Bulletin

Vol. 81, No. 5

May 2018

RESERVE
BANK
OF NEW ZEALAND
TE PŪTEA MATUA

Reserve Bank of New Zealand *Bulletin*

Subscribe online: https://www.rbnz.govt.nz/email-updates

For back issues visit: https://www.rbnz.govt.nz/research-and-publications/reserve-bank-bulletin

Copyright © 2018 Reserve Bank of New Zealand

ISSN 1177-8644

Decrypting the role of distributed ledger technology in payments processes

Amber Wadsworth[1]

The financial sector has grown ever more interested in crypto-currencies and the innovative Distributed Ledger Technology (DLT) that underpins them. For central banks, in their role as providers of currency and critical payments infrastructure, a key area of interest is whether DLTs could be used to enhance existing payment processes. This article gives a high-level explanation of how different DLTs can change payments processes. The answer depends on what form the distributed ledger takes. We identify four binary elements that determine the different properties of distributed ledgers and use case studies to evaluate how these elements can improve on, or fall short of, existing payments infrastructure. We find that Blockchain – the most well-known DLT that underpins Bitcoin – brings benefits in terms of the speed of cross-border settlement and improves security by removing the single point of failure, but has drawbacks in terms of slowing the speed and increasing the cost of smaller domestic transactions, and being energy intensive. Some central banks have experimented with other forms of DLTs that try to capture some of the benefits of Blockchain while minimising the costs, but so far these DLTs have tended to mimic existing payment processes and have not demonstrated many additional benefits.

1 Introduction

Crypto-currencies grabbed headlines around the world in 2017 as the value of Bitcoin and other crypto-currencies soared. Much attention focused on the role that speculation played in creating a bubble, but for the financial sector, Bitcoin's soaring value was only one reason to pay attention to crypto-currencies. The other more fundamental reason was the Distributed Ledger Technology (DLT) that underpins them, and the risks and opportunities that the new technology could bring.

For central banks, a key area of interest in DLTs is the role they could play in changing payment processes. The Reserve Bank of New Zealand is responsible for providing critical payment system infrastructure as well as maintaining financial system soundness. Therefore, we are interested in whether DLT could improve payments processes and how the use of distributed ledgers could impact the stability of payment systems. To determine this, we need to understand DLTs and how they differ from existing payments systems.

[1] The author would like to thank Jamie Culling, Andrew Rodgers, Christie Smith, and Tom Smith for their contributions. This article is dedicated to the late Roger Perry who contributed significantly to the direction of this *Bulletin* series.

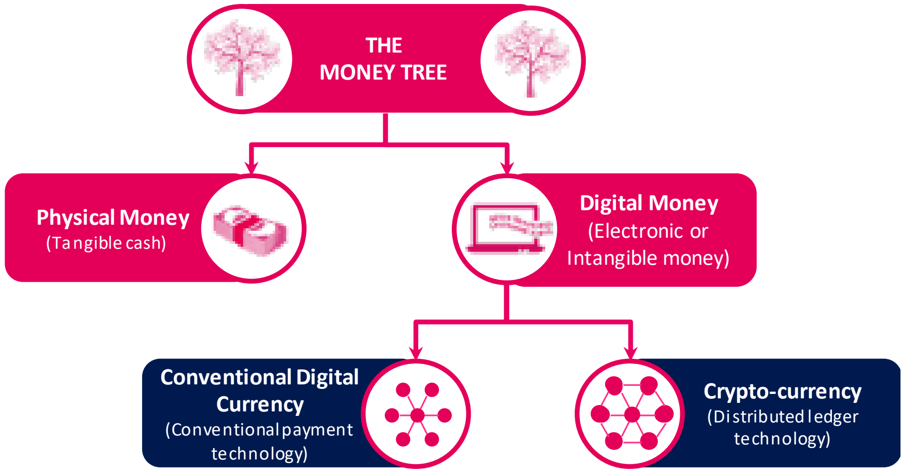
This article provides an overview of DLTs and how they compare to existing payments processes.[2] Section 2 describes how the existing payment process works and how it compares to payments under DLT. Section 3 describes DLTs in more detail, outlining four key elements that determine the characteristics of particular DLTs. Section 4 uses those four key elements to develop a framework for assessing the benefits and costs of different payments processes, and then uses that framework to assess existing payments systems. Section 5 then uses the same framework to evaluate the costs and benefits of different types of DLTs, through several case studies. Section 6 draws together emerging insights on the role DLTs can play in payments processes based on the evidence available so far. A glossary of key terms is included as an appendix.

2 Crypto-currencies, DLTs and how they affect payments processes

What makes crypto-currencies different from other kinds of money?

In an earlier article, we used the 'Money Tree' to help think about different kinds of money (figure 1).[3] On the money tree, crypto-currencies are a branch of digital currency – a form of intangible or electronic money. The key distinguishing feature between crypto-currencies and conventional digital currencies is the payments technology that underpins them. Conventional digital currencies rely on existing financial market infrastructure to conduct transactions, while crypto-currencies rely on Distributed Ledger Technology.

Figure 1
The money tree


THE MONEY TREE
Physical Money
(Tangible cash)
Digital Money
(Electronic or Intangible money)
Conventional Digital Currency
(Conventional payment technology)
Crypto-currency
(Distributed ledger technology)

What is Distributed Ledger Technology?

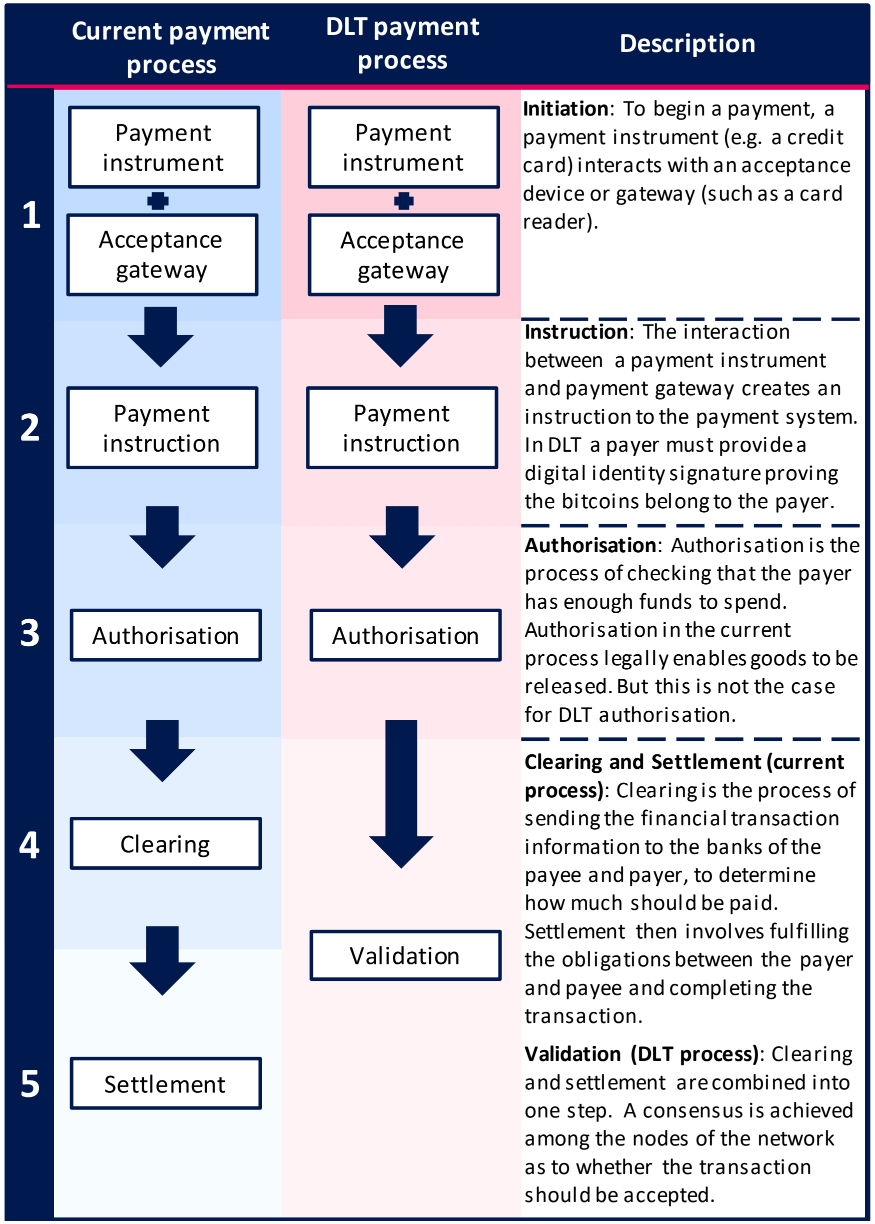
Most people think of distributed ledgers as a digital database that is shared across a network of computers (nodes).[4] The ledger is used to record transactions and ownership of crypto-currencies. The system is distributed, which means records are not held centrally and communicated to nodes by a central authority. Instead, a full copy of the

[2] This is the second article in a three-part series titled 'The central bank digital currency series'. The first article in the series, 'What is digital currency?', explains the different forms that digital currencies can take. The third article in the series, 'Pros and cons of a central bank digital currency', provides a high-level introduction to the pros and cons of a central bank issuing a digital currency.

[3] See Wadsworth (2018a) 'What is digital currency?' Reserve Bank of New Zealand *Bulletin*. Vol 81. No 3.

[4] Mills *et al* (2016) also defines nodes as "the devices running the DLT software that collectively maintain the database records".

Figure 2
Conventional payment process vs DLT payment process



	Current payment process	DLT payment process	Description
1	Payment instrument Acceptance gateway	Payment instrument Acceptance gateway	**Initiation**: To begin a payment, a payment instrument (e.g. a credit card) interacts with an acceptance device or gateway (such as a card reader).
2	Payment instruction	Payment instruction	**Instruction**: The interaction between a payment instrument and payment gateway creates an instruction to the payment system. In DLT a payer must provide a digital identity signature proving the bitcoins belong to the payer.
3	Authorisation	Authorisation	**Authorisation**: Authorisation is the process of checking that the payer has enough funds to spend. Authorisation in the current process legally enables goods to be released. But this is not the case for DLT authorisation.
4	Clearing	Validation	**Clearing and Settlement (current process)**: Clearing is the process of sending the financial transaction information to the banks of the payee and payer, to determine how much should be paid. Settlement then involves fulfilling the obligations between the payer and payee and completing the transaction.
5	Settlement		**Validation (DLT process)**: Clearing and settlement are combined into one step. A consensus is achieved among the nodes of the network as to whether the transaction should be accepted.

ledger is held by every node and updates to the ledger are made when the majority of nodes agree to the change (consensus). A key feature of the technology is that it removes the need for users to trust a centralised payment authority to conduct a transaction and replaces that with an architecture that creates trust through consensus. This innovation has implications for the way payments processes are conducted. However, section 3 will explain how distributed ledgers have evolved to incorporate some centralisation.

How does Distributed Ledger Technology change the payment process?

The process for conducting conventional electronic payments in New Zealand can be broadly characterised into five discrete steps: 1) an interaction between a payment instrument and an acceptance gateway; 2) the payment instruction; 3) payment authorisation; 4) clearing; and 5) settlement (figure 2 provides an overview). The key difference between this process and one relying on DLT is that the final two steps are combined when using DLT.

Existing financial market infrastructure requires payments to be cleared before being settled. Clearing is the process of sending the transaction information to the issuing bank (payer's bank) and the acquiring bank (payee's bank) – communicating who should be paid what, and by whom. Settlement is the actual exchange of money between banks.[5] It is important to distinguish between clearing and settlement because in the current system there is a risk that funds may not be exchanged after

[5] If the payer and payee have bank accounts at different banks, then settlement may involve several obligations. For example, payer to issuer; issuer to acquirer; and acquirer to payee. In New Zealand, the settlement of funds between two commercial banks occurs via their accounts in the exchange settlement account system (ESAS) which is operated by the Reserve Bank. By contrast, if the payer and payee have accounts at the same bank, then settlement occurs within the bank by updating balances to reflect the transaction

being cleared but before being settled. This is a non-trivial risk and could occur when there is a system failure or bank failure. Many protocols have been built into existing payment systems to mitigate this possibility.

By contrast, DLT combines clearing and settlement into one step, which this article refers to as 'validation'. There is no separation of sending the financial transaction information and final interchange of money. Thus, payments on DLT are not exposed to the risk of funds not being settled after the transaction information is finalised, and the number of agents required for the end-to-end payment process is reduced.

To understand how the validation process differs from conventional clearing and settlement, it is helpful to consider the process used by the Bitcoin-Blockchain (Blockchain).[6] A key risk when transacting digital currencies is that they may be spent more than once. Digital currencies are represented by a string of bits. Like any information stored electronically, they are easy to copy and send. Therefore, Blockchain needed to create some way of ensuring that digital money once spent could not be spent again. In existing payment systems, this risk is mitigated by relying on trusted third parties. However, in a payment system where people do not want to trust a central agent,, other methods must be used. In Blockchain, validation of payments relies on 'proof of work', and 'consensus'. Validation is completed once the block of transactions is added to the Blockchain. How 'proof of work' and 'consensus' enable validation is described below:

1. All recent transactions that have been sent to the network are grouped together in a block and are sent to the ledger to be validated. Third party nodes decide which transactions to validate depending on which transaction offers the highest payment. These third parties are referred to as miners because they receive compensation for validating transactions (including newly issued currency).

2. To validate transactions a miner must provide '**proof of work'**. This means they must find a 'hash', which represents all the details in the block of transactions, including each transaction's details.[7] The hash is found by solving a cryptographic problem using brute computing power to guess correct answers. The cryptographic problem is designed to take around 10 minutes to solve (and so is costly to obtain).

3. The 'proof-of-work' hash is shown to the network and the nodes on the Blockchain must then agree that the block of transactions can be added to the Blockchain – this is referred to as '**consensus'**.

4. Blocks are added to the Blockchain only when the majority of the network downloads the copy of the Blockchain that includes the new blocks.[8]

[6] Since the Blockchain was developed, many other DLTs have been created which use a similar blockbuilding method. Therefore, the noun 'blockchain' can refer to the blockbuilding form of DLT, or the Bitcoin-Blockchain.

[7] A hash is a string of numbers and letters which represents an exact piece of information (such as transaction details). If the transaction details change then the hash will also be different. Therefore, hash cryptography can be used to validate the authenticity of information.

[8] Transactions that are not added to the Blockchain are rejected even if proof of work is obtained.

3 Understanding different types of Distributed Ledger Technology

There are many different forms of DLTs and they can have different payments transaction characteristics. Some forms of DLT are similar to existing payment systems, while others differ considerably. These differences result from how the DLT is designed. Four design choices are particularly important, whether the DLT is: 1) permissionless or permissioned; 2) public or private; 3) non-hierarchical or hierarchical; and 4) open source or closed source (table 1).[9]

To illustrate how these key elements matter, consider the example of Blockchain, which is a permissionless, public, non-hierarchical, and open-source DLT. The combination of elements are particularly important in determining how the validation process occurs.

Permissionless, public, and non-hierarchical distributed ledgers require some form of mechanism to avoid the 'double spend problem', that is, to provide secure transactions without requiring trust between nodes. In Blockchain, 'proof of work' provides this mechanism by adding artificial computational difficulty to validating the transaction. The key property of this 'proof of work' test, is that the solution is hard to generate but easy to verify, adding security to the transaction. However, 'proof of work' is also expensive to implement because of the computing power required

Table 1
Distributed ledger technology key elements

1	**Permissionless**	Any node (computer) can download the ledger and validate transactions.
	Permissioned	Permission is required to download the ledger and validate transactions.
2	**Public**	Any node can read and initiate transactions on the ledger.
	Private	Only a selected group of nodes can read and initiate transactions.
3	**Non-hierarchical**	Each node has a full copy of the ledger.
	Hierarchical	Only designated nodes have a full copy of the ledger.
4	**Open source**	Anyone can suggest improvements to the code underpinning the ledger platform.
	Closed source	Only trusted entities can see and add improvements to the code underpinning the ledger platform.

[9] The concepts of private or public; and permissioned or permissionless distributed ledgers is also discussed by Pisa and Juden (2017). Permissioned and permissionless ledgers and differing roles of nodes are discussed by Mills et al (2016) and CPMI (2017).

to validate a transaction. This has resulted in the development of other DLTs that have permissioned, private, hierarchical elements. This type of DLT is used in environments where a trusted third party already exists. Validation can be faster and cheaper in a permissioned, private and hierarchical DLT compared to Blockchain:

- The payer and payee authorise that the payer has enough funds to make the payment.
- A central node (third party) checks whether the funds have not been spent already, and then validates the payment if it is deemed legitimate.
- Ledger balances are updated to reflect payment.

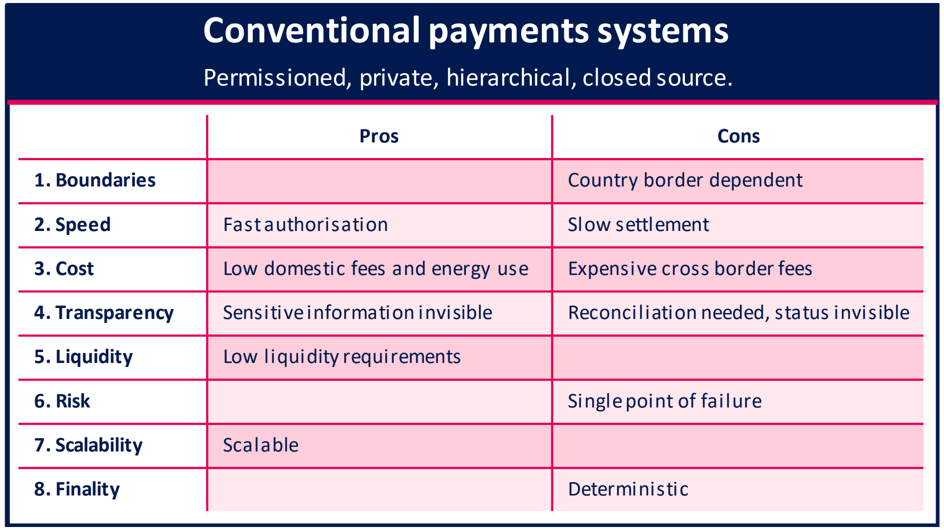
The DLT elements in table 1 are closely related. Whether a DLT is private or public, and permissioned or permissionless, determines whether it may also need to be closed or open source and whether it should include hierarchy.[10] For example, a permissionless DLT would typically not be hierarchical as a full copy of the ledger must be available to all nodes for consensus to take place. On the other hand, developers that design a permissioned and private ledger may also want the ledger to be closed source and hierarchical so as to achieve similar properties of existing payments processes. This leads us to the question of how different forms of DLT compare to existing financial market infrastructure – the focus of sections 4 and 5.

4 A simple framework for assessing payment processes

To assess the costs and benefits of different forms of DLT relative to existing payment processes, we first need to define a set of criteria on which to base that assessment. Here, we consider eight such criteria:[11]

To provide a benchmark for comparison, we begin by assessing how existing payments systems score against the criteria in table 2 (as summarised in figure 3).

Figure 3
An evaluation of existing payments systems.



Conventional payments systems

Permissioned, private, hierarchical, closed source.

	Pros	Cons
1. Boundaries		Country border dependent
2. Speed	Fast authorisation	Slow settlement
3. Cost	Low domestic fees and energy use	Expensive cross border fees
4. Transparency	Sensitive information invisible	Reconciliation needed, status invisible
5. Liquidity	Low liquidity requirements	
6. Risk		Single point of failure
7. Scalability	Scalable	
8. Finality		Deterministic

[10] An additional element that can also be considered is governance of the ledger. This is not considered explicitly in this article outside of the hierarchy element as it has fewer operational implications for the payments process and transaction characteristics.

[11] These criteria fit within the Committee on Payments and Market Infrastructures' (2017) analytical framework for considering DLT arrangements. Some of the elements in the committee's framework are not considered as they are outside of the scope of this article.

Table 2
DLT assessment criteria

1	**Boundaries** – Whether the physical location of payer and payee affects the complexity of the payment system.	Scope
2	**Speed** – Speed of end-to-end payment process including hours of operation and how soon goods or services can be released.	Efficiency
3	**Cost** – Fees and energy costs of transaction processing.	
4	**Transparency** – How much of the transaction process and information is viewable to the public.	
5	**Liquidity** – Liquidity implications for payers and payees	
6	**Operational and security risk** – Risk of payment failure due to operational failure or cyber-attack on a centralised point in the system.	Safety
7	**Scalability** – Whether the payments process can process large volumes of transactions.	
8	**Finality** – How the settlement of the payment is finalised.	

1. Boundaries: Border dependent

Settlement of electronic payments across country borders adds additional complexity to the payments process. Currently, the majority of cross-border payments require international messaging systems to instruct, authorise and clear card payments, as well as correspondent banking relationships to enable money transfers and settlement of card payments. A correspondent bank is a financial institution that performs services for another bank. These include facilitating payments and accepting deposits on behalf of another bank in another country. An international network of payments infrastructure also presents coordination issues between jurisdictions regarding systems compatibility and operational resilience.

2. Speed: Fast authorisation, slow settlement.

In the existing payments systems, the speed of the end-to-end payment process depends on whether it is a domestic or cross-border payment. Domestic electronic payments are processed faster than cross-border payments, which can take up to five days to be processed.[12]

Cards are the most popular payment method in New Zealand. During 2017 each person in New Zealand made 337 card transactions on average.[13] Cards and other forms of electronic payments are convenient because authorisation is very fast. Authorisation in the current process provides legal certainty of the payment which means that goods can be released straight away. For this reason the majority of payment innovations have occurred at the payment instruction and authorisation level of the payments process. For example, contactless card technology. However, these payments will not be settled as quickly.

In New Zealand, domestic electronic payments can wait up to an hour to be settled if they are instructed during operating hours (9am

[12] He *et al* (2017) note that settlement can take up to five days for the majority of common currencies. See also Mills *et al* (2016).

[13] Data sourced from Stats NZ

to 12.15am). However, card payments are not settled until the end of the day. Moreover, electronic payments that are instructed outside of business hours, on weekends, or on holidays, are not settled until the next business day.

3. Costs: Low energy use, cheap domestic, expensive cross border

The energy cost of processing transactions in the existing payments system is relatively low due to economies of scale and network centralisation. This is because it is computationally easy to update ledgers and send messages in the existing payment system, resulting in low energy consumption. Developing and maintaining these closed-source systems is expensive but this cost can be spread over a large volume of transactions. The Ministry of Business, Innovation and Employment (MBIE) estimates that the resource cost of processing card payments in New Zealand each year is around $950 million, but this is only 1.3 percent of the total value of card transactions.[14]

Typically, electronic payments are relatively cheap for payers and payees, but cross-border payments are more expensive. Electronic payments incur fees such as interchange fees or merchant service fees. For example, in New Zealand, domestic card transactions (excluding EFTPOS) incur a fee to the merchant (payee) of between 1.2 to 1.6 percent. This fee is charged by banks and can be passed onto the consumer (payer) via higher goods prices or surcharges.[15] However, cross-border payments require more intermediaries, which results in a greater degree of fee variability.[16] For example, sending money oversees via a New Zealand bank could cost around $9 to $30 per transaction.

4. Transparent: Payment information and processing status not visible

In existing payment systems, payment information is kept private between the payer, payee, and processing intermediaries. In addition, the status of the payment through the process is not visible to all parties. Payers and payees can see when money leaves their account and when it arrives, but they cannot see the status of the payment in the meantime. Therefore, it can be difficult to detect the source of payments delays. This can be particularly problematic for cross-border payments, which rely on a more complex network of financial institutions. In addition, this lack of transparency means that financial market institutions must reconcile their payments records between systems to ensure a correct and complete record of accounts.

5. Liquidity: Fewer liquidity requirements

In the existing payments system, interbank payments are netted before being settled. Netting involves banks counting up what they owe to another bank, then offsetting that amount with what their counterpart owes them. This significantly reduces the number of transactions that need to be settled and the amount of easily accessible funds banks need to have on hand.

6. Operational and security risk: single points of failure present

Existing payment systems are hierarchical and centralised in nature, which creates a risk that an operational failure in the central component of the system could cause failure of the entire payment process. Centralised networks can also be a target for cyber-attacks as they can provide a gateway to the entire system. Therefore, these risks are managed through prudential regulation. In addition, the software is closed source, which means the service providers have greater control over the development of the software. However, service providers must

[14] MBIE (2016)

[15] Retail NZ (2018). In addition, banks charge annual fees to cardholders.

[16] As noted by He et al (2017), the more correspondent banking relationships required for a transaction, the greater the possibility of higher fees charged to the payer.

also ensure the software does not become out of date or vulnerable to cyber-attacks.

7. Scalability: Can process a high volume of transactions.

New Zealand's interbank settlement system (ESAS) processes around 13,498 transactions totalling around $30 billion on average each day. This daily average includes around 1100 retail transactions totalling around $3.9 billion (processed in the SBI system).[17]

8. Finality: Deterministic settlement

In the existing payments process, payments are not final until money has exchanged bank accounts. There is a risk that a payment will be authorised and goods or services released, but the money might not be exchanged. For example, if the issuing bank goes bankrupt in between payment authorisation and settlement. To combat this risk, payments system providers build additional protocols to ensure that after a certain point in the payment process, settlement is legally guaranteed. For example, in New Zealand, retail transactions are processed through the Settlement Before Interchange (SBI) system, which provides legal certainty for the payment settlement before the exchange of money has taken place. Therefore, settlement in existing payments systems can be described as deterministic.

5 Evaluating DLT case studies: Blockchain and central bank experiments

Now that we have set out eight characteristics of payments we can apply them to three case studies of DLT. The first is Blockchain. The second is the first phase of two central bank experiments with DLTs: Bank of Canada's Project Jasper, and Monetary Authority of Singapore's Project Ubin. The third case study is the second phase of the two central bank experiments.

i. Case study: Blockchain

As mentioned, Blockchain is a permissionless, public, non-hierarchical and open-source DLT.[18] The ledger is public and permissionless so anyone can download Blockchain to begin validating transactions. The open-source nature of Blockchain is partially responsible for the growth in DLT since 2008 as at any time a vast number of developers can be building on and improving the code.[19] This section assesses how Blockchain compares to existing payments system infrastructure on our eight criteria (as summarised in figure 4).

[17] ESAS is used to settle payments between New Zealand banks. It processes transactions from SBI as well as two other payment systems: NZ Clear and Assured Value Payment closed user group. These volumes refer to post-netting volumes. RBNZ (2017)

[18] A more in-depth discussion of bitcoin and blockchain technology is given by Kumar and Smith (2017).

[19] Iansiti and Lakhani (2017)

Figure 4
An evaluation of Blockchain

Blockchain

Permissionless, public, non-hierarchical, open source.

	Pros	Cons
1. Boundaries	Borderless	
2. Speed	Faster settlement	Slower authorisation
3. Cost	Cheaper cross border	Higher domestic fees and energy use
4. Transparency	Status visible, no reconciliation	Sensitive information visible
5. Liquidity		More liquidity required
6. Risk	No single point of failure	
7. Scalability		Not scalable
8. Finality		Probabilistic

1. *Boundaries: Borderless*

Blockchain operates over the internet and the currency is not tied to any country, which means the physical location of payer and payee does not matter. This is particularly useful for cross-country payments.

2. *Speed: Faster settlement, slower authorisation*

Payments in Blockchain are processed in 10 minutes and validation can occur at any time. However, if Blockchain payments are being used to purchase goods or services, the 10 minute delay in the payment process could result in a similar delay before the goods or services are released. This is because the payment is not certain until it has been validated, unlike existing payments systems. However, once a Bitcoin payment is validated the payee immediately receives the payment, which is beneficial for individual liquidity management. In addition, the global community of miners in Blockchain means that it is possible for validation to occur around the clock.

3. *Cost: High energy requirements, cheaper cross border, and expensive domestic*

It is more costly to validate each transaction on the blockchain compared to existing payments systems because proof of work is required. Proof of work uses brute computer power to guess solutions to a difficult mathematical problem so may not be considered a socially efficient use of electricity. Currently, Blockchain uses 58TWh per year – equivalent to 1.4 times New Zealand's total annual energy consumption.[20]

Miners also require compensation to incentivise validation and cover the cost of electricity. Some of this comes via newly issued Bitcoins, but some comes from fees placed on payers. The fees vary depending on the payer's willingness to pay – a higher fee increases the likelihood of faster validation. At the time of writing, average Bitcoin transaction fees were around 1 USD but have reached as high as 55 USD.[21] A small fee on Bitcoin transactions would be more expensive than most current transactions fees, but is cheaper than current cross-border transaction fees.

4. *Transparent: Payment information and processing status visible to all*

All transactions on the Blockchain can be viewed by anyone. Each block includes information about when it was added to the blockchain, the transaction hash, and a link to the previous block's hash. This means each Bitcoin contains a complete record of its transaction history. This

[20] https://digiconomist.net/bitcoin-energy-consumption#assumptions https://www.iea.org/publications/freepublications/publication/key-world-energy-statistics.html

[21] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

transparency is necessary for permissionless validation. It also creates a global record of Bitcoin transactions, which reduces the need for payment information reconciliation. That is, it reduces the need to ensure that all records of transactions are matching and correct, which currently exists in conventional financial market infrastructure. However, this level of transparency may not be desirable for commercially sensitive payments.

5. *Liquidity: High liquidity requirements*

Blockchain settles each payment in real time without using netting. This means that more money must be available for settling payments. This does not change consumer liquidity requirements. However, it would result in a higher level of money to be set aside for making payments at a wholesale level compared to the existing payment system (i.e. for interbank and commercial transactions).

6. *Operational and security risk: No single point of failure*

The distributed network is more resilient to a single point of failure. Weaknesses in individual users' computers (nodes) cannot compromise the ledger. However, Blockchain could be attacked in several ways, such as a 51 percent attack, exploiting a bug in the code, or convincing the network to download a compromised version of the blockchain. The open-source nature and global network of users of Blockchain help mitigate these risks because there are many nodes validating transactions. There are also many nodes developing and investigating updates to the Blockchain code. Many of these nodes will have large holdings of Bitcoin so will be interested in protecting the Blockchain. However, exchanges between Bitcoin and other crypto-currencies can reintroduce a single point of failure and result in large thefts. One example is the Mt. Gox exchange hack, where a hacker sold a large amount of bitcoins to themselves at a severely discounted price. In addition, because blockchain is unregulated and still relatively new there may be other unknown sources of operational or security risks.

7. *Scalability: Not scalable*

The computer power and time delay required to validate transactions make Blockchain less scalable to large volumes of transactions. It would currently take Blockchain about a month to process the volume of card transactions New Zealanders make in one day.[22]

8. *Finality: Probabilistic settlement*

Payments on the Blockchain are finalised once validation is completed. However, this finality is based on a high probability that the Blockchain will not be changed and the transaction nullified. The proof-of-work hash and the length of Blockchain make it difficult for a malicious agent to change historical transactions (i.e. fraudulently spending bitcoins that have been already spent). To change the Blockchain an agent would need to control the majority of computing power to provide proof of work for the changed historical transactions. They would then need the newly altered blocks to be accepted by the Blockchain network, which would be unlikely if the changes were doubtful. As more blocks are added to the Blockchain it becomes less likely that it could be changed and so settlement finality can be described as probabilistic.

Summary

Overall, Blockchain has a number of benefits over existing payments systems. It could make cross-border payments simpler, faster and cheaper. It also removes the single point of failure that results in operational and security risks for existing payments systems. However,

[22] Assuming there are 1000 transactions per block and it takes 10 minutes to validate a block of transactions in the Blockchain. There were 337 card transactions on average per capita in New Zealand during 2017. This equates to around 4.5 million electronic card transactions each day based on a population of 4,790,000. Electronic payments data sourced from Stats NZ.

it also comes with a number of costs. It does not improve domestic retail payments, is not scalable and requires high energy use. It would also increase liquidity requirements for payers.

ii. Case study: Phase one of Project Jasper and Project Ubin

The second case study we evaluate is the first phase of two central bank DLT experiments. The Bank of Canada (BoC) and the Monetary Authority of Singapore (MAS) have experimented with DLT and have done so in two phases. Both experiments were limited to testing transactions between commercial banks using a DLT ledger and a crypto-currency created for the experiment. The focus on this case study is phase one of the two experiments. The next case study then evaluates phase two of the experiments by comparing them to our eight criteria (as summarised in figure 5).

However, before we evaluate the DLTs, it is useful to understand the mechanics of the two projects. Project Jasper began in mid-2016 and included the BoC, R3 consortium, six Canadian banks and Payments Canada.[23] In the project, the Canadian banks exchanged Canadian dollars for a crypto-currency. The transactions were instructed and authorised by the Canadian banks and uploaded to the ledger by the remaining members of the R3 consortium using proof-of-work validation. Project Ubin began later in 2016 and included the MAS, R3 consortium, and a group of banks in Singapore.[24] Project Ubin was similar to phase one of Project Jasper but banks in the project could make payments with the crypto-currency outside of operating hours.

Figure 5
An evaluation of Project Jasper and Project Ubin: Phase one

Project Jasper and Project Ubin: Phase one

Permissioned, public, non-hierarchical, open source.

	Pros	Cons
1. Boundaries		Border dependent
2. Speed	Faster settlement	Slower authorisation
3. Cost		High energy use
4. Transparency	Some status visibility, less reconciliation	Sensitive information visible
5. Liquidity		More liquidity required
6. Risk		Single point of failure
7. Scalability		Not scalable
8. Finality		Probabilistic

The motivation of the experiments was to see whether the benefits of Blockchain could be captured, while mitigating the costs. This led to a DLT design that was permissioned, private, and non-hierarchical. Both projects used an open-source DLT platform called Ethereum to develop their ledgers. This is a publicly available distributed ledger that can be coded to have different design elements.

1. Borderless: Border dependent

The ledgers were built for a domestic experiment and not designed for international transactions.

2. Speed: Faster settlement

The ledgers required proof-of-work validation which makes authorisation slower than existing payments systems. However, settlement of payments is faster compared to existing payments systems. Validation of

[23] Payments Canada, Bank of Canada, and R3 (2017)

[24] Deloitte and Monetary Authority of Singapore (2017), Monetary Authority of Singapore and the Association of Banks in Singapore (2017)

payments in Project Jasper occurred only during business hours, but the validation of payments in Project Ubin occurred at any time.

3. Cost: No fees, high energy cost

The experiments did not indicate whether fees were charged to the users. However, the use of proof of work for validation results in an inefficient use of energy per each settled transaction.

4. Transparency: Less reconciliation, and moderate payment information and status visible

The ledgers were designed to be private and permissioned to ensure that only ledger participants could see the payment information. This is important because wholesale payments contain sensitive information. Overall, the ledgers were transparent enough to decrease the need for account reconciliation and increased the status of payments for payers and payees. However, it also resulted in sharing of commercially sensitive payment information between the ledger participants. Both projects identified that this level of transparency was not desirable for interbank payments.

5. Liquidity: Increased liquidity requirements

Payments between banks were settled as they were instructed. This created a much larger liquidity requirement on the banks compared to existing interbank payment systems. High liquidity requirements means more money must be set aside for payments, rather than for more productive activities such as lending.

6. Operational and security risk: Single point of failure

The phase one ledgers were designed to be private and permissioned to enable faster validation. However, these elements also introduced a single point of failure to the ledger. This is because the distributed ledger is now held within a smaller group of computer nodes making them more vulnerable to cyber-attacks. The BoC and MAS both recognised that the reintroduction of the single point of failure resulted in increased operational risks which would need to be mitigated. The DLT platforms are open-source so the experiment benefited from a global network of developers improving and maintaining the platform. However, this comes with a longer term risk that the community may abandon this particular software in favour of another DLT.

7. Scalability: Non-scalable

Similar to Blockchain, the proof-of-work validation to process transactions made the system less scalable to large volumes of wholesale transactions. New Zealand's high value clearing system settles large payments such as house payments and commercial payments. It currently processes around 10,000 transactions each day, which take 0:01 seconds each.[25] It would take about 2.5 months to settle 10,000 transactions using proof-of-work validation assuming a 10 minute delay per transaction.

8. Finality: Probabilistic

Again, similar to Blockchain, proof-of-work validation means that settlement of payments is probabilistic. This means there is a small chance the ledger could be changed to reflect a different history. This chance is increased in this experiment because there are fewer nodes validating payments so the risk of a malicious node gaining access to the ledger and changing the ledger to create fraudulent payments is greater than public and permissionless systems.

[25] HVCS uses a dedicated system to settle payments that is separate to ESAS. Data sourced from www.paymentsnz.co.nz.

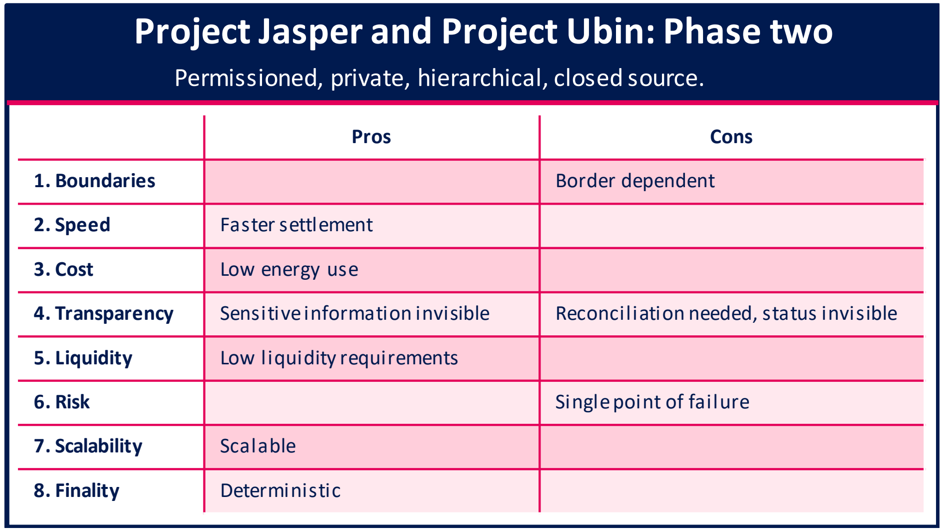
Summary

Overall, phase one of Project Jasper and Project Ubin achieved some of the benefits of Blockchain, including faster settlement, fewer reconciliation requirements and high visibility of the payment status. However, it also resulted in greater visibility of sensitive information between participants and greater liquidity requirements compared to existing payments infrastructure. It also did not remove slow authorisation, lack of scalability, and probabilistic settlement from the DLT. In addition, by adding these privacy and permissioned elements, the projects reintroduced a single point of failure, resulting in greater operational and security risk to the ledger.

iii. Case study: Phase two of Project Jasper and Project Ubin

Phase two of the projects took on the learnings from phase one. Specifically, phase two sought to mitigate the problems of high liquidity requirements and transparency of sensitive information. To do this Project Jasper and Project Ubin used closed-source DLT platforms and designed them to be private, permissioned, and **hierarchical.**[26] The introduction of hierarchy enabled validation to be conducted by a central trusted node and removed the need for proof of work. It also enabled greater information privacy. Transactions are still instructed and authorised by the payer and payee banks but now they are validated by the central node (BoC or MAS) and there is no validation role for R3 members. The central node has a full copy of the ledger and can see all transactions, but the commercial banks can only see information regarding their own transactions.[27] This section evaluates phase two of the experiments compared to our criteria (as summarised in figure 6).

Figure 6
An evaluation of Project Jasper and Project Ubin: Phase two



Project Jasper and Project Ubin: Phase two

Permissioned, private, hierarchical, closed source.

	Pros	Cons
1. Boundaries		Border dependent
2. Speed	Faster settlement	
3. Cost	Low energy use	
4. Transparency	Sensitive information invisible	Reconciliation needed, status invisible
5. Liquidity	Low liquidity requirements	
6. Risk		Single point of failure
7. Scalability	Scalable	
8. Finality	Deterministic	

1. Boundaries: Border dependent

The phase two experiments were not designed for cross-border transactions.

2. Speed: Faster settlement

The hierarchic, permissioned and private elements enabled fast authorisation and settlement. This is because the centralised node for validating payments was introduced. The centralised node is trusted to validate transactions because it has full view of the ledger balances and transaction history. Therefore, the ledgers improved the speed of the

[26] Project Jasper phase two used a Corda network for the experiments, which is a DLT platform built and owned by the R3 consortium. Carlyle et al. (2016). Project Ubin phase two experimented with four networks: Corda, Hyperledger Fabric, and Quorum.

[27] The experiments also included a supervisory node which oversees compliance with the ledger nodes, for example ensuring that each node has the up-to-date version of the distributed ledger and correct system specifications.

end-to-end payment process compared to existing payments systems, as well as the other DLT case studies. However, the hours of operation relied on the centralised node, which is similar to existing payments systems.

3. *Cost: Low energy cost*

The ledgers processed transactions with a similar amount of energy as existing centralised payment systems so did not impose additional energy costs. The experiments did not indicate whether fees were charged to the users.

4. *Transparency: Low status and information visibility*

The hierarchy in the phase two ledgers allowed transaction information to be kept private. The banks each had a copy of the ledger that only contained their individual transaction and account balances, while the central node had a full copy of the ledger. This is similar to existing payments systems. The lack of transparency also means that there is less advantage for account reconciliation and the payment status is less visible.

5. *Operational and security risk: Single point of failure*

The phase two ledgers also reintroduced a single point of failure into the payment system via the central node. Validation by the central node relies on trust that it will not misuse its ability, or allow malicious users to obtain access to the validation function. This is similar to the trust we place in existing payments systems. Therefore, phase two introduced a greater risk of fraudulent payments by hacking or by intent. It also reintroduces the risk of system failure or exploitable bugs in the code due to the closed-source nature of the ledger. But it is easier to control the development and specifications of the code, so removes the risk of the software being abandoned by the global community.

6. *Liquidity: low liquidity requirements*

The DLT design in phase two of the experiments improved the liquidity requirements. It did this by building an option for commercial banks to send payments to the central node for validation via a queue. Payments that were in the queue could be netted against one another, reducing the overall value of transactions requiring settlement.

7. *Finality: Deterministic*

Settlement is no longer subject to probabilistic finality as proof-of-work validation is removed and settlement is conducted by a central node. Therefore, it can be regarded as deterministic settlement, similar to existing systems.

8. *Scalability: Scalable*

The phase two experiments demonstrated the system is scalable to average volumes of high value transactions. This is due to netting and also because the central node can process transactions faster than proof-of-work validation, which requires a time delay.

Summary

Overall, phase two of Project Jasper and Project Ubin mitigated the costs identified in phase one of the experiments. In particular, the ledgers reduced the level of liquidity required for intraday transactions, and sensitive information was no longer shared amongst all participants. However, this also increased the risk of a single point of failure due to operational failure or cyber-attack. In the end, the phase two ledgers became more similar to existing payments system, than to Blockchain as they were also border dependent, scalable, closed source, and had deterministic settlement. Following phase two of the experiments, both the BoC and MAS were continuing to evaluate the potential for, and resiliency of, DLT in payments and finance.

6 Conclusion

This article describes the payments process at a high level and evaluates the characteristics of DLT compared to existing payment systems. It finds that DLT is a term that has come to represent a broad range of shared ledger technologies. It observes that the elements in DLT determine what type of characteristics it introduces to payments. It finds that some forms of DLT result in different payments characteristics compared to existing payment systems, and other forms of DLT result in more similar payment characteristics.

Blockchain is a form of DLT that has introduced different payment characteristics compared to existing payments systems. It has introduced faster and borderless payment settlements, increased payments transparency, and removed a single point of failure in the payments process. However, it also comes with low efficiency and scalability as well as concerns regarding the cost and speed of small value domestic payments.

Central banks have experimented with DLT to try to capture the benefits that the Blockchain introduces to payments, while avoiding the costs. However, the resulting ledgers became more similar to existing payment systems and did not demonstrate many additional benefits. The main difference between the phase two experiments and existing payment systems was that the distributed ledgers enabled faster settlement due to validation.

Therefore, it is important to consider the elements present in DLT in order to determine whether it will bring additional benefits to payments. Not all DLTs will bring the benefits or risks to payments that are commonly associated with Blockchain technology.

References

CPMI (2017) ‘Distributed ledger technology in payment, clearing and settlement’, *Bank for International Settlements.*

Deloitte and Monetary Authority of Singapore (2017) ‘The future is here. Project Ubin: SGC on distributed ledger’.

Iansiti M and K R Lakhani (2017) ‘The truth about Blockchain’, *Harvard Business Review.* https://hbr.org/2017/01/the-truth-about-blockchain accessed 24 April 2018.

Kumar, A and C Smith (2017) ‘Crypto-currencies – An introduction to not-so-funny moneys’, *Reserve Bank of New Zealand Analytical Note Series*, AN2017/07.

Monetary Authority of Singapore and the Association of Banks in Singapore (2017) ‘Project Ubin phase two. Reimagining interbank real-time gross settlement system using distributed ledger technologies’.

Mills, D, Wang, K, Malone, B, Ravi, A, Marquardt, J, Badev, A, Brezinski, T, Fahy, L, Liao, K, Kargenian, V, Ellithorpe, M, Ng, W, and M Baird, (2016) ‘Distributed ledger Technology in Payments, Clearing, and Settlement’, *FEDS Working Paper* No. 2016-095.

Morgan, P (2017) 'Bitcoin, Blockchains, Smart Contracts: For Lawyers', presentation to the Blockchain.NZ Conference, Auckland, 8 May 2017. https://www.youtube.com/watch?v=sdBDmfseWjQ accessed 21 February 2018.

Payments Canada, Bank of Canada, and R3 (2017) 'Project Jasper: A Canadian experiment with distributed ledger technology for domestic interbank payments settlement'.

Payments New Zealand (2016) 'Benchmarking New Zealand's payment system', *Research Paper.*

Pisa, M and M Juden (2017) 'Blockchain and economic development : Hype vs reality', *CGD Policy Paper 107.*

Reserve Bank of New Zealand (2017) 'Exchange settlement account system Report to accountholders 30 June 2017'.

Retail NZ (2018) 'The 2018 retail NZ payments survey report'. http://www.retail.org.nz/advocacy/payments accessed 24 April 2018.

Stats NZ (2018) 'Electronic Card Transactions'. http://archive.stats.govt.nz/browse_for_stats/businesses/business_characteristics/ElectronicCardTransactions_HOTPOct17/Related%20Links.aspx accessed 24 April 2018.

Wadsworth (2018a) 'What is digital currency?' Reserve Bank of New Zealand *Bulletin*. Vol 81. No 3.

Glossary

Acceptance device/gateway: An acceptance device/gateway reads the payment instrument to initiate a payment instruction. For example, in-store acceptance devices are credit, debit and EFTPOS card readers. Online, an acceptance gateway is the portal on a webpage into which credit or debit card details are entered.

Acquirer: The bank that holds the account of the person or institution that is receiving a payment.

Authorisation: The process of requesting approval for the transaction from the issuer and routeing the decision back to the merchant. The issuer will give authorisation if the payer has sufficient funds or credit to effect the payment.

Clearing: The process of sending the financial transaction information to the acquirer and issuer and determining settlement obligations.

Crypto-currency: A digital currency that requires distributed ledger technology and encryption techniques to be transferred.

Crypto-currency exchange: An online exchange market that enables crypto-currencies to be changed for other crypto-currencies or domestic currencies.

Cryptography (digital): Converting data into a code for transmission over a public network. Typically the data text will be turned into a coded text using an encryption algorithm.

Cyber-attack: An attack by malicious hackers to steal information from or destroy a computer network system.

Digital (electronic) currency: A broad term that captures all forms of money that are not physical or tangible.

Exchange settlement account system (ESAS): Accounts system held by the RBNZ and used for commercial banks and other approved financial institutions to settle their obligations on a real-time gross settlement basis.

Fixed conventional digital currency: Digital currency with a fixed exchange rate to national currency and which does not use cryptography or distributed ledger technology.

Fixed crypto-currency: Crypto-currency that is pegged to a pool of national currency enabling it to have a fixed exchange rate to that currency.

Issuer: The bank that holds the account from which a payment is being made. It will authorise payment requests by checking that the account holder has enough funds in their account.

Payment instruction: The instruction between issuing and acquirer banks enabling a transaction to take place.

Point of sale (POS): Place where the transaction is initiated, i.e. at the shop till, or online checkout page.

Proof of stake: The validator of a transaction in a distributed ledger is chosen based on a combination of random selection, and coin holding characteristics (stake).

Proof of work: The validator of the transaction is the miner who can solve a difficult mathematical problem first (provide proof of work).

Settlement: Settlement involves fulfilling the obligations between payer and payee. This may involve several different obligations such as payer to issuer, issuer to acquirer, and acquirer to merchant.

Single point of failure: A point in a system, that if it failures, will cause the whole system to stop working.

Validation: In a DLT transaction, validation is the process of ensuring that the funds are not being double spent and that ledger balances are accurate and true.

Variable conventional digital currency: Conventional digital currency with a flexible exchange rate to other currencies, including national currencies.

Variable crypto-currency: Crypto-currency that has a flexible exchange rate to other currencies, including national currencies.