologies, it is only because of Bitcoin and the proliferation of permissioned ledger products that this possibility has seriously come on the agenda. Second, permissioned ledger products make distributed consensus systems easier to build among parties who do not completely trust each other in a competitive environment.

As recently noted by the developers of Corda, "In particular, each financial institution maintains its own ledgers, which record that firm's view of its agreements and positions with respect to its customer set and its counterparts. Its counterparts, in turn, maintain their views. This duplication can lead to inconsistencies, and it drives a need for costly matching, reconciliation and fixing of errors by and among the various parties to a transaction. To the extent that differences remain between two firms' views of the same transaction, this is also a source of risk, some of it potentially systemic. A plurality of financial institutions drives competition and choice but the plurality of technology platforms upon which they rely drives complexity and creates operational risk. However, until recently, this was unavoidable: except for centralised market infrastructures, there were few effective ways to consolidate technology across firms without also consolidating the firms themselves" (Brown et al. 2016, p. 3).

7 The value of distributed ledger technology

Public discussions about the Bitcoin system, particularly regarding its intended purpose and supposed value, are often mired in controversy. But in my own view the primary purpose of the Bitcoin system must really be seen as political, namely to offer sound money in digital form. The term sound money traditionally refers to money in the form of gold or silver, or in paper form but backed by those precious metals, to be contrasted with money that exists purely due to government fiat. In digital form, the main intention behind Bitcoin is to provide a money that, compared to fiat currencies, (1) is a better store of value, and (2) more enables financial sovereignty. A key aspect to that value proposition is the attempt to wrest some control over our money production and flows away from states and banks, and to make governance over network activities and rules decentralized. Importantly, Bitcoin at its basis is, thus, not primarily intended to provide its users with cheaper and faster transactions, as is commonly supposed. At its basis, Bitcoin is about offering a qualitatively different type of money.

This is not to say that the Bitcoin system could not be valuable in some other way than only as sound digital money. As already mentioned, there may be ways to scale the Bitcoin system through innovations such as the Lightning Network, so that it can indeed perform better as a payment system, particularly in terms of costs. Perhaps there is potentially a lot of value to creating other types of digital bearer assets on top of the basic Bitcoin system, from playing cards to stocks. The tamper-resistance property of the Block Chain makes it appealing for storing certain data references, such as seen in the OpenTimestamps application. Bitcoin, in fact, really seems to be a new category of thing that may have various, currently difficult to imagine applications. But at the core, in order for Bitcoin to be secure, requires its desirability as money. In addition, as money is one of our most fundamental social institutions, it should also be this application and potential of Bitcoin that should be treated as most important.

Clearly, Bitcoin still has a lot of challenges with regards to the sound money proposition. To be a store of value, for example, bitcoin still has too high a degree of volatility. Nevertheless, the potential for becoming sound money is certainly there. Most importantly, this is because power over the activities on the network and the rules that govern it indeed seems to be distributed among a community, rather than concentrated with one or a small group of entities. This was attested to in the last year by the failure of several large miners and Bitcoin companies to impose their will regarding governance of the network, against the majority of the community. It is precisely this decentralized character of Bitcoin that makes it innovative as a system, and that to a large extent separates it from alternative cryptocurrency systems, which generally do not have the same degree of decentralization.

Although permissioned ledgers and public blockchains such as Bitcoin are often presented as two different models of the same basic concept-most vividly in employing the distinction between “private” and “public” blockchains as is commonly done-this is far from the truth. Permissioned ledger systems have an entirely different purpose, namely to help build a

[13] See Chaia et al. 2009.

more reliable, common view of the interactions and agreements between enterprises.

This is particularly important in financial services. Given that its IT landscape is vast and scattered, used for millions of data messages regarding financial assets and contracts each day, there are a number of potential advantages for financial institutions in building a more reliable, common view on business interactions through a shared ledger system. Operational simplification is probably the major advantage. By improving the integration of the financial IT landscape, it is less likely that these systems will have diverging views on the same interaction. If such a divergence does occur, it will be easier resolve. This operational simplification would lead to a significant reduction in risks and substantial cost savings. But there are other advantages too. In some contexts, for example, this more reliable, common view can help simplify the tasks of regulatory compliance, reduce counterparty risk, and decrease the potential for fraud. More broadly, the business to business platforms which these permissioned ledger systems can enable, offer the potential for new business models.

Though shared ledgers can offer significant value to financial institutions, it is important to realize they are not the magic bullet they are often presented to be. They will not solve all the challenges and problems financial institutions currently face with the push of a button. To start, any project to build a shared ledger application will need to peruse carefully how exactly the concept should be implemented. Even more importantly, the success of such projects usually rides on much more than just this piece of technology. They often require building out more tightly-knit ecosystems, improving operational processes and standards, revising business and commercial models, better adhering to regulatory frameworks, improving security practices, change management, integration, and the rest of the technology toolbox. The key to success of any shared ledger project is, in fact, managing all these aspects to building an application.

8 Conclusion

Distributed ledger platforms all have in common that they enable the storage of ledger entries among a network or subnetworks of actors who participate in the platform. It is common to treat all these types of platforms as variations on the same basic model. But, as the discussion has shown, this is clearly not the case. First, Bitcoin should be carefully distinguished from its 1000s of competitors. Second, we need to draw a clear distinction between public blockchain systems and permissioned ledger systems, which differ vastly in their purpose and design.

Bitcoin solves the double spending problem in an open network without verifiable identities and, therefore, has enabled the creation of decentralized digital cash. In this regard, the inherent cryptocurrency, the proof of work mining process, and the network effects it has enjoyed in recent years are essential to Bitcoin's sound operation. Though others have set up similar open decentralized networks such as Bitcoin, all of these seem to have substantially less security than Bitcoin. Although there are potentially other promising applications for the Bitcoin Network, it should always be remembered that the primary purpose is a politically motivated, decentralized digital cash system; without that system, Bitcoin will not function.

Other than perhaps having acted as an accelerator for activities in this area, Bitcoin has little to do with permissioned ledger systems. Their direct purpose is to help create better integrated views business interactions and agreements. This may have a number of benefits, but in the financial industry is particularly important with respect to reconciliation efforts. In a broader sense, the importance of these platforms should be seen primarily as an enabler of business to business networks. These often cross-border, cross-sector platforms can unlock as much as $10 trillion of business and societal value in the next decade according to the World Economic Forum (2017).

References

Antonopoulous, Andreas. 2014. Mastering Bitcoin: Unlocking Digital Currencies. Sebastopol, California: O'Reilly Media.

Breckenridge, S.P. 1903. Legal Tender: A Study in English and American Monetary History. Chicago: The University of Chicago Press.

Brown, Richard Gendal, James Carlyle, Ian Grigg, and Mike Hearn. 2016. Corda: An introduction. Avail-able at < https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda2fdebbd1acc9c0309b2/1472045822585/corda-introductory-whitepaper-final.pdf> (last accessed June 12, 2017).

Chaum, David. 1983. Blind signatures for untraceable payments. Advances in Cryptology Proceedings, 82, 199-203.

Chaum, David, Amos Fiat, and Moni Naor. 1988. Untraceable electronic cash. Advances in Cryptology, 403: 319-327.

Graeber, David. 2012. Debt: The First 5000 Years. Brooklyn, NY: Melville House Publishing.

Haber, Stuart and Scott Stornetta. 1991. How to time-stamp a digital document. Journal of Cryptology, 3: 99-111.

Lamport, Leslie, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4: 382-401.

Mujagic, Edin. 2016. Boeiend en Geboeid: Een Monetaire Geschiedenis van Nederland sinds 1814/1816. Blaricum, the Netherlands: Ezbook.

Nakamoto, Satoshi. 2008. A peer-to-peer electronic cash system. Available at <https://bitcoin.org/bitcoin.pdf> (last accessed June 12, 2017).

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. Bitcoin and Cryptocurrency Technologies. Princeton: Princeton University Press.

Poelstra, Andrew. 2015. On stake and consensus. Available at <https://download.wpsoftware.net/bitcoin/pos.pdf>.

Rid, Thomas. 2016. The cypherpunk revolution: How the tech vanguard turned public-key cryptography into one of the most potent political ideas of the 21st century. Christian Science Monitor, July 20.

World Economic Forum. 2017. Digital transformation initiative: Unlocking B2B platform value. Geneva: World Economic Forum.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com/nl-nl

For more information contact:

Jan-Willem Burgers
Capgemini Financial Services Benelux B.V.
Technology Lead Europe, Distributed Ledger Practice
Email: financialservices.nl@capgemini.com

People matter, results count.

IN/05-022.18 © Shutterstock photos