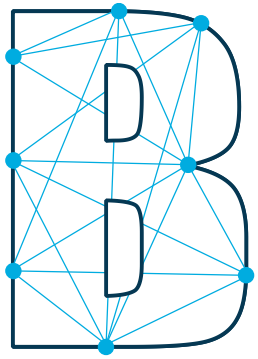


WHITEPAPER

Blockchain: Powering the Internet of Value

BANK 2020

EVRY

Foreword

This paper is the result of a research project carried out by EVRY's Innovation Lab during the fall of 2015. The content of this report is the result of a comprehensive study, featuring online sources, literary works, as well as recordings of financial conferences such as Consensus 2015 and Fintech Week 2015.

We aim to provide a comprehensive report detailing the opportunities, challenges and key success factors for financial institutions looking to leverage the opportunities presented by blockchain technology.

We hope you enjoy this study and that it helps give you greater understanding.

Peter Frøystad
Lead researcher & technical analyst
EVRY Financial Services

Jarle Holm
VP Innovation and Business Development
EVRY Financial Services

Executive Summary

Seven years after the blockchain was invented, there is a shift in focus occurring in the discussion around the applications for the technology. Previously, the discussion has focused mainly on the cryptocurrency known as Bitcoin.

This year however, the attention has shifted more and more towards the core elements of the blockchain itself and how its nature as a distributed ledger for transactions could be leveraged. Several startups and incumbents in the financial sector are racing to provide both new products and services, and to improve existing ones.

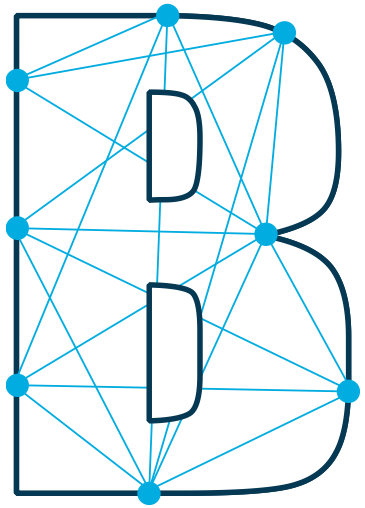
Blockchain technology was first developed to provide an alternative approach to payments, by using cryptographic methods to provide an alternative trust-mechanism between two transacting parties. Now it is being used as a solution for a wider variety of transactions.

Based on various sources, we have chosen to categorize blockchain technology into four different development areas. Of these four, we found that the category we chose to name Value Web, provides the biggest set of use-cases and potential applications. Our research also found that this is where the most amount of money and effort is being poured into.

New startup companies who offer solutions in these areas have already emerged and incumbent institutions in both financial services and technology are considering blockchain based solutions. Moreover, incumbent financial institutions are responding to new entrants by investing in blockchain companies, developing in-house solutions, or forming partnerships.

This paper provides an overview of the development of the blockchain, details how transactions are processed on a blockchain network , a summary of current initiatives and proposes a strategy for how organizations can leverage this new technology in the future.

2 UNDERSTANDING THE BLOCKCHAIN



Over the last few years, a major IT innovation colloquially known as blockchain technology has emerged as a potentially disruptive technology. The core of this innovation is built around the concept of a distributed consensus ledger, where the ledger is kept and maintained on a distributed network of computers.
This ledger makes it possible for the entire network to jointly create, evolve and keep track of one immutable history of transactions or other successive events, and it is today most commonly known as the blockchain. Up until recently, the most prominent blockchain technology application has been a cryptocurrency known as Bitcoin. It used a ledger called the Block chain, from where blockchain technology got its name. Bitcoin, however, is just the first of many potential applications of blockchain technology.

The world's first "internet-scale open platform for value-exchange"

Bitcoin was an audacious idea: until cryptocurrencies came along, no one had the ability to transmit value at a distance without the permission and support of a third party. This is the core of what blockchain technology makes possible; This simple, but revolutionary idea of instant value transfer. This is why so many people, both with technological and financial background are so enthusiastic about what this technology can offer. Bill Gates has called it "a technological tour de force", and Bob Greifeld, CEO of NASDAQ, called Blockchain "the biggest opportunity set we can think of over the next decade or so". The blockchain is being heralded as the fifth disruptive computing paradigm, which would bring with it an ubiquitous experience of value exchange on the web.

"Blockchain can bring the experience of a continuously connected, seamless, multi-device computing layer, with an overlay for payments —not just basic payments, but micropayments, decentralized exchange, token earning, digital asset invocation and transfer, and smart contract issuance and execution — as the economic layer that the Web never had."
- Melanie Swan [1]

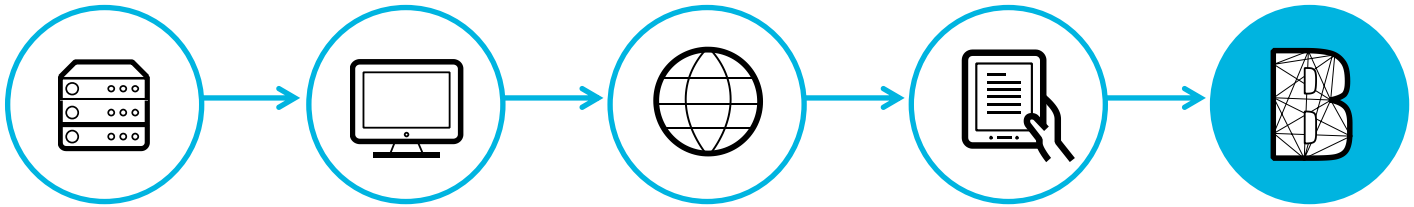


Figure 1: A new paradigm for computing

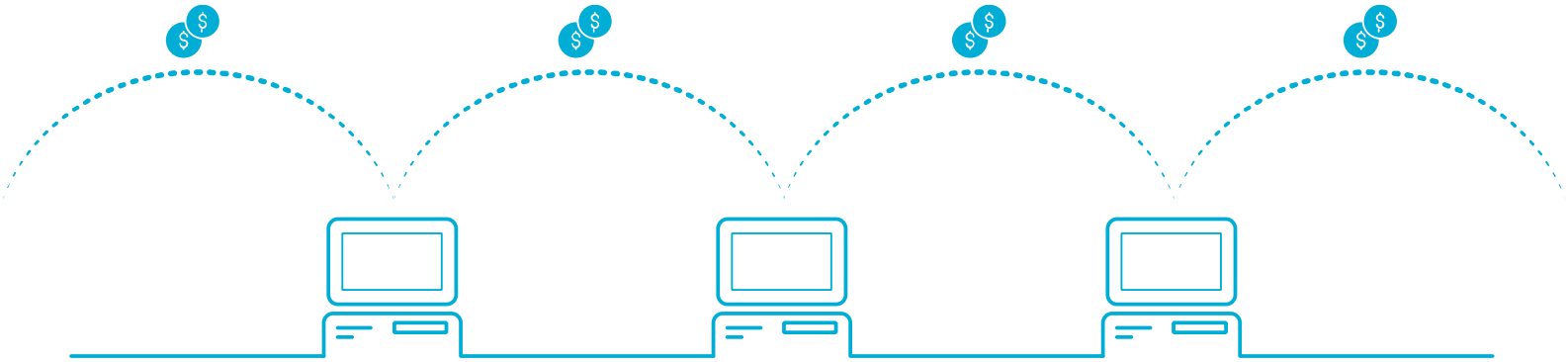
1: Swan,M (2015); Blockchain: Blueprint for a new economy

2.1 WHAT IS THE BLOCKCHAIN?

The blockchain is a global distributed ledger, which facilitates the movement of assets across the world in seconds, with only a minimal transaction fee. These assets can be any type of value, as long as they can be represented digitally.

Up until Bitcoin and its distributed ledger was invented, digital currencies were seen as unfeasible due to the relative ease of which digital information can be copied. This is know as the "double-spend" problem where each transaction carries a risk of the holder sending a copy of the digital coin to the merchant while retaining the original. The traditional way of mitigating this risk has been to have a trusted third party, such as a bank, to act as a centralised authority keeping track of all transactions.

Bitcoin has shifted this responsibility to a whole network. To exchange ownership of a digital coin, a centralised database is no longer required. Instead, a distributed ledger keeps a history of all transactions, and requires validation from its users to verify each change of ownership.



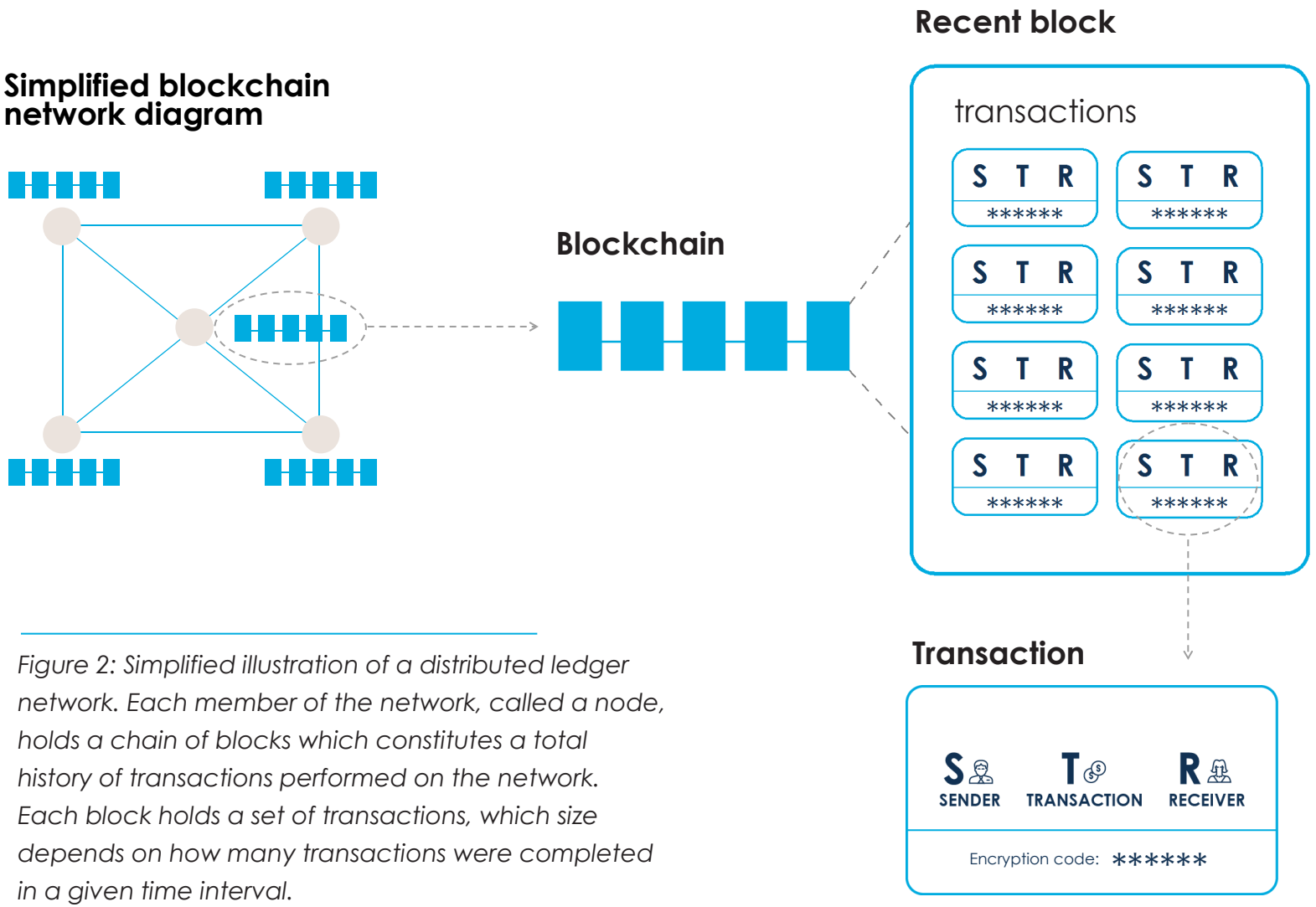


Figure 2: Simplified illustration of a distributed ledger network. Each member of the network, called a node, holds a chain of blocks which constitutes a total history of transactions performed on the network. Each block holds a set of transactions, which size depends on how many transactions were completed in a given time interval.

2.2 How does it work?

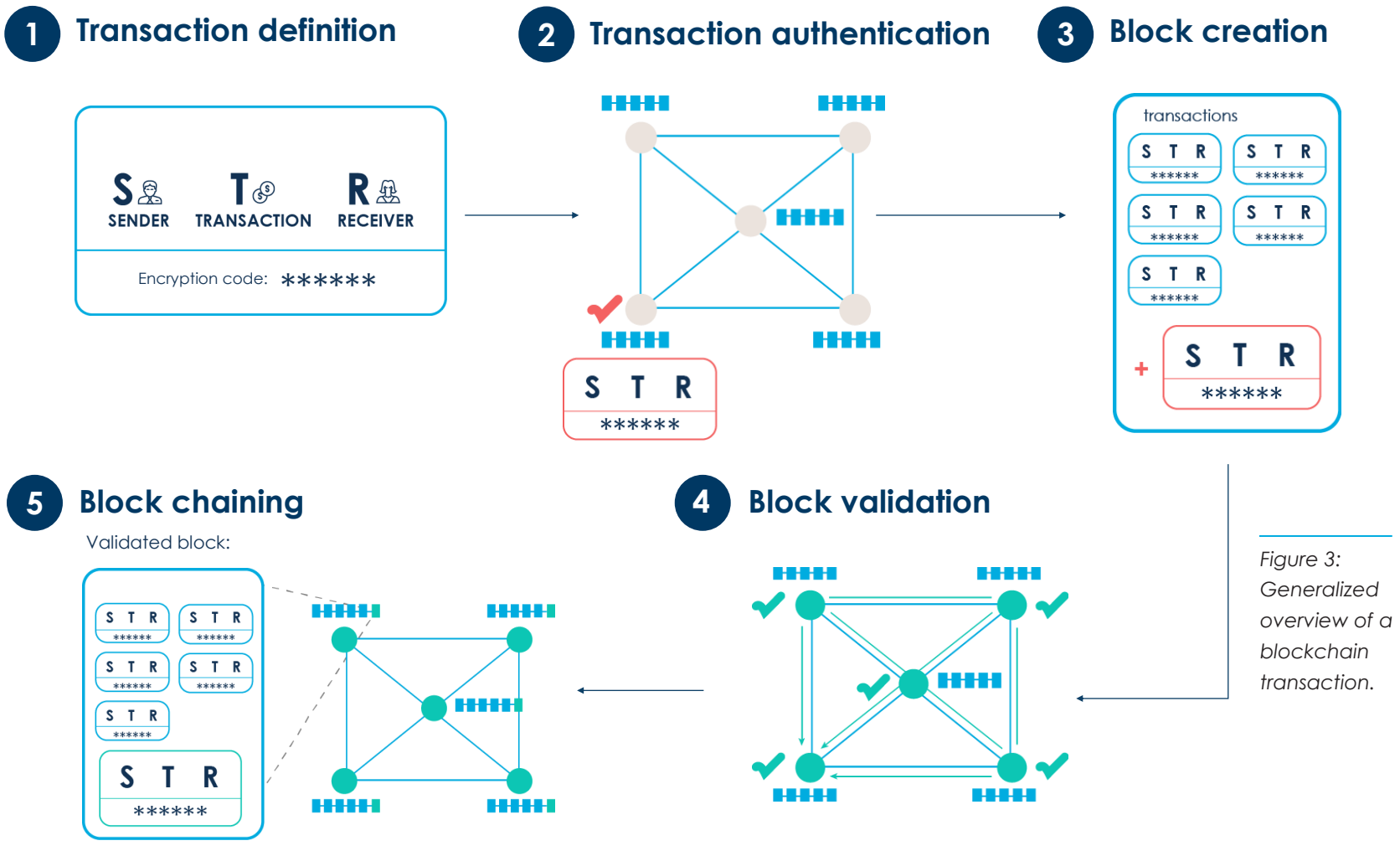


Figure 3: Generalized overview of a blockchain transaction.

1 Transaction definition

The "Sender" creates a transaction and transmits it to the network. The transaction message includes details of the Receiver's public address, the value of the transaction, and a cryptographic digital signature that proves the authenticity of the transaction.

2 Transaction authentication

The nodes (computers/users) of the network receive the message and authenticate the validity of the message by decrypting the digital signature. The authenticated transaction is placed in a 'pool' of pending transactions.

3 Block creation

These pending transactions are put together in an updated version of the ledger, called a block, by one of the nodes in the network. At a specific time interval, the node broadcasts the block to the network for validation.

4 Block validation

The validator nodes of the network receive the proposed block and work to validate it through an iterative process which requires consensus from a majority of the network. Different blockchain networks use different validation techniques. Bitcoin's Block chain uses a technique called "proof-of-work", Ripple uses "Distributed Consensus", and Ethereum uses "proof-of-stake". The various techniques have different pros and cons. The common denominator is that they ensure that every transaction is valid, and make fraudulent transactions impossible.

5 Block chaining

If all transactions are validated, the new block is "chained" into the blockchain, and the new current state of the ledger is broadcast to the network. This whole process can be completed in 3-10 seconds.

2.3 TWO REVOLUTIONS FOR THE PRICE OF ONE

The blockchain revolution is so fascinating because it could actually be TWO completely different revolutions both profound in their implications: 1) Industry-level systems of record providing massive efficiency gain for incumbents. 2) Censorship-resistant digital cash providing a new platform for open, permissionless innovation.[2]

Bitcoin and its Block chain was successful because it did not ask for permission. It was built upon the idea of a system where a central authority and oversight is to be avoided, and that the network itself should be resistant to all forms of censorship. At the same, time the network should be open to all, and all members should be able to transact anonymously.

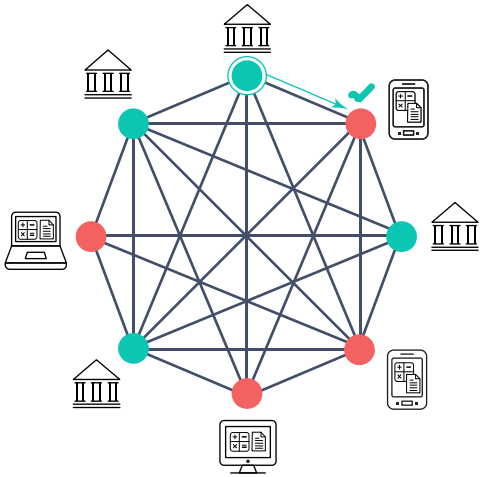
This meant that the idea of Bitcoin was initially scorned and avoided by financial institutions, and its Blockchain technology was seen as too slow and too risky for traditional finance [3]. As the technology matured, however, more and more people began to see the potential of a distributed ledger technology, just in a more controlled setting. If the distributed ledger technology could be adapted to fit into existing laws and regulations, this could lead to a lot of costly inefficiencies being removed and a prime system of record being introduced to the financial world.

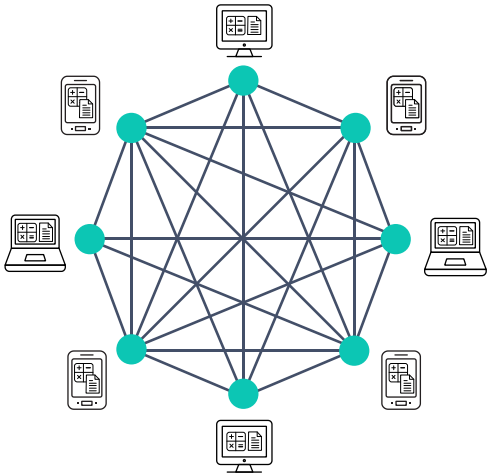
This led to the development of what is now commonly called permissioned ledgers. In contrast to the permissionless ledger of Bitcoin, the nodes doing block validation (see p. 11) are known and trusted, meaning that they can be held accountable according to laws and regulations. Another difference is that normal member nodes, meaning those who can only initiate and receive transactions, are also required to identify themselves when they join the network, similar to how a bank account is opened today. (More details are presented on page 14 and 15.)

2: http://gendal.me/2015/07/23/bitcoin-and-blockchain-two-revolutions-for-the-price-of-one/
3: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

Validator node
(Can both initiate/receive and validate transactions)

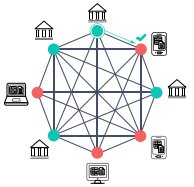
Member node
(Can only initiate/receive transactions)





	Permissioned Blockchain (Private)	Permissionless Blockchain (public)
How do you get access to the network?	Authorized access	Open access
How are their approach to laws and regulations?	Aims to follow financial regulations such as AML/ KYC	Aims to create censorship resistant, anonymous transactions, outside current legal framework
Who are the validators?	Pre-selected, trusted validators	Anonymous, fully decentralized validators
What can it be used for?	Enterprise-level systems	Permissionless innovation, open-access applications

Permissioned Ledgers: Industry-Level Systems of Record



In a permissioned ledger, also commonly called a private or consortium ledger, the validation process is controlled by a pre-selected set of nodes. One can here imagine a system run by a consortium of financial institutions, where a certain majority have to sign every block in order for it to be valid. The access rights to read the blockchain might be public or restricted to just a certain number of participants, such as government-approved auditors.

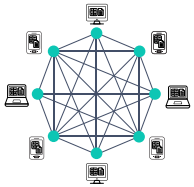
This is an example of how an industry-level system might be implemented, and as of the time of writing the main development focus for companies backed by financial institutions seems to lean towards such an approach.

Permissioned ledgers replicate the high degree of transparency and accountability in traditional banking systems. It is because we place so much trust in banks, after all, that they are required to take on a great deal of responsibility. Banks are given an important task to fulfil, and they are heavily regulated and scrutinized and will be held responsible for their actions. The population of the entire country, as represented by the government, stands behind bank deposits and promises to honour them even if the bank goes bust.

The main benefits offered by employing a permissioned ledger approach over a permissionless have been suggested to be: cheaper energy cost for transactions, greater privacy, and a faster validation process [4].

4: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Permissionless Ledgers: Censorship resistant



What characterizes the permissionless ledgers is that there is no gating or authorizing process to enroll into the transactions scheme, they are in theory a public ledger. Everyone is free to download a copy of the blockchain ledger, and they are able to join as anonymous validators by performing computationally intensive proof-of-works.

It has also been argued that these public ledgers are practical for primarily on-chain assets, meaning assets that are endogenous and created on the ledger (e.g Bitcoin). This argument is based on the fact that off-chain assets are not controllable by the validators in the same way as the native assets, and any conflicts in a transaction would need to be solved by an outside party or legal entity.

Although a strong argument is presented for the drive towards permissioned ledgers, financial institutions would be remiss to ignore the ideas and concepts adopted by the permissionless ledgers. Their openness means they are likely to be used by various people and gain unforeseen network effects.

Disruptive innovations usually find their first customers at the bottom of the market, as their unproven and unpolished products cannot command a high price. But as iterative improvements allow them to gain new grounds and attract new customers, they may end up reshaping entire industries.

3 CATEGORIZING DEVELOPMENT & FUTURE APPLICATIONS

The first applications of blockchain technology, dubbed blockchain 1.0, was various virtual currencies with the goal of being an alternative to fiat money. As the technology matured it entered a new phase of development, called blockchain 2.0. Here the focus expanded to include more advanced solutions for ownership and transactions, such as trade of physical assets according to the rules of smart contracts. This shift started happening around 2013/2014, but the development process is still ongoing. In this expanded landscape, all kinds of value can be registered and traded on various blockchains, which can be both specialized for one type of asset (e.g. diamonds) to a generalized platform capable of all forms of trade.

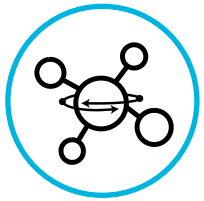
Following the goal of this paper, we will provide an analysis of the current landscape for the benefit of banks and the payment industries. Although the technical and regulatory details are not quite mature enough for widespread mass-market adoption yet, they do provide compelling future use-cases and opportunities. This merits the close monitoring of the technology by industry players.

3.1

CRYPTOCURRENCIES

3.2

VALUE-REGISTRY



3.3

VALUE-ECOSYSTEM

3.4

VALUE-WEB

3.1 CRYPTOCURRENCIES

A cryptocurrency is a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency, but is accepted by two or more parties as a means of exchange and can be transferred, stored or traded electronically.

Cryptocurrencies provide consumers with certain functions that address key consumer and merchant requirements. Both will benefit from a short time for the verification and settlement of the payment transaction, as this can be done in seconds (permissioned approach) or minutes (permissionless approach), regardless of geographical distance. For the merchant, there is another strong advantage in the low cost of acceptance. Since all transactions are done in a direct manner there is no need for a payment service provider, meaning transaction costs are very low.

Bitcoin was the first cryptocurrency and remains the largest in terms of market capitalization. Research estimates that the total number of bitcoin wallet holders will reach 12 million by the end of 2015, and proponents of the bitcoin advocate that there is only a matter of time before a «killer app» catapults the cryptocurrency into mainstream use.

There are however several fundamental challenges that need to be addressed for any cryptocurrency to become suitable for day-to-day use for the general public:

- High volatility leads to fluctuating value over time.
- The risk of deflation or inflation cannot be controlled, and only mitigated to a limited extent.
- There are no monetary policies due to lack of regulatory authority [5].

5: http://andolfatto.blogspot.no/2015/11/bitcoin-and-central-banking.html?spref=tw

All these points raise questions about cryptocurrencies' suitability as a widespread payment rail. Regulators in both USA and Europe have advocated caution, but also recognized the potential of virtual currency schemes. A recent landmark case from the European Court of Justice decided to exempt bitcoin transactions from VAT, and in doing so effectively recognized cryptocurrencies as a legitimate means of payment within Europe [6].

There is still a large challenge to work out how cryptocurrencies fit into current regulatory financial frameworks. Recent reports have indicated that virtual currency schemes may be incorporated into the definition of electronic money in EU's Third Electronic Money Directive, although there is very little information thus far [7].

The UK government, has announced as part of its 2015 budget that it will be investing £10 million into a research initiative to study digital currencies, and perceives the blockchain technology as a positive innovation that facilitates the fast, efficient and secure transfer of ownership of a digital asset over the internet. Although no similar plans have yet to be announced by any of the Nordic governments, there is an argument to be made that these countries might be fertile ground for similar research and development. The Nordic countries have the highest amount of non-cash transactions in the world, and are believed to be among the first to adopt a cashless society [8]. Finance Norway released a statement in 2014 where they argued that this could save society a massive amount in costs and reduced crime [9].

A potential path towards this future could be built on top of cryptocurrencies and blockchain technology. The banks and the governments could emulate the objectives made by the UK government, which aims:

- to provide clarity and certainty on the application of existing legislation and regulation for users
- to create the right environment for legitimate virtual currency entrepreneurs to flourish
- to support the research, development and application of new technology
- to support monetary and financial stability.

6: http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/
7: http://www.antimoneylaunderinglaw.com/2015/02/
8. http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/
9. http://www.nrk.no/norge/onsker-et-kontantfritt-norge-i-2020-1.11830344

3.2 VALUE REGISTRY

As the Blockchain technology matured, the development focus started to shift away from handling exclusively cryptocurrencies and started to use the public ledger to register physical assets. This shift started happening around the second half of 2013 and heralded the beginning of what is called "Blockchain 2.0".

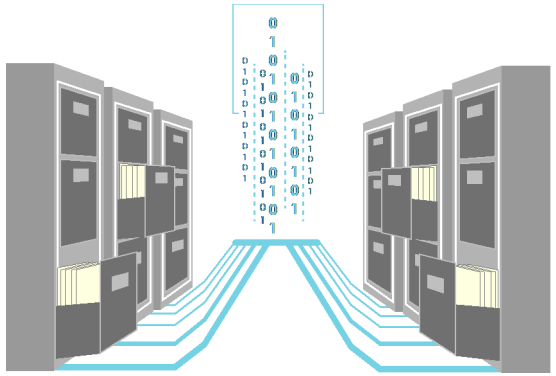


Figure 4: Digitalisation of physical documents.

Validating the existence or the possession of signed documents plays an important part in many financial and legal processes. The challenge of traditional document validation models is that they rely on central authorities for storing and validating the documents, which presents various risks in regards to transfers, risk of breach, as well as risk of deterioration.

Blockchain technology provides an alternative model to proof-of-existence and possession of legal documents. By leveraging the blockchain, a user can simply store the signature and timestamp associated with a document in the blockchain and validate it at any point using native blockchain mechanisms. To register ownership of an asset, a transaction is created with a reference to the physical asset. This information is stored on a Blockchain record, holding roughly 40 bytes of data, and can be associated with all manner of goods or services. The owner of the private key to that public record is then registered as the owner of that asset.

Case Study: Factom

A very ambitious Blockchain 2.0 project is in development from the Factom team. They are working on a system that secures and proves the authenticity of records, documents or other important types of data. The Factom system will ultimately consist of a four-tier architecture designed to both produce verified chains of information and secure that data within the Block chain.
They have a variety of use-cases, such as creating trustless audit chains, record keeping for sensitive personal, medical and corporate materials, and identity management as a KYC solution [9].

Factom has raised $1.7m so far in their series A funding, and is currently valued $11m. Paul Snow, one of the founders of Factom, told in an interview that they plan on building a node network with an infrastructure that can handle high transaction volume and that the architecture itself will be comprised of both full nodes capable of replicating all the data, and partial nodes replicating only the data needed in specified chains [10].

Its initial use-case is a land registry initiative being developed in coordination with the government of Honduras. The nation has a history of land rights abuse, where corruption and mismanagement have fueled a conflict over property rights which have lasted decades. Factom hopes that a system making it easy to store proof of ownership will find initial success in countries where government registries are missing or otherwise lacking, but that their solution can spread to the rest of the world if successful.

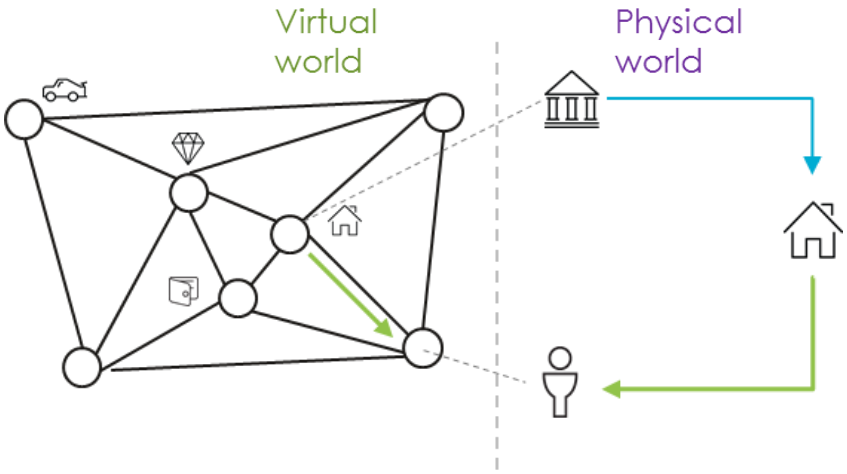
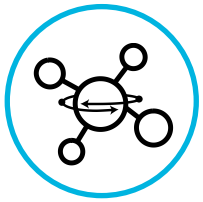


Figure 5: The distributed ledger can serve as a proof-of-existence for all forms of ownership documents, here represented as a house.

9: https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf
10: http://www.coindesk.com/factom-white-paper-outlines-record-keeping-layer-bitcoin/

3.3 VALUE ECOSYSTEM



Up until now, this paper has presented the expansion in reasoning from Blockchain 1.0 to 2.0, which have made the technology usable for far more than just currency. All of the protocols and use-cases that have been presented have been specialised, attempting to offer specific and rich feature sets targeted toward specific industries or applications that are financial in nature.

There are however a group of developers that takes an opposite track: a blockchain network that intends to be as generalised as possible, allowing anyone to create specialized applications on top for almost any purpose imaginable. They focus on developing the building blocks for entire ecosystems that will come into existence in the future. These are massively ambitious projects, which will take years to come into proper fruition. This paper will therefore present two of these projects which show the most promise at the time of writing.

The first to be described is called Ethereum, which are built around the philosophy of an public ledger. This means they intend to create an ecosystem that is accessible by all. The second is the project initiated by R3CEV, intending to create a private blockchain solution they envision as a global fabric for finance.

Case Study: Ethereum

The best way to explain Ethereum is to view it as a platform for future ecosystems: It allows people to easily create the infrastructure to set up new services on the internet. Furthermore, any infrastructure created on Ethereum sits alongside everyone else's creations, and can therefore interact with those other platforms in a guaranteed and seamless manner. Compare this with the last 20 years of internet development, which have produced innovative solutions and services built on top of other platforms. The likes of eBay and Facebook have made setting up a shop or marketing firm much easier, since you have an established platform allowing people to realize their ideas quickly and easily. Ethereum aims to provide something similar, which is why we categorize them as a value ecosystem.

Their initial work focused on defining a simple way to create smart contracts (see page 30). They created a simple language which allows such smart contracts to run on the Ethereum platform, and are now pushing to take it one step further. Looking forward, they envision a future decentralized system; where anyone can unilaterally join and participate in, one in which all participants contribute to the running and maintenance, and where there exists no entity that can prevent participation or arbitrarily censor the content or usage [11]. Suffice to say, Ethereum has grand ambitions.

Whether or not they succeed is yet to be determined, but their ambitions give a clear indication of what the blockchain technology might be capable of in the future. These value ecosystems are building the best digital system we can have for administering multi-user interactions without any need for centralized coordination or oversight, where all things of value will move freely between the various corners of the world.

11: :https://github.com/ethereum/wiki/wiki/What-is-Ethereum

Case Study: R3CEV

Differentiating themselves from many other blockchain startups, R3CEV started from scratch knowing that they were going to provide a flexible, holistic base layer with the specific functional requirements for secure, scalable enterprise use. This meant they would need to incorporate a set of non-functional requirements that globally regulated financial institutions must adhere to such as: compliance, privacy, reporting and reconciliation.

They also knew that if financial institutions and regulatory bodies were not involved and engaged from the beginning, then whatever solution that was created would likely: 1) fail to be viewed as an authoritative and legal record of truth and 2) fall short of adequately address their exacting needs [12].

R3's strategy was therefore to make partnerships with 25 of the world's leading financial institutions and create a collaborative lab which would create a common distributed ledger standard. Press releases have indicated that their first use-case will be deployable early 2016, and from there further improvements will be built continuously.

"This partnership signals a significant commitment by the banks to collaboratively evaluate and apply this emerging technology to the global financial system. Our bank partners recognize the promise of distributed ledger technologies and their potential to transform financial market technology platforms where standards must be secure, scalable and adaptable."

- David Rutter, CEO of R3CEV [13]

12: http://www.ofnumbers.com/2015/09/29/designing-a-global-fabric-for-finance-g3f/
13: https://www.rt.com/usa/315619-banking-giants-blockchain-technology/

Partnerships of R3CEV

3.4 VALUE WEB

Blockchain technology that are centered around the trade of financial assets are potentially the most interesting category for the transaction banking and payments domain, both for processes within and between organizations.

The moniker "value web" was introduced by noted economist Chris Skinner [14], but the idea is also known as the "Internet of Value". This refers to the next massive evolution of the internet that are expected to be brought about by a combination of different technologies, of which the blockchain will be a key pillar. The world of finance will not look the same once the Value Web hits mainstream adoption, and both consumers and financial institutions stand to gain a great amount.

One of the main benefits from blockchain technology comes from being able to speed up processes and reduce the transaction complexity and risk. New advantages will spring forth as the technology are integrated with legacy IT, legal frameworks and existing assets such as currencies, stock, bonds, etc. Therefore, existing financial services could be powered by blockchain systems offering financial institutions potentially lower costs, better products and faster time to market.

These systems will most likely run on permissioned ledgers where access are restricted until a user are authenticated, as user trust in the network is key to a successful service. The participants in the network need to commit to publishing a digital representation of an physical asset, such as USD or gold. For this purpose, a 'gateway' are needed to bridge the gap between the physical and digital world, meaning they will convert the

14: http://thefinanser.co.uk/fsclub/2015/02/forget-fintech-welcome-to-the-valueweb.html

assets onto the network. This is a natural position for banks to take, as they hold a strong position of trust in society.

Another actor that is needed in the network, is that of the 'market maker', as they will exchange one digital asset for another and provide market liquidity. An example would be forex trading institutions in the case of international payments.

A numerous amount of developers are rushing to develop software that can enable these use-cases and establish themselves as the best solution provider, often in several markets at the same time. One can here imagine a winner-takes-it-all scenario due to the strong network effect that the biggest provider will enjoy, but interestingly certain signs have been indicating that this might not be the case. Building further upon the blockchain technology's open-source roots and Bitcoin's ideal of an open network, developers have focused on making solutions for interoperable ledgers. This means that value can be transferred between different ledgers, and allow trade of assets that today are not considered tradeable.

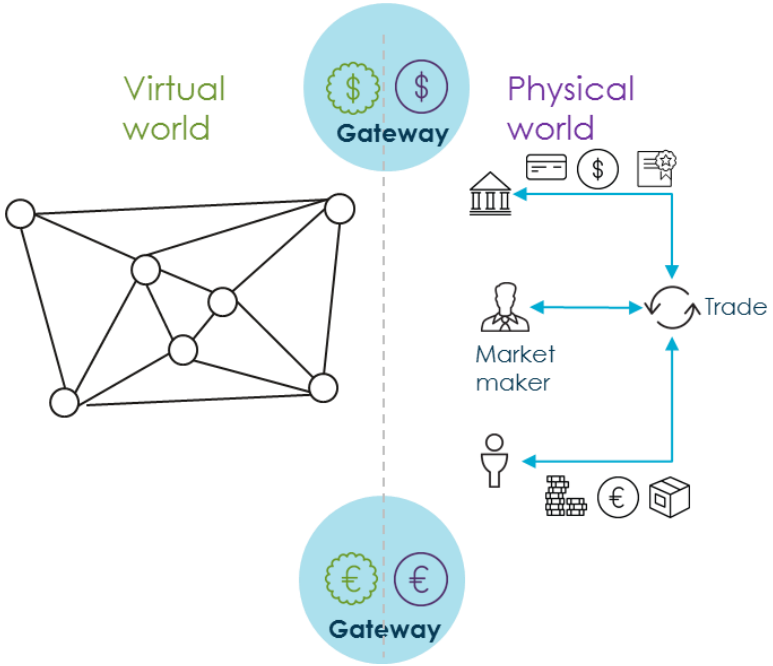
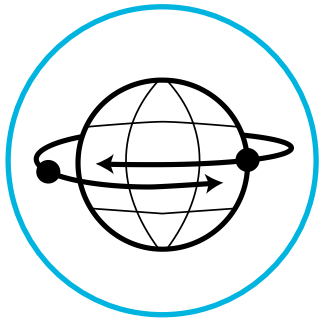


Figure 6: The value web will facilitate the trade of all forms of assets, such as currencies, stocks, goods, and gold.

4

VALUE WEB: FIVE USE-CASES



This chapter will focus on expanding on five use-cases of the value web, which currently have the highest amount of money invested and created massive engagement around the world.

Each use-case will be introduced and described in the context of applicability for financial institutions. Case studies of some of the major players in the field at the time of writing will also be introduced.

4.1 SMART CONTRACTS

4.2 DOMESTIC PAYMENTS

4.3 INTERNATIONAL PAYMENTS

4.4 TRADE FINANCE

4.5 CAPITAL MARKETS

4.1 SMART CONTRACTS

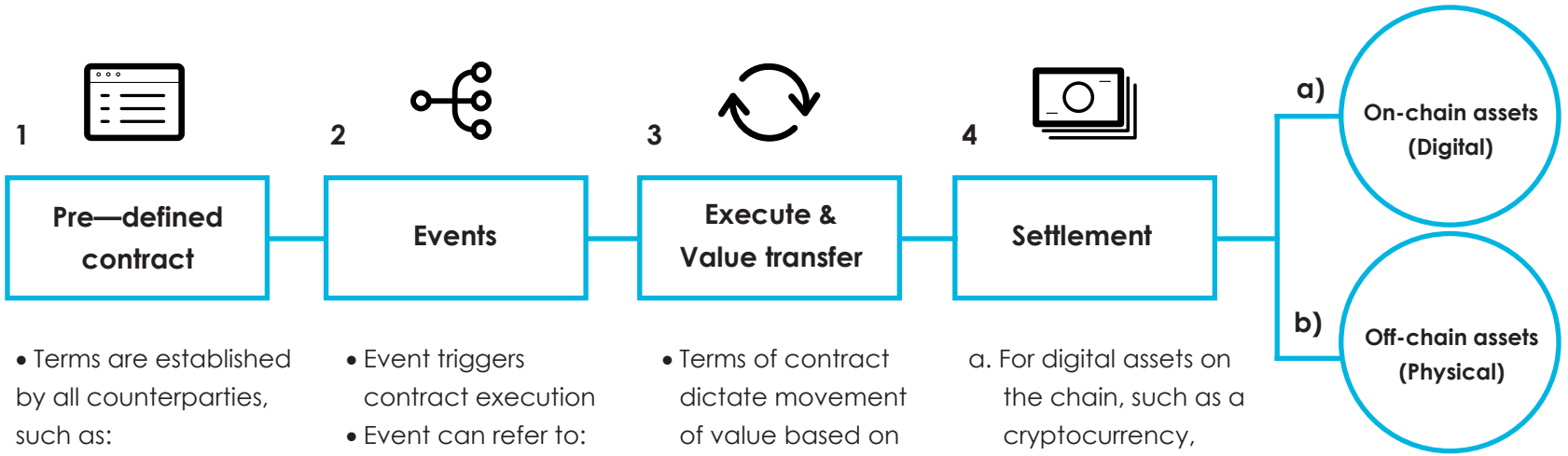
Being familiar with the concept of smart contracts is paramount to understanding how the value web will be used to handle all sorts of value transactions in the future.

A general definition of a smart contract would be a computer program that can automatically execute the terms of a contract. By being self-executing and having property ownership information embedded, they can solve the problems of counterparty trust. Smart contracts are trustless, autonomous, and self-sufficient. Instead of reinventing contractual relationships, smart contracts are making their formation and performance more efficient, cost-effective, and transparent [15].

A strong benefit of code-based contracts is the transactional efficiency of being able to automatically generate contracts based on agreed-upon patterns and syntax, which is something unlikely to develop in our current contract drafting and negotiating environment. Maybe even more beneficial than the efficiencies gained by automation is the fact that code based contracts would be capable of debugging themselves. Progress in artificial intelligence research will soon allow machines to understand more and more complex logic, which will ultimately lead to a system being capable of alerting a drafter to inconsistencies that often go unnoticed by human drafters. The ability to have a machine apply this sort of compliance logic would save certain industries a massive amount of time and money, especially within the financial and securities sectors.

One of the first markets where smart contracts are expected to be put to work are in syndicated loans. This is a $4 trillion market that still runs on faxes, email and excel spread sheets [16]. Already in the first half of 2016, banks are expected to start turning paper syndicated loans into smart contracts where the terms and conditions are programmed, then shared to the syndicate of lenders across the distributed ledger. This will improve a process that today takes on average 27 days, down to as quickly as two or three days.

15: https://bol.bna.com/what-is-a-smart-contract/
16: http://www.euromoney.com/Article/3501936/Getting-to-grips-with-blockchain.html



- Terms are established by all counterparties, such as:
  - ◊ Variable interest rate (e.g LIBOR)
  - ◊ Currency of payments
  - ◊ Currency rate
- Conditions for execution (e.g time and date, LIBOR rate at given value)

- Event triggers contract execution
- Event can refer to:
  - ◊ Transaction initiated
  - ◊ Information received

- Terms of contract dictate movement of value based on conditions met.

a. For digital assets on the chain, such as a cryptocurrency, accounts are atomically settled

b. For assets represented off the chain, such as stocks and fiat, changes to accounts on the ledger will match off-chain settlement instructions

4.2 DOMESTIC PAYMENTS

There is a strong drive within Europe to achieve "instant payment solution should become available to end-users in the short term, consisting of a common scheme cooperatively developed on the market [17]."
Government regulators believe that faster payments will accelerate economic growth, as businesses will be able to speed up its cash conversion cycle, generate working capital, and reduce the need for expensive short-term financing. A secondary driver for financial institutions to strive for real-time payments is their commercial need: They need to respond to customer expectations, and respond to competitive threats from new entrants.

In the payments space, the biggest challenges financial institutions face have to do with the silos within banks. Many of them have built various and complex IT infrastructure over the years, which on average cost 7,3% of a bank's yearly revenue in operating expenses, compared to an average of 3.7% across all other industries [18].

At a procedural level, the process of inter-bank clearing requires an intricate coordination of resource-intensive steps between banks, clearing houses, and the central bank. These steps are typically not executed at a constant basis, but rather as a processing cycle which happens several times a day. The outcome of it is that payment can often end up credited one or more days after their initiation, especially over weekends or holidays. The intricacy of the current system constitute a procedural challenge for payment service providers, and highlights the need for a more efficient system for real-time payment, both domestically and internationally.

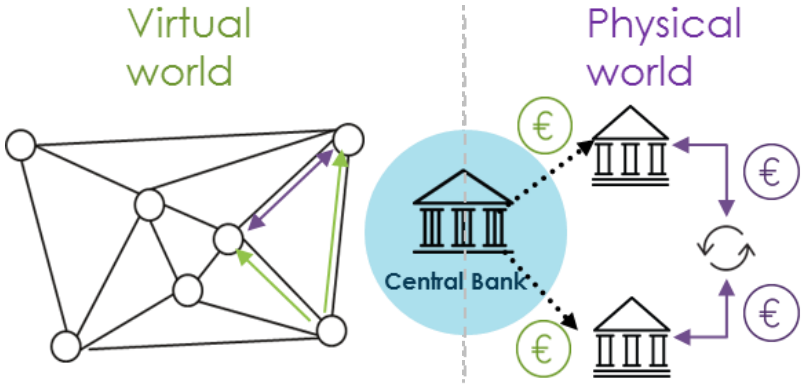


Figure 7: Blockchain solution where central bank issues cryptoeuro, allowing for real-time settlement between banks.

17: https://www.abe-eba.eu/thought-leadership/instant-payments/
18: DB research; *IT in banks: What does it cost?*(2012)

If a country can move towards an domestic economy where all transactions are recorded in real-time on a blockchain ledger, then this would mean more efficient execution of inter-bank payments. The central bank would need to launch a digital asset, preferably a cryptocurrency, which all parties agree upon as being representative of the same liability.

This would allow the government to balance the economy more efficiently and systematically, as they could leverage big data analysis to keep an up-to-date view of the money flow inside the country. An upcoming report by HSBC suggest that such comprehensive insights would allow the central bank to conduct a more direct version of quantitative easing. By performing targeted cash injections into the real economy, the central bank can extend the monetary policy interventions to include businesses and even private households, not just financial institutions and thereby significantly increase the effectiveness of the measures [19].

This idea is still years away from being put into practice, as a World Economic Forum (WEF) report suggest that about 10% of global GDP will be stored on blockchain technology around 2025 [20]. Before that however, blockchain technology will benefit several parties:

Consumers: Allows customers to make faster payments over their phone or mobile device, and online.

Small Businesses: Help merchants and small businesses make payments on time and receive payment faster.

Corporations: Large firms can ease cash management by timely incoming and outgoing payments. Employee payments can be delivered at customizable schedules based on smart contracts.

Financial Institutions: Can provide the most convenient online and mobile banking experience. They will also be able to serve as a springboard for new services. By adopting interoperable distributed ledger platforms such as those being developed by Ripple (see p.35) and R3CEV (see p.24) financial institutions can deliver real-time payment services that will work as quickly and efficiently both domestically and internationally.

19: http://www.businessinsider.com/hsbc-says-the-blockchain-could-be-used-for-radical-central-bank-helicopter-money-policies-2015-11
20: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

4.3 INTERNATIONAL PAYMENTS

To achieve real-time payments on an international scale, there will be a need to introduce foreign exchange (FX) market makers to the blockchain network. They will perform currency conversions on transactions between consumer bank accounts. Central bank participation on the network in a market maker capacity would also be needed between payment service providers in different currency jurisdictions. In this way, real-time payments could potentially be achieved on a cost-effective basis.

The foreign exchange market alone averaged more than $5.3 trillion per day in 2013 [21] and has been increasing at a steady rate each year. The World Bank estimates that the global flow of remittances will reach a total of $610 billion (See table for Scandinavian numbers). Both of these huge markets can be improved in terms of speed and efficiency through asset-centric blockchain technology, which could form an alternative to the current systems which involves various payment service providers and clearing and settlement structures.

Country	Remittances paid in $bn (2013)	Remittances received in $bn (2013)
Norway	5,78	0,79
Sweden	1,16	3,96
Denmark	3,06	1,22
Europe	109,40	36,50

Table: Remittances outflow and inflow in Scandinavia and Europe [22]

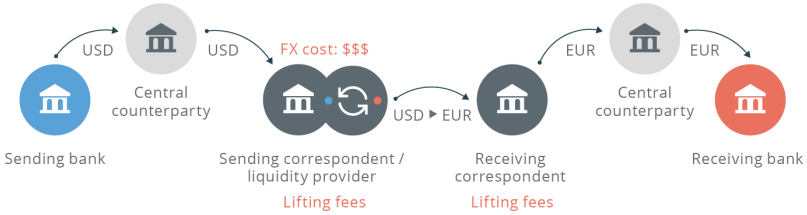


Figure 8: Present day system for international payments, where third parties such automated clearing houses, correspondent banks, and central banks are necessary to facilitate a transaction.

21: http://www.bis.org/publ/rpfx13.htm
22: http://www.worldbank.org/prospects/migrationandremittances

Case Study: Ripple

Several companies are working on developing Forex solution based on blockchain technology, such as Ripple, Stellar, and Coinbase. At the time of writing, the platform created by Ripple seems to show the most potential for further growth. They are all developing platforms based on partnering with payment service providers (PSP) in different jurisdictions to act as gateways to their ledger network. The gateway holds the fiat currency as collateral, and creates a digital version of the currency on the network. These gateways can then trade in real-time with each other, either directly or through 'market makers'. These will typically be FX companies.

Ripple's goal is to connect the world of money much like email does for communication and they have been steadily growing since their inception in 2012. Ripple partnered with the German bank Fidor AG in 2014 to use its platform for both interbank transactions and intra-bank transfers with its own subsidiaries overseas [23], and later started working together with Santander for the same purpose.

In the start of October 2015 they announced that their experimentation had borne fruit, and that they were ready to deliver enterprise-grade solutions for both FX market making and real-time settlement. Having raised more than $32 million in Series A funding [24], Ripple plans to grow and add more bank partnerships in the near future. There have been strong indications that key Nordic financial institutions are experimenting with the Ripple network, and are considering a partnership.

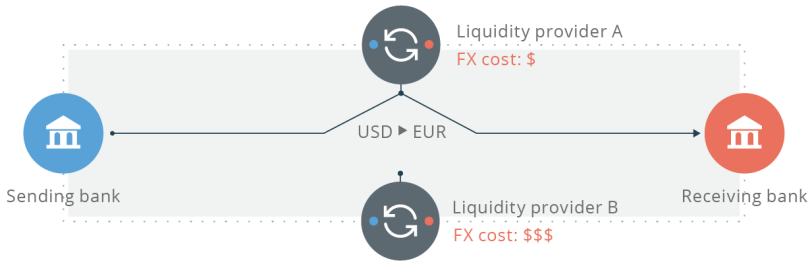


Figure 9: Visualization of Ripple international payments solution, where an US bank transmits to a bank in EU. The Ripple network automatically chooses the market maker with the best USD->EUR conversion rate

23: https://ripple.com/blog/fidor-bank-ag-the-first-bank-to-use-the-ripple-protocol/
24: https://ripple.com/ripple_press/ripple-adds-santander-innoventures-fund-as-series-a-investor/

4.4 TRADE FINANCE

Digitization and automation of trade processes has been ongoing for many years, but the banks' updated processes are still largely based around the logistics of handling physical documents.

A lot of processes share similar characteristics, but requires completely different IT systems and procedural steps to manage. An example here would be documentary collection, letter of credit and consignment. All of these processes follow roughly the same five steps:

1. Extension of credit to customer
2. Informing the customer of credit status
3. Banks open a communication channel regarding the customer
4. Updating the status of goods from freight forwarder
5. Execution of full or partial payment of funds based on certain criteria.

Blockchain technology could bring the benefits of automation to these trades. Through the use of cryptographic keys and multisignature wallets, one can create a replacement for traditional trade finance documents, which are stored on the blockchain as a smart contract. The document is updated by blockchain transactions as it moves through the steps of the trade process.

Two cryptographic keys are used to sign a blockchain transaction, one private and one public. This is analogous to how a signature on a physical document or a cheque proves validity in the physical world, only with an added layer of security. Ownership of the private key provides access to the digital assets stored at an 'address', which is analogous to accessing a bank account using a personal pin. Both keys are needed to create a transaction output, which means transferring your assets to another 'address'.

Wallets are a service which do not store the assets themselves but they can generate, manage and store the needed cryptographic keys. Added functionality enables a wallet to require multiple signatures before the digital assets in them can be accessed, meaning that multiple parties can be involved in the same trade process.

Case Study: Wave

Blockchain-based supply chain startup Wave emerged from the TechStars FinTech accelerator and was able to secure a partnership with UK bank Barclays at the start of October this year. The company describes its service as a way to replace traditional bill of lading documents which are used by trading partners to provide information on shipments [25].

Wave incorporates industry standard workflows, replacing printed documents with versions that are stored electronically in blockchain transaction metadata. Sharing many similarities with the ideas presented in the chapter on Value Registry, Wave use blockchain technology to manage the ownership of each document or goods in transport.

As the goods are being shipped from one receiving port to another, that change of ownership is recorded as an transaction with the port's private key, and the smart contract governing the trade will note that an update has taken place. Partial payment will then be executed automatically to the designated port.

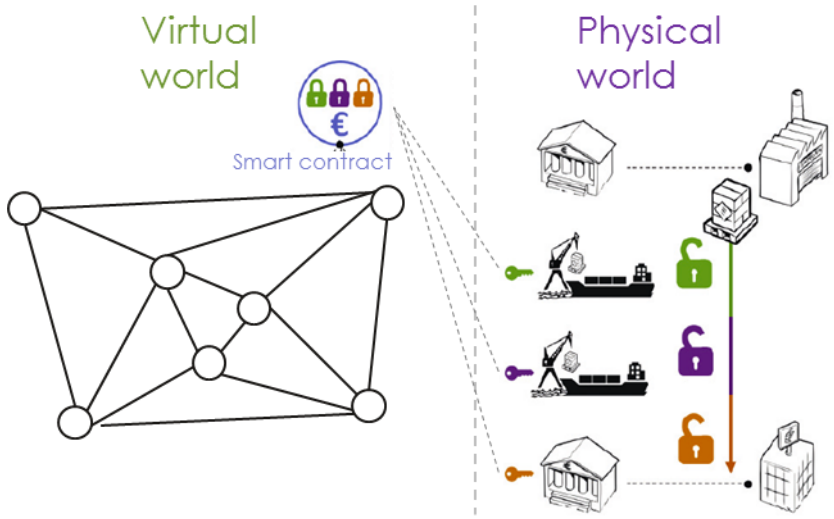


Figure 10: Trade finance process following the shipment of goods

25: http://www.coindesk.com/wave-blockchain-trade-finance-barclays/

4.5 CAPITAL MARKETS

When trading on the capital market, there exist a set of procedural steps that enable the trading of assets in a legally conforming fashion, as well as a number of custodian services revolving around facilitating the trade. A broad definition of these steps can be termed as such:

1. Create a representation of an asset, such as a currency, bonds, stocks, gold, etc.
2. Enable a trade to take place between two or more stakeholders.
3. Balances must be recorded and kept.
4. The eventual liquidation of an investor's position.

This process is made considerably more complex due to coordination between multiple necessary stakeholders. Typical examples of such stakeholders would be:

- Securities custodian: Licensed to create a certain asset
- Currencies custodian: Guarantees that the asset is backed by a currency, so that the asset can be eventually liquidated.
- Investor: The buyer of the asset
- Originators: The seller of the asset, though can often be a bank acting as an intermediary.

Due to the increasing amount of stakeholders and intermediaries over time, the trade process has become overly complex, prone to error, and expensive. This is underpinned by a wide variety of inefficient legacy IT infrastructure which are not interoperable.

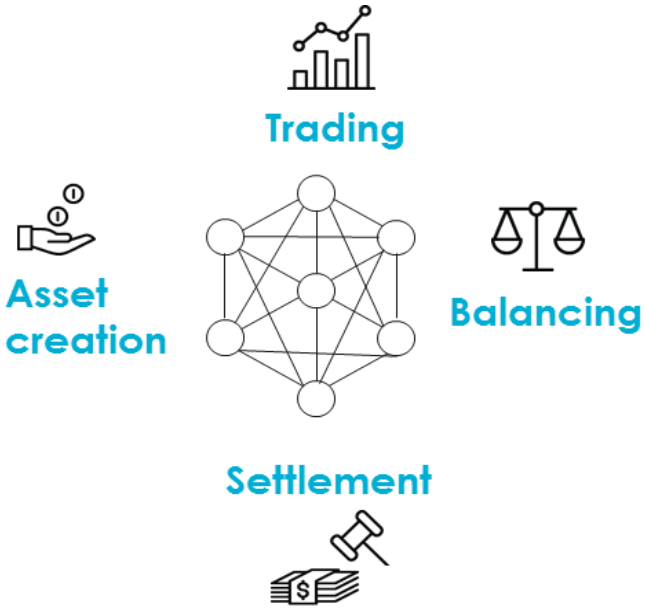


Figure 11: Trade process steps illustrated to run on top of a distributed ledger.

By adopting a shared distributed ledger platform, stakeholders could be eliminating the need for replication and duplication of the same data. As a consequence there will reduced error rates, increased speed, and cut cost associated with reconciliation and management of data. If you can speed up the process of which assets change hands, capital requirements drop because there is a resulting lower rate of operational risk and counterparty risk. As an added bonus, these environments are cryptographically secured, and since they are distributed they are less vulnerable to single-point-of-error due or operational failure due to cyber attacks.

Moving away from the more general benefits, we can also observe the advantages achieved in each of the trade process steps:

- **Asset creation** – Any type of asset can be created on the network if the trading partners are in agreement.
- **Trading** – Assets can be traded on the network with a minimal transaction fee in atomic transactions (either fully executed, or not at all)
- **Balance** – Balances are recorded on an shared replicated ledger where each position are constantly netted.
- **Settlement** – The network can also host the currency assets that back the tradable assets.

Securities trading is a massive market worldwide, with plenty of stakeholders set to either gain a lot from blockchain technology, or be disintermediated by it. Both in pre and post trade processes there are several companies vying to develop and deliver the blockchain software that will run the future financial market. This paper will look at two of them, one created by NASDAQ partnered with blockchain startup Chain, and the other delivered by Digital Asset Holdings.

Case Study: NASDAQ & Chain

NASDAQ will leverage the Open Assets Protocol, a coloured coin innovation built by blockchain startup Chain. In its first application expected late 2015, they will launch a blockchain-enabled distributed ledger that will be used to expand and enhance the equity management capabilities offered by its Private Market platform. NASDAQ's claims that their blockchain solution will offer efficient, fully-electronic services that facilitate the issuance, transfer, and management of private company securities.

For their first use-case, they decided to use the Bitcoin Block chain to issue shares in the form of coloured coins. These coins are essentially a micro transaction (a hundred-millionth of a bitcoin), on which would be coded metadata stating how many shares of the company are being transferred along with it. If some of the shareholders later wanted to sell all or part of those shares to an investor, a currency custodian could be tasked to hold the shares of all wanting to sell. The shareholders would then transfer their shares to that currency custodian's wallet, and investors could buy those shares. Each transaction would only move a tiny fraction of bitcoin encoded with the number of shares, not an amount in bitcoin equal to the value of the shares themselves.

This is currently a pilot project, but if it goes well, the system could be rolled out to more private companies in Nasdaq Private Market and even the public exchange in the near future. Although the current pilot is run on a public ledger solution, i.e. the Bitcoin Block Chain, they are also developing a private ledger solution named Linq[26].

Figure 12: NASDAQ invested $30m in Chain, together with Visa and Citi. They also partnered to develop a pre-trade platform[27]

26: www.cryptocoinsnews.com/nasdaq-launches-linq-a-private-blockchain-powered-trading-platform/
27: www.forbes.com/sites/laurashin/2015/09/09/visa-citi-nasdaq-invest-30-million-in-blockchain-startup-chain-com/

Case Study: Digital Asset Holdings

The Depository Trust & Clearing Corporation (DTCC) is one of the biggest post-trade financial service firm, with an annual handling of more than $1.6 quadrillion in transactions. This is an example of an incumbent being in danger of disruption, due to its position as third party and facilitator in a securities transaction. Former JPMorgan top exec Blythe Masters, now the CEO of Digital Asset Holdings, said in a recent panel debating the current pain points of post-trade processes: "We're spending a lot on keeping everything in synch, instead of having one truth and agreeing on it. We incessantly send it off to each other and attempt to reconcile, and go through expensive post-trade processes to remedy errors, fails, and inconsistencies. Distributed ledger technology could solve these points of pain [28]".

She followed up with an interview with Bloomberg where she claimed that the blockchain threatens to disintermediate almost every process in financial services, and that her company, Digital Asset Holdings are out to fundamentally overhaul how the back end processes involved in the post-trade effort are carried out [29].

Digital Asset Holdings recently acquired three different startups called HyperLedger, Bits of Proof, and Blockstack.io. Between them, the capabilities offered by Digital Asset's acquisitions have the potential to address perceived performance, scalability and integrity challenges that exist in Bitcoin's Block Chain, and also make integration of existing financial markets back-office systems into the digital ledger world a more straightforward exercise.

Little is yet known about their blockchain platform, but indications are that they are building a significantly different solution to some of the current approaches. Unlike similar distributed ledgers, their Hyperledger has no native cryptocurrency and a quite strict permissioned protocol [30].

28: http://livestream.com/internetsociety/consensus2015/videos/100778795
29: www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything
30: http://digitalasset.com/hyperledger/index.html

5 STRATEGIES TO LEVERAGE BLOCKCHAIN TECHNOLOGY

A growing number of both corporate and institutional incumbents are announcing their interest in the possible implementation of the blockchain. The pace of investment in blockchain companies is increasing each year.

This chapter will outline three different strategies employed by some of the incumbents to leverage blockchain technology, and provide a recommended strategy for both the near-term and long-term future.

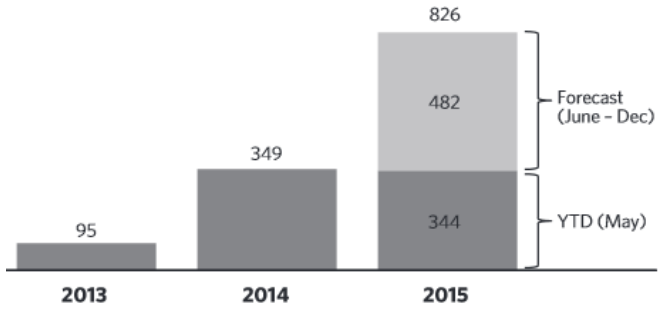


Figure 13: Venture Capital yearly investments ($m) in companies developing Bitcoin and/or blockchain applications [31]

31:http://www.coindesk.com/research/state-of-bitcoin-q3-2015/

STRATEGY	COMPANY			DESCRIPTION
Investment	Santander	→ ripple	$32m	• First funding rounds for three startups raised a total of $102m • Goldman Sachs acts as a VC in the Bitcoin's Block chain space • Santander InnoVentures has created a $100m investment fund, • Visa joined a syndicate to invest $30m in Chain
	Goldman Sachs	→ CIRCLE	$50m	
	VISA	→ chain	$30m	
In-house development	Nasdaq	IBM		• NASDAQ in-house platform described on p.40 • Citibank has created citicoin, a cryptocurrency being tested internally • IBM is working on a blockchain platform for the Internet of Things
	citibank			
Partnership	earthport, WESTERN UNION WU moving money for better, fidor BANK	↔ ripple		• Ripple has attracted many partners for its real-time payments system • UBS and Clearmatics partnered to create a securities settlement system • Barclays partnered with Safello to deliver "proof-of-concepts"
	UBS	↔ clearmatics		
	BARCLAYS	↔ safello		

5.1 RECOMMENDED STRATEGY

Short Term (3-12 months)

- Developing and publishing an internal "road map"
- Identifying opportunities to strengthen business through proactive innovation
- Conducting ongoing research to keep abreast of blockchain-driven changes within the sector
- Ensuring key staff are educated on developments, threats and opportunities in the payments business.
- Offering closed sessions/workshops
- Developing an innovation program
- Start testing the technology, to find out what kind of solutions technology provide.

Long Term (1-5 years)

- Become a cryptocurrency exchange (Ripple for example). If customers can use existing bank services to benefit from the new consumer-facing aspects of the blockchain technology,.
- Offer a free or otherwise really cheap cross-border remittances service. This is one of the most valuable use-cases for normal customers, and would give your business an competitive edge.
- Re-think trading and capital markets in light of the removal of delays and intermediaries. Delays means more costs, which will now be done in real-time to level off inefficiencies. Remove process steps that are not needed during the settlement and clearing stages.
- Start making partnerships with other banks and technology providers to develop a common platform and set of standards for the new technology.

5.2 CONCLUDING REMARKS

"If you can disrupt your business successfully, then you can also disrupt your competitors, but if you just focus on protecting your business, you're really living in the status quo. Internal disruption is always more benign than an external one, especially if it is done pro-actively and on your own terms. It's better to shoot yourself in the foot, rather than having someone else shoot you in the head"

- William Mougayar [32]

Those financial institutions who are willing to move first will most likely gain the largest benefits. The blockchain is not the perfect technology right out of the gates, but neither was the iPhone at first launch, nor the Internet. However, it is that perfect catalyst for business process changes, and this type of opportunity does not present itself that often. Embrace the ideal of openness, decentralization, and speed that first drew people to the Bitcoin's Blockchain, as that is what consumers and business users want.

Blockchain technology is still an emerging area of innovation, that is not being developed in a vacuum. Its impact on the various areas of the financial industry will very much depend on the future cooperation as well as the adoption of blockchain applications by existing or new market players.

32: http://startupmanagement.org/2015/08/05/dear-big-bank-ceo-re-blockchains-obliterate-dont-automate/

SOURCES

Primary Sources

- Euro Banking Association report (Jul, 2015); Cryptotechnologies, a major IT innovation and catalyst for change https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf
- Swanson, T (Mar, 2014); Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management
- Panel debates at Consensus 2015 conference. http://livestream.com/internetsociety/consensus2015

Chapter 2

1:Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly.

2.2 Two Revolutions for the price of one

2: http://gendal.me/2015/07/23/bitcoin-and-blockchain-two-revolutions-for-the-price-of-one/

3: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

4: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Chapter 3

3.1 Cryptocurrencies

5: http://andolfatto.blogspot.no/2015/11/bitcoin-and-central-banking.html

6: http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/

7: http://www.antimoneylaunderinglaw.com/2015/02/

8. http://money.cnn.com/2015/06/02/technology/cashless-society-denmark/

9. http://www.nrk.no/norge/onsker-et-kontantfritt-norge-i-2020-1.11830344

3.2 Value Registry

9: https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf

10:http://www.coindesk.com/factom-white-paper-outlines-record-keeping-layer-bitcoin/

3.2 Value Ecosystem

11: :https://github.com/ethereum/wiki/wiki/What-is-Ethereum

12: http://www.ofnumbers.com/2015/09/29/designing-a-global-fabric-for-finance-g3f/

13: https://www.rt.com/usa/315619-banking-giants-blockchain-technology/

3.2 Value Web

14: http://thefinanser.co.uk/fsclub/2015/02/forget-fintech-welcome-to-the-valueweb.html

Chapter 4

4.1 Smart Contracts

15: https://bol.bna.com/what-is-a-smart-contract/
16: http://www.euromoney.com/Article/3501936/Getting-to-grips-with-blockchain.html

4.2 Domestic Payments

17: https://www.abe-eba.eu/thought-leadership/instant-payments/
18: DB research; IT in banks: What does it cost?(2012)
19: http://www.businessinsider.com/hsbc-says-the-blockchain-could-be-used-for-radical-central-bank-helicopter-money-policies-2015-11
20: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

4.2 International Payments

21: http://www.bis.org/publ/rpfx13.htm
22: http://www.worldbank.org/prospects/migrationandremittances
23: https://ripple.com/blog/fidor-bank-ag-the-first-bank-to-use-the-ripple-protocol/
24: https://ripple.com/ripple_press/ripple-adds-santander-innoventures-fund-as-series-a-investor/

4.3 Trade Finance

25: http://www.coindesk.com/wave-blockchain-trade-finance-barclays/

4.4 Capital Markets

26: www.cryptocoinsnews.com/nasdaq-launches-linq-a-private-blockchain-powered-trading-platform/
27: www.forbes.com/sites/laurashin/2015/09/09/visa-citi-nasdaq-invest-30-million-in-blockchain-startup-chain-com/
28: http://livestream.com/internetsociety/consensus2015/videos/100778795
29: http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything
30: http://digitalasset.com/hyperledger/index.html

Chapter 5

31:http://www.coindesk.com/research/state-of-bitcoin-q3-2015/
32: http://startupmanagement.org/2015/08/05/dear-big-bank-ceo-re-blockchains-obliterate-dont-automate/

The Innovation Lab

Bank 2020 research papers

Small Business Banking

Small businesses are not often prioritized by banks, even though they account for a large part of the GDP in the Nordic. How can banks create solutions that bring value for both small businesses and banks?

First home buying for Millennials

Buying a home is the first major financial event for the Millennials. Banks need to recognize and alleviate the uncertainty experienced by Millennials when designing digital services.

Engaging the Millennials

Millennials are not engaged with banks. This paper brings insights to how banks can engage with this generation by exploring their mindset, lifestyle and needs.

Blockchain: Powering the Internet of Value

Blockchain is poised to become a massive disruptor for the financial world. This paper describes the technology, how it will alter the financial world, and a recommended strategy for financial institutions.

The New Wave of Artificial Intelligence

Artificial Intelligence is becoming increasingly prevalent in our everyday lives. This paper investigates the possible implications of the rise of Artificial Intelligence in the banking industry.

Big Data in banking

Norwegian banks are not using their data to optimize their decision making process and improve their business. This research explores the value of Big Data in banking.

We accelerate innovation in EVRY,
creating the financial solutions of the future.

evry.com/innovationlab

jarle.holm@evry.com

We bring information to life