To Centralize or Decentralize: What is the Question? An Application to Digital Payments

Ron Berndsen, Ruth Wandhöfer

To centralize or decentralize: what is the question? An application to digital payments[1]

Ron Berndsen[1][0000-0002-8340-9041] and Ruth Wandhöfer[2]

[1] Tilburg University, Tilburg, The Netherlands
LCH Ltd and LCH SA,
[2] CASS Business School, London, UK
ron.berndsen@tilburguniversity.edu,
ruth.wandhofer@cass.city.ac.uk

Abstract. Computing in the general sense of the word has been centralized in the early days of IFIP (1960s) with mainframe computers and became distributed in later decades (1980s) with stand-alone personal computers. Then distributed ledger technology was introduced and the arrival of Bitcoin emphasized the intention in addition to distribution to also decentralize the system as much as possible. In this article we focus on the meaning of centralized versus decentralized computing and apply this to the world of digital payments.

Keywords: distributed ledger technology, Bitcoin, centralized computing, decentralized computing, digital payments

1 Introduction

Computing in the general sense of the word has been centralized in the early days of IFIP (1960s) with mainframe computers and became distributed in later decades (1980s) with stand-alone personal computers. Subsequently, the internet connected those personal computers and computing became mobile. In 2009 the Bitcoin network started to mine the first bitcoins. The intention of bitcoin is to decentralize the system as much as possible out of a lack of any trust in intermediaries. Initially, because of the Lehman crisis financial institutions were the target to disintermediate but within a couple of years distributed ledger technology became a hype, trying to cut out intermediaries in almost any sector of the economy. The next major development in payments will probably be the introduction of central bank digital currency (CBDC). This means opening up the possibility of consumer (retail) payments in central bank money in a digital form where the trend seems to be to move back to centralized but distributed systems.

There is still substantial confusion about what decentralization in the above-mentioned trends entails [15]. In this article we focus on the meaning of centralized versus

[1] The views expressed in this paper do not necessarily reflect the views of our affiliations. All remaining errors are ours.

decentralized computing in terms of governance and geographical location. To illustrate and make the difference more concrete, those concepts are applied to the world of digital payments or in general the transfer of monetary or financial value. In section 2 we provide a working definition of (de)centralization. In section 3 we present the centralized world of financial market infrastructures. Section 4 provides examples of decentralized means of payment such as bitcoin. Section 5 discusses central bank digital currencies in two prominent cases: Sweden and China. Section 6 concludes briefly.

2 Working definition of decentralization of governance

In order to set the scene, we will begin this section by explaining the core differences between centralized and decentralized systems. From the literature, e.g. [8], it appears that it is difficult to arrive at an all-purpose definition of centralization and decentralization as it depends very much on the domain of application as well as the aspect under consideration.

The domain we will be examining is that of computer systems, which are the underlying operating systems for the transfer of value in digital format, i.e. in a broad sense the exchange of fiat currency (the official currency of a country) as well as cryptocurrency or crypto assets. For simplicity we will refer to such systems as 'payment systems'. In general, a payment system consists of a network of one or more nodes where nodes can have the same function or different functions. If all nodes have exactly the same function, we will call such nodes 'peers'.

Governance in Centralized Systems

The first question to ask in order to establish as to whether a system is centralized is the following: 'Is there a single decision maker?' With a single decision maker or central authority, the well-known advantages of a centralized system become immediately clear: those systems are simple to administer and reaching 'consensus' is cheaper and faster compared to truly decentralized computing. The underlying reason for centralization in the system context, including computer systems, is the network effect. The positive utility of the network effect increases with more participants joining – a reinforcing cycle. The drawbacks of centralized systems are of course the single point of failure at the governance level, the lack of controllability of the user vis-a-vis the single decision maker and the possibility of censorship.

Governance in Decentralized Systems

In contrast to the centralized system, the question we ask here is 'Are there several decision makers, which ensure that no single individual or entity is in control?' If the answer is affirmative, we are dealing with a decentralized system: there is no single entity representing authority. Instead we encounter a plethora of authoritative nodes, which are in charge of serving a group of end users. Full decentralization would denote that decision-making would be dispersed across all participants. Full decentralization

would therefore imply the absence of any form of influence, power, or control over developers or contributors.

The advantage of a decentralized system is its resiliency and redundancy, which however tends to also make it more costly in terms of computing and more complex to manage. In the early days the Internet was an example of a decentralized system, which however has evolved into a much more centralized system when we think about the controls that governments have established within it.

There is one overarching type of governance architecture when creating decentralized systems in the space of distributed ledger technology: public/un-permissioned ledgers. A public blockchain typically aims at providing anonymity or pseudonymity, the governance structure is cooperative, and the association or network is aimed at being democratically controlled based on the consensus mechanism employed.

In practice there are many hybrid versions that may be public but still permissioned and are therefore not completely decentralized given that a gatekeeper function is established in order to limit participation in the decision making of the system. Examples include the Ripple ledger and Hedera Hashgraph among others. In terms of permissioned blockchains there are state run distributed ledgers (DLs), e.g. for land registries or identity management systems (Estonia) where stakeholders elect board members that provide a certain level of know-how and direction and where a broad audience may be able to view the ledger but only select entities can validate and process transactions. There are also private blockchains where the aim is the creation of applications for the business and where the management board are the primary stakeholders or owners and they ultimately govern the direction of the system. And we have seen consortium-run permissioned DLs which are managed by a group of organizations such as financial institutions (for example R3 Corda) where a process is followed to elect or remove members that hold seats on collective boards as part of the network.

It is important to note that the openness of the system, i.e. unpermissioned versus permissioned or hybrid, as well as the consensus mechanism which governs the transaction validation process all have a direct impact on the degree of decentralization in terms of governing the underlying system. So, (de)centralization is not a binary concept. The major consensus mechanisms, which we want to mention here as a manifestation of governance, are Proof of Work and Proof of Stake.

Proof of Work is commonly seen as the first type of consensus mechanism that was used in a public blockchain, specifically the Bitcoin Blockchain [13]. Proof of Work uses a process of mining where the nodes, which keep the network operational, solve complex mathematical problems through the use of computing power. The more computational power used, the faster the asymmetric mathematical problems that need to be solved in order to calculate the hash of a new block [17]. For solving these problems, miners are then rewarded with coins in return. In order for the miners to make a successful attempt at identifying the winning block they randomly vary what is termed a nonce, the timestamp of the previous block. Node operators are incentivized in the Proof-of-Work model by rewards of transaction fees and block rewards if and only if the block they have identified is included in the chain [14]. Due to this architecture, it is often assumed that it is difficult for any one party or entity to control the majority of total computational power and thus prevent a Sybil attack from occurring [6].

Proof of Stake utilizes a randomized process to identify who or what will determine the consecutive block. In order to be considered by the process a certain number of tokens must be staked/locked up for a particular duration. Once this is done, the entity will become a validator on the network whereby they are able to discover new blocks of data and receive a reward if the transaction is included in the chain. This is the protocol that is aimed to be used in Ethereum, which will undergo a shift from the Proof of Work mechanism to a Proof of Stake one, planned to occur by 2021. Proof-of-Stake is considered to be more energy efficient than Proof-of-Work [12]. The central tenet to the various Proof-of-Stake mechanisms is that the node, which is allowed to propose a consecutive block, is determined by the proportion of a particular digital asset being staked. This assumes that the more an entity, individual, or group stakes, the less likely they will attempt to sabotage the decision-making process because they have 'skin in the game' [17].

Furthermore, there are a variety of hybrid solutions that have emerged or are beginning to emerge, which include private databases on public blockchains, or off-chain storage units with a public blockchain, alternatively open consensus but permissioned governance (e.g. Hedera Hashgraph with their 39 multination corporates serving as their Global Governing Council and their main node operators) but also Ripple. Although these hybrid models do not allow any individual or entity to participate, they are partially permissioned environments. Due to this there have been implementations of Proof of Authority where the consensus itself is determined by selecting or randomly selecting an authority and it is assumed that these authorities are trustworthy to determine the most recent version of the database [1]. There are many other consensus mechanisms that exist and that are being researched, tried, and tested including proof-of-existence, proof-of-burn, proof-of-elapsed time.

In terms of practical application of these three key definitions we see that systems can either operate on a pure basis, e.g. a fully centralized system, or they can combine features of two types of systems, e.g. a centralized and at the same time distributed system. In the paragraphs below we depict the definitions reflecting this.

Distributed Systems

In order to find out if a system is distributed, the question to ask is 'Are all actors (or nodes in computer system terms) in the same geographical location?' A negative answer means that the system is distributed. Distribution therefore refers to the geographic location of the 'nodes' and the storage of the recorded data, as well as the location of the requisite computational power being utilized. Control by one or more entities has no bearing on whether a system is distributed. The most important difference between a decentralized and a distributed system is that in the latter every node is in communication with every other node such that they all behave as a single unit. Whereas the processing in the system is distributed in the sense of being shared across the nodes, decisions are centralized as the nodes behave in a collective decision-making process. In a fully distributed system, there are no end users and only individual nodes. The database is distributed to all participants and viewable in real time. When we compare this to the way Bitcoin operates today, we can see that a tiering of participants took place and we have many end users that are not running a node themselves but relying

on other nodes (e.g. a crypto wallet provider or crypto exchange). This also means that they do not see the full Bitcoin blockchain but instead are being presented with a recent snapshot in relation to their transaction [16].

Overview of the four dimensions

To conclude this section, within the domain of payment systems, we present the three different system characteristics discussed above applied to digital payments in Table 1.

		Governance	
		Centralized	Decentralized
Geographical Location	Concentrated	Classical Mainframes	_
	Distributed	Multiple sites Cloud computing	Pure Bitcoin system

Table 1. The four dimensions of (de)centralization and distribution/concentration

First aspect: in terms of governance, centralization means the presence of a central authority, which controls the payment system and is responsible for its operational services to its users. The central authority has complete control and up-to-date information about the state of the system [3]. A central authority may be a single person or a small group – in terms of the ledger, which is also relevant for our purpose – which has the exclusive power to write and update the ledger. We also distinguish IT-wise between 'run' and 'change'. In a governance-centralized system the single authority also decides how to change the system i.e. on the content and timing of new software releases.

A fully decentralized system from a governance perspective is a system where there is no central control and responsibility only exists at the level of peers i.e. individual nodes which all have full autonomy, e.g. each node can decide to join or leave the network by itself. The way to achieve a uniquely defined state in a decentralized environment is by consensus.

Looking at the issue of running versus changing the software, it is an intriguing question whether full decentralization in terms of changing the software is really possible. This only seems to be the case if every peer is in principle able to propose and effect a new software release. Consensus is then reached if other peers adopt that release and reach a majority over time. Peers, which keep running an old version or are in a minority using the new version would then represent the outcome of decentralization.

Second aspect: As far as the location is concerned, payment systems will to some extent have a geographically dispersed structure nowadays. The obvious reason is adequate business continuity: in order to be resilient against all kinds of natural hazards the system needs to have nodes that have a distinct geographical risk profile (see the principle on Operational Risk in [5]) such that a single incident (e.g. flooding, fire, earth-

quake, gas explosion) will not impact all nodes of the system. Hence, a fully concentrated payment system – i.e. in terms of location - will not exist anymore [5]. Every payment system will be distributed in terms of location. Applied to the concept of ledger, this implies that ledgers will be decentralized to some extent. The term distributed ledger or distributed ledger technology does therefore not refer to decentralization in terms of geographical location. In that sense all ledgers of payment systems are distributed nowadays.

For the remainder of this article, we will take as a working definition for the term decentralization to mean decentralization in terms of governance. Furthermore, (de)centralization is not a binary concept; we will allow for a certain degree of decentralization as some functions or actions can be delegated.

3 Centralized systems: Financial Market Infrastructures

Building on the concepts of decentralization and distribution of the previous section, we will discuss a prominent class of centralized but distributed systems in this section: Financial Market Infrastructures (FMIs). These infrastructures take care of the fundamental task of providing the function of transfer of value (monetary and financial) to an economy. There are four main types of FMI: Automated Clearing House (ACH), Systemically Important Payment System (SIPS), Central Securities Depository (CSD) and Central Counterparty (CCP). Additionally, there is fifth type of FMI, the Trade Repository. However, that type does not play a role in the payment, clearing and settlement processes. Instead it provides ex-post transparency on over-the-counter derivative transactions. Every FMI performs a specific function for its participants (Ps) which can vary from a few dozen to several thousands. Given the various types of FMIs it may be insightful to use a stylized network structure for visualization. In Figure 1 the different FMIs are depicted in a multiplex consisting of three layers [4].

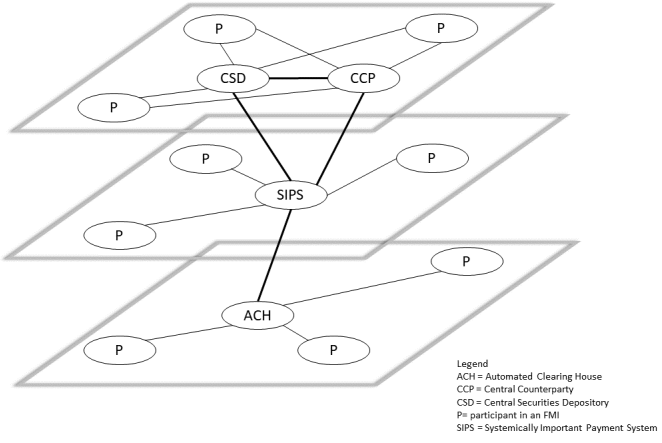

Fig. 1. FMI Multiplex

The bottom layer represents the network of retail payments with the Automated Clearing House in the center. The ACH acts as a concentrator: the millions of individual payments (part of which may be in batches) are collected, aggregated per participant and multilaterally netted (this process is called clearing). The resulting long or short position of each participant is then sent by the ACH to a Systemically Important Payment System.

Located in the middle layer of the multiplex, the SIPS perform the actual transfer of value (settlement) by debiting the account of all 'short' participants and crediting the account of all 'long' participants. If this is all successful, the SIPS send the positive result back to the ACH. In general, the SIPS will be operated by the central bank and uses the Real-Time Gross Settlement mode where every transaction is settled individually (gross settlement) and processed as soon as possible after receipt (real-time). In addition to acting as the settlement agent for the ACH, the SIPS also perform settlement among its participants for various purposes such as large-value payments, monetary policy and settlement of securities transactions (payment side).

The top layer contains two FMIs: the central securities depository settles securities transactions (settlement of the delivery side); the central counterparty clears (comparable to clearing by the ACH) and in addition mitigates pre-settlement risk. The latter means that if a participant would default prior to settlement, the CCP would take over the portfolio of the defaulter thereby guaranteeing that all obligations and rights of that portfolio are maintained.

All FMIs are centralized in the sense of their governance: the Board of the FMI is the central authority which controls the system and is responsible for its operational services to its users. The day-to-day operations are delegated to operational departments within the organization of the FMI. The transactions that are sent in by the participants are validated by the FMI, subsequently processed by the FMI, and the results are sent back to the participants, hence the FMI has complete control and up-to-date information about the state of its system. The underlying reasons for centralization are straightforward. First, as the Board is responsible and accountable, it wants to ensure that the FMI is performing as it should, which supposes ultimate control. Second, regulation and supervision apply to each FMI, given that these are usually systemically important: the multiplex of the euro area transfers a total amount of value every working day of € 6,700 bn., roughly half of the annual Gross Domestic Product (GDP) of the euro area. Third, FMIs need to process many transactions and/or complex transactions in short timespans, which in industrial applications so far is only possible using traditional databases and client-server configuration.

The fact that in the multiplex governance is centralized per FMI does not mean that FMIs are geographically concentrated. In reality, FMIs are distributed in order to be operationally resilient (business continuity) as well as cyber resilient. FMI's operate a two (or more) data center configuration, which are geographically distinct so as to minimize the risk that all data centers are affected by a single incident, yet close enough to allow for synchronous communication. In this regard, the increasing use of cloud services for computing, storage and backup by FMIs implies a potential further dispersion of location but also provides for an extra layer of defense against cyber risks. In case

one datacenter suffers from a cyber-attack, the other datacenter will be infected immediately as well because of the synchronous communication between the two. A disaster recovery or datacenter in the cloud may then provide a cyber-resilient option in the form of an earlier known-to-be-good state of the system with minimal data-loss. All in all, at the time of writing centralized processing is still superior in terms of performance compared to the decentralized techniques discussed in the next section.

4 Decentralized systems

A good example of a decentralized and distributed system is the Bitcoin blockchain, which we will discuss in this section which is largely based on [16]. In practice, blockchain is considered a type of DLT that utilizes cryptographically-linked blocks to store data through hashes in a distributed data architecture, whereas distributed ledger technology is any form of ledger-based technology whether using hashes and linked blocks or not but which does utilize ledgers in a distributed data architecture environment replicated across the network as part of the system. The ultimate benefit of any such system is to effectively transfer value directly to another party or entity.
In addition, we will also explain the emerging Libra project, a form of e-money that is aiming at providing domestic and cross-border retail payment services over the coming years.

The Bitcoin System
In 2008 Nakamoto postulated a protocol and network for exchanging value that would not rely on financial institutions as centralized trusted third parties but instead be based on cryptographic proof. As such it is aimed at functioning in a completely trust-less world. The problem of creating a workable system in a trust-less environment is a difficult one, which previous attempts to create electronic cash systems such as e-gold, Liberty Reserve etc. could not solve. In essence, it relates to two important challenges in distributed computing:

1. the Byzantine Generals Problem [10] which describes the difficulty of ensuring the secure exchange of messages in a network of unknown participants that cannot be trusted; and
2. the Double Spending Problem [7], which occurs when electronic cash can be spent twice or more times by broadcasting malicious transactions to the network, which has no central authority to check and track transactions and thus cannot validate the correct sequence of transactions.

The solution to these two problems provided in [13] builds on a particular combination of well-known algorithms for asymmetric cryptography such as SHA-256 (Secure Hash Algorithm) and Proof of Work consensus algorithm Hashcash developed in [2]. The key differences and similarities between Bitcoin and traditional payment systems are summarized in Table 2 below.

Payment Systems	Bitcoin Blockchain
• Network with a central operating node	• Distributed network
• Account Based	• Cryptographic Keys
• Fiat currency (backed by or in central bank money)	• Private cryptocurrency (not backed)
• System and currency are separate	• System and currency are integrated
• Highly regulated and supervised	• Not regulated and in parts almost impossible to supervise
• Full information/transparency on sender and receiver by central operator	• Pseudonymity, with option to separately combine data to identify individuals
• Batch or single transaction processing	• Batch processing
• Within ledger transfers	• Within ledger transfers
• Multitude of ledgers with no common view and associated complexity, significant reconciliation costs for participants	• One immutable ledger or transaction log, that is shared with all participants and updates automatically

Table 2. : Comparison of Bitcoin and payment systems

Blockchain technology is a type of distributed database, which is shared across a computing network. Within the blockchain network, each computer node maintains a full copy of the database. Nodes are the hardware or software that broadcasts or transmits information to begin the transaction process which, if validated will result in a new appended block. Nodes also contain full copies of the total transaction history of the network.

In the Bitcoin system specific algorithms plus the use of cryptography enable the creation of consensus over transactions in the system, which result in a chain of verifiable transactions on the DL, thus removing the need for a central authority, e.g. a bank. The ledger is distributed to all users of Bitcoin and the system is decentralized, i.e. administered by multiple authoritative nodes. The key is the underlying decision-making governance and the way information is shared through the control nodes in the system. A miner, responsible for the validation of transaction blocks, must necessarily always be operating a node in the Bitcoin blockchain. Every new piece of information added to the data base is added as a block of data along the historic data chain, which records information in the database. The aim of the Bitcoin blockchain is to allow parties who do not necessarily trust one another to agree on information and to engage in a series of different activities directly in an encrypted and pseudo-anonymous way through the use of public and private cryptographic keys. A public key is the identification of the storage of an individual's or entity's digital assets, and a private key provides access to their unique storage facility.

In practice the Bitcoin system however has been displaying increasing signs of control and at this stage it appears that only a few coders maintain and evolve the ledger's core algorithm (and for those that do not agree these code changes can result in a 'hard fork').

With regard to our classification the Bitcoin system can be considered as decentralized and distributed, with the level of decentralization having decreased over time. Decentralization still therefore makes it impossible to be regulated from within, which is why all applicable regulations at this stage, such as Anti-Money-Laundering and Know-Your-Customer (KYC) rules, only apply to entities and processes at the nexus between the Bitcoin system and fiat currencies, administered in most cases by cryptocurrency exchanges and crypto wallet providers.

Libra 1.0 and 2.0

In June 2019 the "Libra Association", founded initially by Facebook, announced its plan to launch a new global digital currency. Referred to as "Libra", the cryptocurrency would be supported on the "Libra Blockchain" and governed by the Libra Association. On the Libra Blockchain, users can utilize Libra as a lower-cost means of payment, providing efficiency, cross-border capability and financial inclusion. Initially scheduled to launch in the first half of 2020, since its announcement, Libra has been the subject of significant attention from governments and regulators alongside interest from the emerging and incumbent financial services ecosystem.

Libra is being widely described as a cryptocurrency, but while it has similarities to existing cryptocurrencies such as Bitcoin, it also has key differences.

Libra will be a "StableCoin" – that is, its value will be pegged to a pool of stable and liquid assets, which the Libra Association has called the "Libra Reserve". The goal of the Libra Association is for Libra to be used as a transactional currency, rather than exploited for speculative or investment purposes. The Libra Reserve will therefore be structured with capital preservation and liquidity in mind. The Libra Reserve is planned to only hold fiat currencies and government securities from stable and reputable central banks. The aim of this is for Libra to be far less volatile than Bitcoin and other cryptocurrencies, which will make it easier to use for transactional purposes.

In addition, unlike Bitcoin, Libra will be a permissioned currency. Only "Validators" – the Libra Association's founding members – will have the power to verify and validate transactions on the Libra Blockchain, earning transaction fees denominated in Libra. These Validators will be granted voting rights based on the number of coins they hold. Due to the size of the network, it should be sufficiently wide to prevent single bad actors from causing disruption. Validators will be selected for their ability, in aggregate to keep costs low and to smooth capacity.

In response to significant challenge by policy makers and central banks around the world a refreshed version, the "Libra White Paper 2.0" [11] was published on 16 April 2020. This second version sets out four key changes:

1. Extension from the global multi-currency Libra coin to include selected single currency StableCoins

2. Reinforced Anti-Money Laundering (AML) and sanctions approach, including a compliance framework, moving away from the initially envisaged outsourcing of KYC checks to wallet providers.
3. Abandoned plan to move from a permissioned network to a permissionless system over time.
4. Development of a capital framework (including a buffer) for the Libra Reserve to increase operational resilience.

When applying our criteria on centralization and distribution, the Libra proposition can be described as centralized and distributed, with initial plans of moving towards more decentralization – via the ambition to potentially move from a permissioned to a permissionless DL – being abandoned as a consequence of regulator demands. In addition to the challenges that Libra faced from central banks and policy makers the refocus of Libra is also relevant with a view to becoming a platform to distribute CBDCs as they come to the market, rather than potentially rivalling sovereign currencies.

5 Central Bank Digital Currencies

Beyond centralized payment systems and infrastructures and distributed and decentralized systems in the cryptocurrency space there is third emerging strand, which will impact the payment infrastructure landscape – Central Bank Digital Currencies (CBDC).

Christine Lagarde, at the time Head of the International Monetary Fund (IMF), made a public statement underlining the importance of central banks to reconsider their role as money issuer in the digital age, emphasizing key principles and design considerations [9]. Simply put, where cryptocurrencies allow for zero control, central-bank owned platforms would give regulators control back, making innovation in money issuance a key priority for central banks. No surprise therefore that a number of research and pilot projects have been developing over the last few years with many central banks and supranational bodies including BIS and IMF issuing research papers and results of Proof-of-Concepts (PoCs). It is also interesting to note that the theme of Central Bank Digital Currencies (CBDC) is gaining further momentum in the current COVID-19 crisis with different bodies (e.g. Positive Money) calling for central bank digital cash in order to maintain financial stability and limit the mass-privatization of money.

In the following we will shed light on two particular CBDC initiatives, which are significantly diverging in their underlying policy approach and objectives and thus in their degrees of centralization and distribution.

The first case is Sweden, which has been primarily motivated to work on a form of CBDC because of its significantly low percentage of cash usage, which continues to decline. The project started in 2017 and in February 2020 the Swedish central bank announced a general public technical trial for the e-krona. The CBDC DLT solution that has been developed for this purpose will run separately to the country's central payment system, the latter only used by node operators (primarily banks) to swap part of their central bank deposits into e-krona. Wallets will be activated by participants of the DLT (again mainly banks) and users can make retail, Person to Person (P2P) and

transfers between wallets and bank accounts. Different interfaces for smartwatches and cards are also available whilst the option of enabling offline usage is still being explored. The Riksbank emphasizes that this is only a test that is designed to learn about the technology and functioning of the e-krona and that no decision to truly launch a CBDC has been made. The e-krona can be described as a centralized and distributed system. The distributed nature of the DLT solution was a key design factor in terms of resilience, in particular in times of crisis such as cyberattacks. Naturally the DLT system had to be operationally kept separate to the existing centralized and concentrated payment system.

The second case is China, which has been exploring CBDC since 2014 and has recently been in the press announcing the launch of their Digital Yuan in 2020 with trials already in progress in a number of selected provinces. China's CBDC is focusing on replicating cash, in digital form, maintaining the three key pillars of money: transactional/medium of exchange, store of value and unit of account. This means that smart contract deployment will be limited to purely monetary functions. The Digital Yuan is 100% backed by deposits from commercial banks at the Chinese central bank (People's Bank of China, PBoC) and other institutions and operated via a two-tier system as the PBoC has no interest in becoming consumer facing. China's largest banks as well as key conglomerates such as AliPay and Tencent have been identified for secondary issuance of CBDC. For China's government the CBDC is a tool that helps pass on zero or negative interest rates faster than traditional monetary policy mechanisms. However, we are wondering whether reducing the lower bound below zero is really the point here. Since the 2008 financial crisis and certainly in light of the current extraordinary circumstances under Covid-19 it is clear that monetary policy itself needs to be rethought and redefined.

China has been clear that it has no intention to impair the commercial banking sector, hence the two-tier system. The Digital Yuan is also seen as a means to reduce the demand for cryptocurrencies and help consolidate the national currency's sovereignty. A slew of patents for the end-to-end value chain are being issued and implemented, revealing that the solution will operate with "controlled anonymity", where anonymity is maintained between sender and receiver, but transactional information is held by the operator. The national supervisor is able to directly block or restrict wallets that are considered suspicious or in violation of Anti-Money-Laundering (AML), Counter Terrorist Financing (CTF) or tax laws for example. At the same time a selection of different types of Digital Yuan wallets – where the Yuan is depicted in digital bank note format – is being proposed based on users' behavioral data and the identity data provided. Whereas some elements of the solution are building on DLT, for China the need for speedy transactions means that none of the major existing cryptocurrency models, e.g. Bitcoin or Ethereum, are being deployed in terms of consensus and validation algorithms. China's online transaction speeds are up to 92771 transactions per second compared to less than 20 transactions for Bitcoin and Ethereum.

China has also created a National Blockchain Platform, where developers can deploy solutions subject to access permissions – clearly not a decentralized model. It operates on permissioned protocols, which amongst other solutions also leverage Hyperledger

Fabric and Baidu's Xuperchain. Cities will operate their own nodes in what is to become a national information highway. China has also recently launched a national blockchain committee with many leading research institutes and organizations in order to facilitate standard setting, the creation and support of their national blockchain infrastructure and the provision of services nation-wide.

In sum, China's approach is significantly centralized. Even the choice of DLT shows that whilst a certain level of 'controlled' distribution is at play, there is no decentralization whatsoever. In particular, the fact that despite secondary issuance full control in terms of monitoring individuals' transactions at all times remains with the central bank shows that the 'bearer' characteristics of physical cash have been all but removed.

6 Concluding remarks

Centralized but distributed systems (FMIs) for the transfer of digital value still seem superior to decentralized systems (Bitcoin and similar altcoins), in terms of settlement speed, costs and accountability. Therefore, it is not surprising to see that both CBDC approaches discussed in this paper (Sweden and China) are built on a combination of centralization in terms of governance – CBDC is issued by the central bank alone who has the control over its lifecycle – and distribution in relation to the physical location of the data nodes and servers. It is overall highly unlikely that a central bank would opt for a decentralized system of CBDC as this would result in a lack of sovereignty and control over the administration of part of its currency with the same ensuing challenges that we today see in cases where countries, in particular certain emerging markets, show a significant amount of economic activity being transacted in non-sovereign currency, whether that is the USD or Bitcoin. In those situations, monetary policy becomes less effective and transparency around financial flows and trade starts lacking. On that basis it can be safely assumed that we will not see a CBDC model emerging that involves the ingredient of decentralization. Whereas decentralized systems such as Bitcoin and other cryptocurrencies have served as a technology driven inspiration for many actors, from businesses to governments and central banks, it is the element of distribution rather than the decentralized governance that is being more or less embraced.

References

1. Angelis et al. (2018), Angelis, S. D., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. In *Italian Conference on Cyber Security*, 1–11.
2. Back (2002). Adam Back, Hashcash - A Denial of Service Counter-Measure, available at: http://www.hashcash.org/papers/hashcash.pdf.
3. Back and Kurki-Sounio (1989), Ralph-Johan Back and Reino Kurki-Sounio, Decentralization of process nets with centralized control, 1989, *Distributed Computing*, 3:73-87
4. Berndsen (2018), Ron J. Berndsen, *Financial Market Infrastructures and Payments: Warehouse Metaphor Textbook*. www.warehousemetaphor.com.

5. CPMI-IOSCO (2012), Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions. *Principles for Financial Market Infrastructures*, Bank of International Settlements, 2012. www.bis.org/cpmi/publ/d101a.pdf.
6. Douceur (2002), Douceur, J. R., The Sybil Attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Eds.), *Peer-to-Peer Systems*. Berlin, Heidelberg, Springer, col. 2429, 251-260.
7. Garcia and Hoepman (2005), Garcia, F.D., Hoepman, J. H., "Off-line Karma: A Decentralised Currency for Static Peer-to-Peer and Grid Networks", *Applied Cryptography and Network Security*, 364-377.
8. King (1983), J.L. King, Centralized versus Decentralized Computing: Organizational Considerations and Management Options, *Computing Surveys*, Vol. 15, No. 4, December 1983.
9. Lagarde (2018), C. Lagarde, *Winds of Change: The Case for New Digital Currency*, Speech at the Singapore Fintech Festival, 14. Nov. .2018, IMF.
10. Lamport et al. (1982), L. lamport, Shostak, R. and Pease, M., (1982), "The Byzantine Generals Problem", *ACM Transactions on Programming Language and Systems*, Vol. 4, No. 3, 382 – 401.
11. Libra White Paper 2.0, https://libra.org/en-US/white-paper/ (last accessed on 17/05/2020).
12. Malone and O'Dwyer (2014), Malone, D. & O'Dwyer, K. (2014). Bitcoin Mining and its Energy Footprint. In *25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014),* 280–285.
13. Nakamoto (2008), Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. https://bitcoin.org/bitcoin.pdf.
14. Narayanan et al. (2016), Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Oxford, UK: Woodstock: Princeton University Press.
15. Walch (2019), Angela Walch, Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems (January 30, 2019). Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming). *Available at SSRN: https://ssrn.com/abstract=3326244*
16. Wandhöfer (2019), Ruth Wandhöfer, *Technology innovation in Financial Markets: Implications for Money, Payments and Settlement Finality*, PhD thesis Tilburg University and CASS Business School, June 2019.
17. Zheng et al (2018), Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, *14*(4), 325–375.