The Land Registry in the blockchain - testbed

A development project with Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay and Kairos Future

KAIROS FUTURE

This report is a part of a project with Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Landshypotek Bank, SBAB, Telia, ChromaWay and Kairos Future to study and test the possibilities of using blockchains as a technical solution for real estate transactions and the mortgage deed processes. The first project ended in June 2016, this is a second project where the solution is further developed and tested.

Summary

The purpose

The purpose of this second project, the testbed-project, and this report has been to build and test the technology and understand any legal, process or security problems that should be taken into consideration before the project is launched.

The testbed built as part of this project includes a private blockchain that can be run by a group of public and private entities. It also includes a software application that manages contracts controlled by and recorded on the blockchain. This technology is sometimes known as a smart contract or distributed application; it is where the process and the conditions for authorization are programmed.

Some improvements to the process have also been made. A contract tailored for mortgage deeds has been developed, and potential improvements to the bidding process have been identified for future development.

The project team has engaged in presentations and discussions with various stakeholders. This has provided valuable opportunities to identify possible legal and technical pitfalls. A secondary objective is to stimulate interest and encourage others to start projects in the area, so that we can learn from each other and strengthen the ecosystem.

The result

The end result is a secure process for real estate transactions and mortgage deeds with the following characteristics:

1. All involved actors will have a digital file representing the agreement of ownership of the real estate, mortgage deeds and the transaction process. These files can be stored in the cloud, locally, or some other method of the actor's choosing.

2. The authenticity of the process, the signatures, the file confirming ownership, mortgage deeds etc. will be secured with a blockchain. The Swedish Lantmäteriet will store the blockchain with the proofs, but the blockchain will also be stored and validated by other actors. It will therefore be easy for authorised third parties to verify information. These third parties would usually be actors who are part of the process: banks, buyers, sellers, real estate agents etc.

3. The records and files that should be public according to Swedish law will be public and those which should be confidential will stay confidential.

4. There will be no bearer instrument stored on the blockchain in the current implementation. This precludes the risk of such authoritative documents being lost, stolen, or tampered with. Bearer instruments could be implemented in the future, but it should be noted that doing so entails risks and legislative uncertainties that require further investigation.

5. The only way to steal a property is through entering a new real estate transaction process with stolen or forged identification. The security of the ID-solution can be improved according to the requirements of the system in question. More stringent identification procedures (photos of physical ID-cards, biometric identification, multi signatures, etc.)

can be easily implemented.

6. The current process is designed to involve Lantmäteriet, real estate agents, buyers, sellers, and banks. These are the parties involved in most real estate transactions in Sweden. The process can be redesigned to involve other actors such as notaries, insurance companies and local public authorities.

Value of the solution

The value of the described solution will be substantial for countries like Sweden. For countries without a trustworthy real estate ownership record and land registry, a similar project may be the easiest, most cost efficient and fastest way to increase GDP in the medium term. It will serve as a foundation for better investments in land, enable the development of a mortgage market and a credit market in general, and become an institution for trust in one of the most fundamental parts of an economy: land and real estate.

Content

About the project

This report is a part of a project with Lantmäteriet (the Swedish Mapping, Cadastre and Land Registration Authority), Telia, SBAB, Landshypotek Bank, ChromaWay and Kairos Future to study the possibilities of using blockchains as a technical solution for real estate transactions. This report is one part of the project. The project also includes the building of a testbed where the technology can be tested and potential weaknesses can be identified.

Introduction

'Blockchains' are one of the most talked about technologies in recent years, especially within the IT community and the financial services industry.

The influential bank Goldman Sachs stated the following in December 2015 regarding blockchain technology: "Silicon Valley and Wall Street are betting that the underlying technology behind [the Bitcoin hype cycle], the Blockchain, can change ... well everything."[1] In a survey of experts by the World Economic Forum in 2015, the majority (57% of respondents) estimated that 10% of the world's GDP will be registered in a blockchain by the year 2025[2].

Recent events in 2017 such as the World Economic Forum, South by South West and the Mobile World Congress have made the growing interest in the blockchain still more evident.

One application of the technology involves creating verification records for digital files, e.g. documents or transactions. These verification records are the uniquely identifiable 'fingerprints' of the actual files. The verification records are grouped into a "block". The block is then added to

---

1   http://uk.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12

2   http://uk.businessinsider.com/goldman-sachs-the-blockchain-can-change-well-everything-2015-12

a chain of blocks such that it bears a verification record of the block that preceded it. This creates a chain of "fingerprints" all the way back to block number one. Therefore, it is impossible to alter information stored in older blocks without changing the subsequent blocks, because changing the block would change its fingerprint and invalidate the chain.

Current IT architectures most often create security by making systems inaccessible behind firewalls and with special network connections. For example, there are just a few actors, such as real estate agents, banks and a number of governmental authorities, who can connect their systems to databases at Lantmäteriet. Blockchain technology makes it possible to make verification records accessible without jeopardizing the security of the original documents.

In practice, confidence in the original transactions and documents improves when several actors have access to the blockchain's verification records. When the verification records are open and demonstrably difficult to manipulate, there is less reason to question them, and trust and confidence in them grow significantly. The blockchain's ability to create a secure shared history, and in doing so create trust, is why it has been called "The Trust Machine" by the Economist[3].

There is a parallel with the right of access to public records in Sweden. Openness and transparency of public documents and decisions creates trust in government agencies and in the welfare society. Anybody can request documents according to the principle of right of access. The blockchain allows many people — sometimes anyone — to check the verification records. Therefore everyone can trust that the person who has the original document, and who can recreate the verification records, is telling the truth.

3   http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

The interest in blockchains originated with Bitcoin and cryptocurrencies. For this reason, the financial services industry has been among the first to start working with blockchains. The possibility of establishing alternative currencies is of interest for central banks as well as other actors within financial services. A completely public blockchain, such as Bitcoin's, is based on global consensus. In other words everyone that participates in the system agrees on the state of the blockchain. Bitcoin's structure has many benefits but it restricts the number of transactions which it is possible to handle, and consumes enormous computing resources. It also takes considerable time to create consensus regarding which transactions and blocks will be accepted, even between machines. Funds, shares, bonds, etc. change hands in billions of transactions each minute across the globe. Public blockchains face significant challenges in handling this volume of transactions, but of course many are working on solving these issues.

The technology that has already been developed works well for transactions that require a high level of security but are not dependent on very high speed and very low latency like a stock exchange. The land registry and real estate transactions is one area where security and transparency are important and where there is a high level of value, but where the required transaction speed and the number of transactions is significantly lower. People who have looked at this area, like The Economist, understand that the value for society may be enormous - especially in countries that lack stable institutions. Brian Behlendorff, executive director at the Hyperledger project, a large blockchain development project, mentioned to the MIT Technology review in January 2017 that the land registry use case was the very reason he decided to start working with blockchains[4].

---

4   https://www.technologyreview.com/s/602731/web-pioneer-tries-to-incubate-a-second-digital-revolution/

With this project, Lantmäteriet, Telia, SBAB, Landshypotek Bank, ChromaWay and Kairos Future want to show how blockchain technology can redefine real estate transactions and mortgage deeds. At the same time, we believe that this technology, and the solutions we develop, will have broader application in real estaterelated issues as well as in a host of other areas, not least in the public sector.

The land registry today

The value of all properties in Sweden is currently over SEK 11 trillion, or roughly three times the value of Sweden's GDP. For many Swedes, their private residences are also their largest asset. The majority of the debt held by individuals is also linked to private residences. Close to SEK 3 trillion of the household debt is in the form of mortgages with real estate as collateral.

Lantmäteriet is one of the oldest public authorities in Sweden. Throughout history new technology has been implemented to secure real estate ownership and transactions, and the properties associated with a particular real estate. In the beginning there was not even paper, thus putting the land registry on paper was a way to secure records of ownership. In the 1970's, Lantmäteriet was one of the first public authorities to make their land registry digital. The full process is not digital, but an ever greater share of the work that Lantmäteriet does is taking advantage of new and improved technology.

Despite the importance of real estate for both society and individuals, there are many parts of the real estate transactions and the information about those transactions that take a long time to update. Many of these things are also based on outdated legislation. Information in the land registry can be missing, including registrations by Lantmäteriet, because some part of the registration process has gone wrong. It usually takes a long time from when the purchasing contract is signed to when the bill of sale is signed and the actual transfer of the property takes place. The sale is registered at Lantmäteriet long after the first contracts are signed, and until that happens it is not visible in the land registry. The sale of tenantowner rights are also not registered with Lantmäteriet at all, since tenantowner rights and owners are only registered with the cooperative housing society that owns the properties to be used.

To summarize some of the main issues to be addressed in the current process we can highlight these problems:

- Lantmäteriet is only involved in a few steps at the end of the real estate transactions. As a consequence of this the majority of the process is not transparent, in other words, visible to the public or other stakeholders.

- The system is slow at registering real estate transactions. The time between the signing a legally binding purchasing contract and when Lantmäteriet receives the bill of sale and make the approval of the title is often three to six months.

- The issues above have resulted in sellers, buyers, banks and real estate agents being forced to create their own complex processes for agreements, since they have to make sure that things can't go wrong, and because the value of the transactions is large. This creates inefficiency.

Lantmäteriet is continuously working on reducing the problems and weaknesses in its processes and systems. Blockchain technology provides the opportunity to solve many of these issues. In the long run, there is also great value if a solution can be developed and shared, or provide a framework and support for multiple government agencies where appropriate.

The value of the solution

The solution provides value by improving processes associated with land registration and real estate transactions. The following is a brief list of some of these improvements:

- Eliminating the need for physical archives of contracts and files.

- Increased resilience and redundancy of the transactional data in the land registry and the mortgage deed registry.

- Greater security for users of the system, in part because validation of the purchasing contracts and ownership can be done independently from Lantmäteriet.

- Faster and more transparent transactions.

- Official registration and confirmation of pending ownership around four months earlier than in the current process, which allows more information and data of transactions to be available, increase liquidity of real estate since it can be sold by the soon to be owner, and more.

- Making it possible to receive automatic confirmation of final land title at the date of transaction.

- Significantly improved mortgage deed handling, and making payments of loans dependent on secure transfer of mortgage deed.

- Elimination of the possibility of selling a property more than once.

- Making it more difficult to steal a property.

The value of the solution continued

As we noted in the first project the value for Sweden could be seen in faster transactions, the development of a fully digital process, increased security, better redundancy of data and the elimination of physical

storage and other paper based work such as traditional mail. The earlier registration of data of prices and transactions is also beneficial for public authorities. In this project we have also noted significant improvements in the process for.mortgage deeds. In total the value for society and the stakeholders may exceed 100 million Euros per year in Sweden. The value of the project should also be considered in the light of the lack of practical alternatives. We may not be able to make a fully digital solutions including, mortgage deeds, IOUs, digital contracts comparable to land titles etc. without using the blockchain.

There are probably other blockchain projects that can be of higher value to Sweden. Bank of England has for example claimed that the creation of a blockchain based currency, "a Britcoin", could permanently increase British GDP by as much as 3% of GDP. This is not the most likely value of the solution but even a fifth of this is significant.

While the value of migrating from the current platform in Sweden is easier to summarise and understand, we believe the value to countries with less trusted land registries may be even greater.

Value to other countries in the world

Looking at the world as a whole, the value of creating a transparent and easy to prove real estate ownership and transaction system is beyond imagination.

The size of the global lending against real estate as collateral i.e. mortgages is overwhelming. The value of mortgages in the US alone totals more than 14 trillion dollars[5]. If the lenders of this money can have greater confidence that the ownership of the real estate is reliably recorded

5   https://www.federalreserve.gov/econresdata/releases/mortoutstand/current.htm

and easy to prove, the risk gets lower and interest rates can be lowered. Lowering interest rates by 0.1% per year on the debt would create 14 billion dollars per year in value.

In countries where the enforcement of land ownership is difficult, providing security for the buyer of a property has very high costs. The cost of insurance safeguarding a real estate can be 10% of the purchasing value. If these costs could be reduced to 1%, the value for the economy is enormous.

A report by the World bank has found that the mortgage market is much higher in developed countries. "Mortgage markets seem to develop only at relatively high levels of gross domestic product per capita."[6]

Having a trustworthy record and possibility to secure land ownership may be a necessary condition for developing a country. A financial market may be difficult to develop without mortgages, and a mortgage market will be difficult to develop without trustworthy and enforceable real estate ownership.

Uncertainty of land ownership is also a major obstacle for agriculture to develop in many countries. Farmers don't dare to invest in the land, new seeds etc. and may actually farm destructively since maximising the harvest in the short term may be rational given the risk of losing ownership of the land. A trusted land registry is fundamental for increased food production and more sustainable land use in many countries. High GDP per capita is arguably only possible with a trusted land registry.

6   http://documents.worldbank.org/curated/en/697351468165251669/pdf/WPS6756.pdf

An institutional innovation

Seminal work by people like Robert Putnam[7] and Douglas North[8] have proven the importance of interpersonal trust and informal institutions for prosperity in a society. North pointed to the lower monitoring and transaction costs in economies with strong institutions. Interestingly the blockchain was described by The Economist as the "trust machine". We believe this metaphor is very accurate. Greater trust lowers monitoring and transaction costs. In countries without developed institutions to create that trust, blockchain technology can help fill the gap. We believe a solution with the land registry on a blockchain similar to the one described in the report may be provide a value similar to informal institutions and create a positive dynamic within an economy.

We therefore believe that a country with a global average GDP per capita can increase their GDP by more than one percent per year permanently, but more importantly, that it is possible to increase the growth rate for at least ten years. The cumulative effect of increasing GDP from 4% to 5% per year will after ten years translate to a 63% increase in GDP compared to a 48% increase.

We believe implementing a solution similar to the one described to be the fastest, easiest, and most cost efficient way to make a medium GDP per capita country into a high GDP per capita country.

7   Making Democracy Work: Civic Traditions in Modern Italy (ISBN 978-0691078892), 1993, Princeton University Press, Robert D. Putnam (with Robert Leonardi and Raffaella Y. Nanetti

8   North, Douglass (1992). Transaction costs, institutions, and economic performance. San Francisco, CA: ICS Press

What are the costs and obstacles?

Privacy

We have briefly looked into the legal aspects of the solution. Privacy and compliance with GDPR (General Data Protection Regulation) is not expected to be more complicated with a blockchain solution. Regulation of and securing personal data is a problem for any technology. One main difference with the blockchain is that it is very difficult to delete information. There may be conflicts between public registries and deleting personal information, but the conflict is then primarily with the digital files in general and not with the blockchain technology. If personal data is going to be deleted the person behind a public key stored in a contract in the blockchain has to be unknown to outsiders. Since real estate ownership is public in most cases in Sweden this information should however be public according to Swedish law.

Digital signatures

The main concern so far is legal uncertainty about when digital signatures on a real estate contract become valid. European law in this area is becoming more oriented towards electronic identification with eIDAS being one example. In Sweden Lantmäteriet already receive most of the contracts for real estate transactions in digital formats from banks and agents. In 2017 this will be made possible for all citizens. Swedish law also allowed for digital signatures on apartments in 2016. As these examples show there is increasing legal acceptance of digital contracts and signatures.

Physical signatures can still be a part of the process, for example by making digital copies of paper based contracts, but for the system to function properly digital signatures must be legally unambiguous.

Technical issues and security

The technical and security issues have been analysed, and so far nothing critical has been identified. We are confident that the technical solution will improve security compared with other solutions seen in the market. Maintaining and improving security and the IT architecture will of course be ongoing, with improvements made all the time.

Overall the technology has a small footprint and is expected to run on existing hardware. This doesn't mean that it will be easy or fast to implement, but considering large technological implementations in general we think this will be easier than many other national IT projects. Considering the value for the world, we think it is hard to identify a better investment in the future for society, people and planet.

A solution with a centralised database would be less costly, but would offer vastly reduced security and minimal improvements over current processes. It is hard to compare with other solutions since we don't know of any that can provide the same capabilities and security guarantees.

The blockchain is the only solution

A very valid question that has come up after the first project is. "Why do we have to learn this? Can't we just use the technology we already know?"

The answer to this question is that we cannot use traditional technology and continue to digitize real estate transactions. We can stay where we are, but in Sweden a further digitization of the process may not make substantial difference. No one has demonstrated a trustworthy solution for creating, enacting, verifying, storing and securing digital contracts. Until such a solution presents itself, the blockchain and the technologies described below seem to be a solution with great benefits and maybe no alternatives. Three properties of digital solutions have been very difficult, or even impossible, before the blockchain. These are described below.

1. Digital units impossible to copy

If we look at a central bank that is about to issue money to the market in the form of cash, i.e. physical bills, we can easily identify some of the concerns that they would have. It is quite obvious that one property is of outmost importance; the bills must be very difficult to copy. If everyone could take a home printer and make thousands of copies of their bills they will soon be worthless.

The same would be true for digital cash. If a central bank would like to issue money in digital form, it is still crucial that it cannot be copied. However, such a property of the digital world hasn't existed until recently. Bitcoin was the first to solve this 'doublespending' problem. A lot of central banks, and commercial banks, have during the past year communicated that they are looking at the opportunity to issue digital cash on the blockchain, or with distributed ledger technology. None of them has done so, and none has said they are looking at doing it with any

The practical consequence of solving this problem is that Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.

Marc Andreessen, Why Bitcoin matters, New York Times, January 21, 2014

other technology. As far as we know, the blockchain is the only solution being investigated by this growing group of central banks and commercial banks. Perhaps the main reason for this is the possibility to create transferrable digital units, which are more or less impossible to copy. If you want to create a digital IOU, and be sure that there are no copies of this IOU, and that its properties are securely preserved, the blockchain is the only known solution.

2. Digital files that can't be manipulated

While digitization has come far in many respects there is another property, except for being possible to copy, that traditional IT has not solved yet. It is very difficult to know if a digital file, photo, contract etc. has been manipulated. As an example the Swedish law states that any changes in the bookkeeping of a company has to be registered with a notification of who made the change, why was it made, and when was it made. The problem with this rule is that it is impossible to audit. A savvy IT person can the make changes in the registry of the bookkeeping that cannot be detected. There is no practical way for a manager or the organization, an accountant or the tax authority to know who made these changes and when they were made, or to notice at all that any change has been made.[9]

With the blockchain it is now possible to make sure that a digital file, register, patent, video etc. is still the same as it was when it was first registered in the blockchain. The hashing technology and the blockchain is the only known technology that can do this. If we want to digitally represent binding contracts it is of paramount importance that they be impossible, or at least very hard, to manipulate. The blockchain is the most trustworthy solution for this.

9   Modern technologies have made it possible to monitor all updates, for example in a cloud environment, so a person who wants to manipulate the data hase to be able to ma-nipulate the external environment as well, which makes is more complicated but possible.

3. Digital processes that can't be manipulated

A third problem the blockchain has solved is securing a process. The most discussed example of such a process is trade finance, where a sequence of actors have to confirm what they are doing at various stages in the agreement. They have to take responsibility for the goods being shipped and confirm the process for actors throughout the chain of transportation. Securing a process is also valuable in a contract such as a purchasing contract of real estate. It is important for all parties involved to be confident that all other parties are signing the contract in an acceptable order. This also makes it possible to proceed even if some of the actors are not physically present.

This may also be of help in securing processes related to objects connected to 'the Internet of Things'. It is very important to prevent or detect any manipulation of the processes these products are involved in, before they do any damage.

Overview of technology and use cases

The new possibilities can be understood through the example of Bitcoin and of more general use cases for the world.

The first widespread use case was for value storage and transfer where Bitcoin made the new technological opportunities evident. In a more general interpretation this is understood as the creation of digital assets and digital identities, whether they are to be traded or not.

The second use case is a register where hashes of any digital entity can be recorded and verified. This is possible in Bitcoin and in most other blockchains. A more generic interpretation of this use case is distributed ledgers. One application is the Estonian system built on technology by Guardtime.

The third use case is the smart contract, first described by Nick Szabo[10] before Bitcoin was released into the world. Ethereum, another major blockchain player, has focused on becoming a platform for creating and executing smart contracts. In Ethereum there is an interpretation of these as distributed applications. They could as well be seen as embedded applications since the application is embedden in the blockchain. While the technology developed by ChromaWay for this project can handle all three use cases, the strength and the core of the technology is the contract engine and associated toolset.

	Asset	Register	Application
	Bitcoin	Blockchain	Smart contract
	Digital assets & identities	Distributed ledger	Embedded/ distributed application

10   http://firstmonday.org/ojs/index.php/fm/article/view/548/469%23Contracts

The technology behind blockchains

In this part of the report, we will try to describe the basics of the technology. In the next part, we will describe real estate transactions today and in the future.

A distributed list of fingerprints (Verification records)

A central part of what is currently called blockchain technology is the ability to create unique verification records of digital files. For example, photos, transaction lists, registers, agreements, video films, patents, etc. Essentially, this includes everything that can be stored as a digital file.

Using an advanced "fingerprint algorithm" any digital file can receive a unique code. This is technically called a cryptographic hash. An example of an algorithm that creates cryptographic hashes is SHA256. This algorithm takes all of the ones and zeros that describe a digital document and recalculates them in a repeatable but irreversible way.

An illustration of how an algorithm like SHA256 works is: take every third digit in the file, multiply the number by 7, and divide the total by every fourth number in the file. Combine every number not used in the previous calculation to the number you have, etc. In the end, a series of digits and/or letters is created, in other words, a hash. If the same digital documents and the same encryption algorithms are used, the result will be the same hash. However, it is not possible to understand what the file looked like that created the hash — it includes just a few characters, for example, 32 numbers and letters. In the same way that a fingerprint is unique, the hash is unique for a digital file. But if you look at a fingerprint, you do not know what the person looks like, and in the same way a person looking at the hash does not know what the digital file looks like. A purchasing contract for a real estate transaction that is scanned and

becomes digital is an example. The hash that is created from the document is unique. For example, if a bank receives a purchasing contract sent via email, the bank can see that the document is correct. The bank takes the document and run the algorithm SHA256 on the file. The bank can then compare the hash with the hash that is on the list of verification records, assuming that it is available to the bank. The bank can then trust that the document really is the original purchasing contract. If someone sends an incorrect contract, the hash will not match. Despite the fact that email has a low level of security, the bank can feel confident about the authenticity of the document.

It is the verification records — the hashes — which are saved in the blockchain.

We can imagine that an individual government agency or organization may see an advantage in creating their own database of verification records. Different parts of the organization then can check the authenticity of documents and files by crossreferencing the list of verification records.
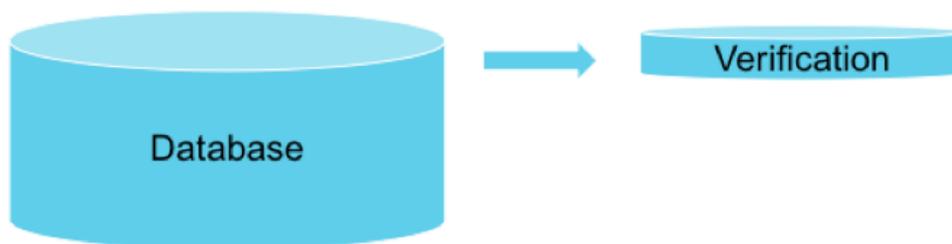
The owners of the agreements, documents, images, patents, etc. also benefit from having the list of verification records distributed to more

stakeholders. A high level of redundancy reduces the danger of a single list of verification records disappearing. When multiple people have access to the verification file, the trust in that file grows. Everyone can therefore be confident that their document is considered authentic because multiple people have access to the verification records.

## The blockchain is a way of saving the list of verification records

Of course, there are large numbers of documents and large amounts of data that can benefit from having an external verification service. Therefore, one of the challenges is to be able to manage the large number of verification records/hashes, the blockchain is a way to save the hashes as a group in a list. A large number of hashes are saved as a group, i.e. a block. Each block with verification records is then distributed to the persons who have access to the blockchain, sometimes even publicly to anyone and everyone. The person who is in charge of approving which of the transactions should be saved and distributed in a blockchain can do this more easily by grouping the hashes in a block. The alternative is to approve each hash one by one. In other words, it is not necessary to make blocks with many transactions, but the technology has the benefit of disseminating many verification records at the same time. In addition, something called a Merkle tree can be used to convert multiple hashes into one and therefore to save space in the block.

Blockchains are divided into different groups. The two main groups are open blockchains and private blockchains. In a private blockchain, there is one or a limited number of actors who approve the hashes that are to be saved in the blockchain, using digital signatures. For example, it could be a group of governmental agencies. In an open blockchain, practically

anybody can approve the block according to predetermined rules. The largest open blockchain is the one that builds up the digital currency or cryptocurrency, Bitcoin. If the system and participants in an open blockchain accept the block, they start building on the next one.

The blockchain is called a blockchain because each block is linked back to the previous block. Each subsequent block gets a hash, i.e. verification, of the previous block, which makes it difficult to cheat by creating another version of what happened. For example, it is not possible to enter a new verification into an old block without changing the subsequent blocks. If a lot of people have saved the blockchain, they can see that changes have been made and that the manipulated blockchain is not correct.
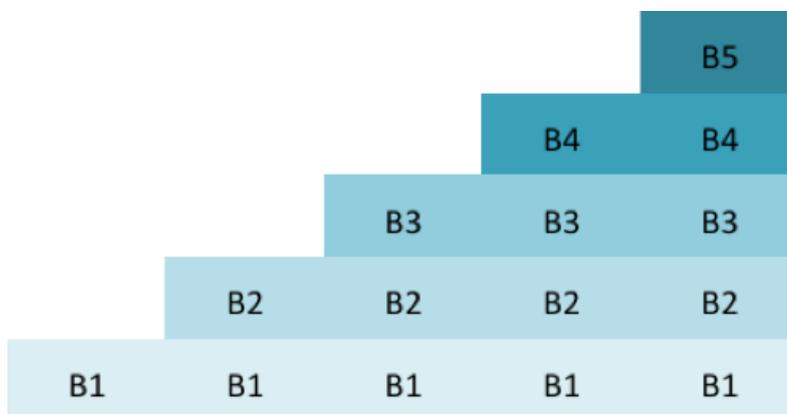
Who registers the block?

The blockchain and its verification records can be accessible to a large group of actors. The persons who approve which verification records will

be added to the block, however, in practice are most often limited. In an open system, such as Bitcoin, the system is limited in that enormous numbers of fast processors and energy are required to win the right to approve the verifications in a block. In a restricted systems with a private blockchain, for example, the system that NASDAQ launched as a trial for trading of unlisted stocks, NASDAQ themselves are the ones who approve the transaction lists and who gets to add transactions. In the case of NASDAQ, this is natural because this is the way they are working in their existing systems. On their exchanges, only persons with access to the trading system and who are connected to their exchanges can trade. Correspondingly, there are only a few actors who have direct links to the databases of Lantmäteriet.

Blockchains can be a mix of private and public, and in these cases several actors can approve transactions but not just anybody. In the future, we can imagine that private organizations and groups of IT companies, banks, central banks and other agencies will have blockchains that they monitor and regulate. While approval of the block is limited, access to the verification lists can be open, to all Swedish residents for example.

The power to approve the blocks

The advantage of having multiple actors who can approve the block is that the system is more transparent. The difficulty is to ensure that those people who contribute to the system by checking and approving transactions are doing it in the best interest of everyone, and they need some incentive to do this. In a government agency or at a bank or at a consortium, this isn't a major problem. The value of the service must naturally justify the investment due to greater security, increased transparency, efficiency, and revenues from the people who use the service,

etc. In Bitcoin's blockchain, the incentive is determined by who provides the greatest security for the system. Those who contribute with the most energy and processing power also increase the system security the most. These are called miners - these are the persons and organizations that uncover codes that are needed to approve new blocks in the blockchain. By giving the power to approve the block to those who are contributing most to the security and speed of the system, the system ensures itself of a high level of security and processing power. Anyone who wants to take over the system needs to exceed the power of the other people who are maintaining the system. At the moment their processing power in terms of hashing is far greater than the 1000 largest supercomputers in the world combined, and the processing power is increasing steadily as well. In practice, those people who are maintaining the system are not particularly interested in the power over the list of verification records since it doesn't do anything other than save the verifications and transactions but not the original documents. There are thousands of copies of the verification list so it cannot be changed without everybody noticing it. What those people who approve the block receive instead is a small payment from the verification records that are entered into the system.

Introduction of a digital currency

When Bitcoin was launched and the first block was created, it was practically free to add verification records. Still today it costs very little to register a verification record in Bitcoin's blockchain. Payment for the registration of the verification records is also important at the same time. If it had been free, the system would have had a harder time handling overloading of verifications. The problem with spam in the form of email depends in part on the fact that it is free to send.

In order to create an incentive for miners who would approve the block with verification records and ensure the security of the system, a digital currency, sometimes called a cryptocurrency, is awarded to them. The miners who dig up and approve blocks with verification records are paid by the system in the form of Bitcoin, which are digital codes that stay in the system. This system is programmed in such a way that Bitcoin is only created when a new block is created, and these are awarded to the person who identified the block and approved the verification records. Even private blockchains work in several cases with digital currencies as a part of the system. The hashes are actually entered as comment fields beside a digital currency or cryptocurrency.

The lottery determines who provides the approval

In the case of Bitcoin, an open lottery determines which computer or "miner" wins Bitcoin as well as the registration fee for the verification records and therefore approves the next block. The system generates a number that all computers that want to can try to guess[11]. The person who has many computers and uses a lot of processing power and energy can guess many times and therefore has the greatest chance of guessing the series of digits correctly first. It is a little bit like a lottery. The person who purchases a lot of lottery tickets has a greater chance of winning. In the case of Bitcoin, the person who purchases many processors and use a lot of energy has the greatest chance of winning. In order to take over the

11   This is a simplification of how it works. In reality each participants add a number and run SHA256 on the block with the number. If the result is a hash with a sufficiently low number the computer has proved it has spent energy on guessing and is rewarded with Bitocons and the transaction fees coming from the verifications that wants to be added to the blockchain. This is known as Proof of Work.

system, you need to have as much processing power as possible so that you are sure to win the lottery many times in a row. Only then can the system be manipulated and controlled in a way that other people who are part of the system do not accept.

Cryptocurrencies remain in the system

An important point with cryptocurrencies in the blockchain is that these remain in the system. Cryptocurrencies can be transferred to another person as a code that can provide access to the cryptocurrency in the system. However, the cryptocurrency cannot leave the system. In other words, the person who owns a cryptocurrency owns an encryption code to an amount of an encrypted currency in a blockchain. If the cryptocurrency is transferred, someone else has access to the code that controls the currency. The word "chain" is therefore particularly relevant for of cryptocurrencies. They are transferred like a chain from one owner to another, but the chain remains linked together.

Do cryptocurrencies have a value?

The idea of creating digital money is naturally something that has attracted many more or less serious actors. The use of money for society is usually described with 3 functions:

1. As a medium for payments.

Money makes it easier to trade. It is expensive and cumbersome to trade with cows and coffee beans. Money makes it cheaper and more efficient to trade.

2. A standard for accounting

Money makes it easier to compare and control businesses and people. We can see how much a company is worth, how much a person earns when there is a standard for reporting amounts that everyone understands. Tax agencies, investors and others benefit greatly from this.

3. A way to store value

Money makes it possible for people to save what they earn, and spend or give it away at a later date. The value can be transferred to another point in time. We can also spend earlier and get indebted i.e. get the value first and earn the money later.

If we look at Bitcoin, as an example, a demonstrated use has been as a medium for payments. Even if the currency's value relative to the US dollar, for example, fluctuated a lot in the initial years, this is a minor problem for the person who wants to transfer money cheaply. One of the challenges that Bitcoin currently faces is that the system in its current form cannot handle large numbers of transactions. The global number of transactions of money and various financial assets is billions per second. This is not possible to handle for Bitcoin today. The system is secure, but it cannot handle frequent trades.

Now the cost of transactions have increased, which makes Bitcoin as a means of payment less attractive, at least for smaller transactions. On the other hand the value as a store of value has become more evident. In general, we can say that all money is currently based on trust. As money has transitioned from raw materials to today's zeros and ones in the banking system, the amount of money in circulation has increased to

dizzying amounts and at dizzying speeds. We are not able to answer in this report whether cryptocurrencies have a future or not.

The subject cryptocurrencies is related and interesting but the process for real estate transactions and embedded contracts/ smart contracts that is described in this report and shown in the technical demo does not need to use any cryptocurrency.

Colored Coins

Regardless of whether cryptocurrencies are valuable in reducing transaction costs for international payments or whether they have value that can be saved and stored, they still have a value that has nothing to do with the function of money. Cryptocurrencies can store other information that is stored in the blockchain.

Digital currencies can, in certain cases like Bitcoin, be the carriers of information and agreements that are controlled by anyone that wants to ascribe value and information to them. The term "Colored Coin" refers to the ability to mark certain coins in a persistent way, to "color" them. The color follows transactions for a particular piece of cryptocurrency and provides the opportunity to give special meaning to a transaction chain of a set of cryptocurrencies.

LHV bank in Estonia has worked with ChromaWay to create a service that is called Cuber based on this logic. The bank enters the color identities into the code of the cryptocurrency Bitcoin. LHV guarantees the asset value of the particular pieces of Bitcoin to whomever owns them. In their case the pieces of cryptocurrency represent Euro. When someone performs a transaction in Euro in Cuber, the properties of the colorcoded

cryptocurrencies are transferred so that they represent a Euro value with a new owner. The value of the Bitcoin currency in this context is completely uninteresting. The cryptocurrency is used as a way to store information, and LHV determines what this information represents in terms of value. This is not very different from the activity of a bank. The bank is currently responsible for what the digital codes in their databases represent in terms of value, which they also reconcile with central banks, markets, and so forth. The advantage for LHV Bank with Cuber, among others, is that the transaction costs are lower and that trade with the currency, i.e. the Euro, can occur around the entire world.

Smart contracts/ embedded contracts

As described above, colored coins are designed to allow a digital code in a blockchain to represent an asset. An even more interesting coding possibility is that we can add additional information that is stored in the blockchain that regulates, for example, data authorization and storage. In addition to separating the verification record from the traditional database structure, we can also separate parts of the application layer. Similar to hashes/verification records, only the person who owns or has programmed the coding and the rules for authorization and storage can interpret how the application works.

The system of adding logic and properties that are normally part of the application layer in an IT architecture has been called "smart contracts". However, there are many different interpretations of what is meant by the term "smart" in this context. Therefore, we also use the term "embedded contracts"[12] to highlight the feature that we are after. The logic is registered in, embedded, in the blockchain.

12   "smart workflows", "distributed consensus workflows" are other names discussed.

The cryptocurrency/system Ethereum was built with a focus on creating smart contracts/embedded contracts in the blockchain. Apart from Bitcoin, Ethereum is one of the current blockchains that is talked about most. Ethereum permits arbitrary code to be executed in Ethereum's blockchain as long as you pay for the number of cycles that is required to run the program.

The technical demo that is currently being built as part of this project uses ChromaWay's open source technology and programming structure Esplix, which creates smart contracts/embedded contracts in a blockchain. Open source is an important part of ensuring confidence in the code. Everyone can inspect the code and detect potential weaknesses. In practice, a chain of messages is saved into a private blockchain, which can execute the transactions between the parties more quickly. When the contract is finished, it can be summarized into a hash that can be added to other blockchains like Bitcoin's blockchain as an extra back up. Everyone involved can also save all or part of the blockchain, which covers the personal transactions in the system. Both buyers, sellers, banks and real estate agents can therefore verify the history of a transaction.

An additional benefit of this procedure is that the solution is even easier to transfer to an alternative blockchain. Let's assume that a few government agencies jointly build a blockchain that they control. The solution we have built in the testbed can be easily secured, even in this blockchain. A solution with Colored Coins is somewhat more hazardous and difficult to transfer since the code is written on top of a specific cryptocurrency.

Traditional database	Blockchain
Application layer	Embedded contract
Database	Verification
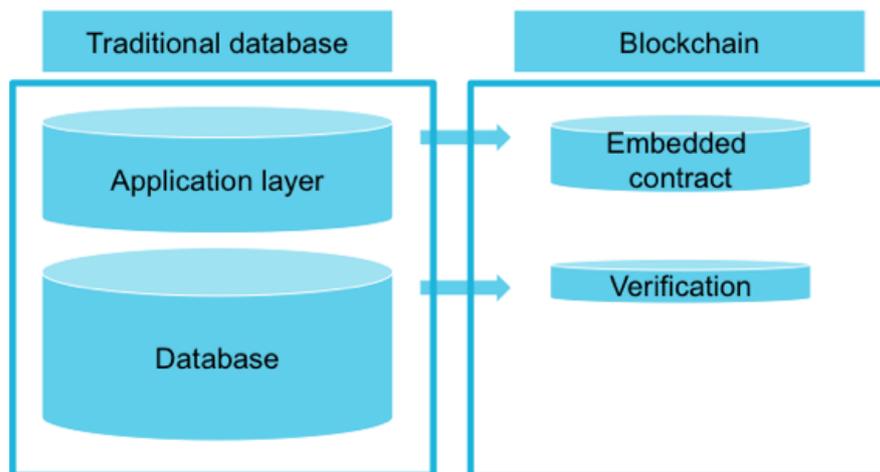
Safeguarding identities

A central part of the practical application of blockchains is the identification of what the digital codes will represent in the physical world. As described above, it is LHV Bank, Lantmäteriet or someone else behind a solution that is the organization that determines what the digital codes represent and who is authorized to transfer or act in a contract. In other words, Lantmäteriet guarantees which digital representation a specific property has. Another central part is the identification of the actors who will have rights to act in the system. For this, a secure ID solution is required. This solution also needs to be easily accessible to the actors involved.

If we look to the future, we see a world where mobile phones play an

increasingly important part in the ID solutions being developed. Telia is a company headquartered in Sweden that is well positioned to create such a solution for the future. Telia already have an ID solution that can be used in mobile phones and can register people with or without a personal identification number (The Swedish equivalent of a social security number). In addition, Telia's solution is currently used by agencies within the healthcare system in many county councils. Telia is also present in several markets and therefore has the resources to do this and comply with existing and forthcoming EU requirements.

Real estate transactions today

The goal of the project is to improve how real estate transactions are performed. The most common real estate transaction is the purchase of a private residence. Here we first describe the main features in this process as it stands today. Following this we will explain how we believe it will look in the future.

Real estate transactions by private persons via real estate agent today

1. A property owner wants to sell her property.

2. The property owner, i.e. the Seller, contacts a real estate agent and draws up an agreement for managing the sale of the property.

3. The agent contacts Lantmäteriet and orders an excerpt from the real estate registry database in order to check the information about the property, i.e. that the seller is in fact the owner and can sell the property.

4. The agent puts the property up for sale and markets the property to potential buyers.

5. The Buyer goes to a bank, the Buyer's bank, and asks for a loan commitment. The bank checks the Buyer's credit rating, often in a digital registry such as UC. The Buyer's bank approves the loan commitment.

6. The property is put out on display to the market and eventually offers are made.

7. The Buyer that makes the highest offer makes an initial inquiry about credit options for the specific residence with the Buyer's bank.

8. The Buyer's bank inspects the property and evaluates the credit options for the Buyer. The property and the Buyer may be inspected again in the respective databases.

9. The Bank approves the purchase price and the amount of the loan for Buyer, which is often communicated over the phone.

10. Prior to signing the purchasing contract, the agent again checks on the seller and the property with Lantmäteriet. The agent also often checks that the Buyer actually has a loan commitment from the bank.

11. A purchasing contract is drawn up between the Buyer and the Seller together with the agent, often at the agent's office. Often four copies of the contract are created, one for the seller, one for the Buyer, one for the agent and one for the Buyer's bank.

12. The contract is sent by the Buyer to the Buyer's bank, often by regular mail.

13. The bank sends credit documents to the Buyer, often via regular mail.

14. The Buyer signs the loan documents and also writes a note to the bank to pay a down payment into the agent's escrow account.

15. The Buyer sends the signed loan agreement to the Buyer's bank via regular mail.

16. The Buyer's bank receives the loan documents and pays the down payment to the Agent.

17. The property may be inspected by the Buyer.

18. The agreement becomes binding if there were conditions in the form of inspection.

19. The agent pays the down payment to the Seller, while deducting the agent's fees.

20. After this step, the main thing remaining is to actually sign the bill of sale, transfer the possession of the property and make the final payment. This is often done roughly 3 months after signing the purchasing contracts.

21. Closing: The agent checks on the property and the Seller in the database of Lantmäteriet again to ensure that there aren't any problems that would prevent the sale of the property.

22. The Buyer and Seller sign the bill of sale at the agent's office. The Buyer signs for the mortgage and any other mortgage deeds on the property.

23. The purchase price is paid by the Buyer's bank to the Seller's bank. Often this payment is made via a direct deposit where the Seller's bank and the Buyer's bank confirm that the transfer has been made.

24. The Buyer, Seller, as well as the agent, each save a copy of the contract, as well as a copy for the Buyer's bank, and the Buyer may now move into the property.

25. The Buyer's bank goes into the mortgage deed system of Lantmäteriet and requests the mortgage deed on the property from the registry.

26. The Seller's bank releases the mortgage deed to the Buyer's bank

27. The agent sends the bill of sale to the Buyer's bank.

28. The Buyer's bank sends the title registry application along with the bill of sale and any application for a new mortgage (i.e. an increase in the mortgage beyond the existing mortgage deeds) to Lantmäteriet.

29. Registering the property title: Lantmäteriet grants The Buyer a Property title, and the title is registered in the land registry.

30. A new mortgage is granted, and the Buyer's bank is registered as the

mortgage deed holder in the mortgage deed system.

31. Lantmäteriet decides on any service charges and stamp duty (based on the purchase price or the assessed value of the property).

32. Lantmäteriet is paid (usually from the bank) via an automatic payment account for the title and the mortgage deed.

33. Lantmäteriet notifies the Buyer's bank, i.e. the title applicant, by regular mail that the title has been granted.

34. The Buyer's bank notifies the Buyer that the title has been granted and the transaction is performed via regular mail.

Summary of the current situation

What we see above is that the Lantmäteriet is involved relatively late in the process. Not until item 28 does Lantmäteriet make any active decisions or receive any of the submitted documents. Prior to that, it is primarily the agent who checks the land registry to check the ownership of the property. There are several disadvantages with this system. Lantmäteriet is the actor with the highest credibility, and if Lantmäteriet is involved earlier, the confidence and transparency in the process increases.

The second thing that can be noticed is that the process takes a long time. There are likely advantages with the process because the buyer and seller of a residence will often want to have time to sell the previous residence and find a new one. It also takes significant time to prepare all the information. The agent needs to check on the owner and the property several times. The bank may check credit and real estate information several times. Information that is already listed in the purchasing contract is written again into the bill of sale.

A third thing we notice is that there are still a lot of documents that are signed on paper and sent via regular mail. Checking these documents and the identity of the people who signed them must be done manually. Today, agents, buyers and sellers can be sitting for two hours signing several hundred pages of documents when signing a purchasing contract, since all of the documents and often all of the pages in several documents need a signature or initials written by hand. This takes time and it's easy to make mistakes.

The amount of documentation and information that must be saved also leads to mistakes. In 2015, Lantmäteriet granted 91% of all applications and 94% of all e-applications. Therefore, it is relatively common that papers need to be filled in a second time because they are incomplete or there are mistakes.

All of these records must be stored by law for ten years, which requires physical space and increased security, e.g. in the agent's offices and at the banks. Searching for information in old records is also timeconsuming.

Property transactions in the blockchain

The example above illustrates the current process for real estate transactions. With the example below, we want to illustrate what this would look like in the future. The testbed that has been developed by ChromaWay as part of this project makes it possible trial the process, including a large part of the suggested improvements below, in an environment that closely resembles a real world implementation.

Purchasing small houses by private persons via real estate agents in the future

1. A property owner wants to sell a property.

   New Solution: The property owner can check their ownership and whether there are any obstacles to the sale by themselves using the app from Lantmäteriet ("My property account") and by verifying their identity via their mobile phone.

2. The property owner, the Seller, contacts, a real estate agent and draws up an agreement for a real estate sale.

   New solution: The property owner, the Seller, contacts a real estate agent and commissions the agent to sell the property via the app. The agent accepts the offer to manage the sale of the property. In practice, the agent can also guide an individual through these steps in the app.

3. The agent contacts Lantmäteriet and orders an excerpt from the property data-base in order to check the information about the property, i.e. that the seller is in fact the owner and can sell the property.

4. The agent puts the property up for sale and markets the property to potential buyers.

5. The Buyer contacts a bank (digitally), the Buyer's bank, and asks for a loan commitment. The bank checks the Buyer's credit rating, often in a digital re-gistry such as UC. The Buyer's bank approves the loan commitment.

6. The property is put out on display to the market and eventually offers are made.

7. The Buyer who makes the highest offer makes an initial inquiry about credit options for the specific residence with the Buyer's bank.

New solution: In the future, this step is superfluous because the agent can see the information directly in the app and any applications for changes in the land registry are communicated immediately.

8. The Buyer's bank inspects the property and evaluates the credit options for the Buyer. The property and the Buyer may be inspected again in the respective databases.

New solution: In the future, the property does not need to be questioned again because the latest information is always available and can otherwise be checked directly in the app.

9. The Bank approves the purchase price and the amount of the loan for the Buyer, which is often communicated over the phone.

New solution: The Buyer's bank can provide preliminary approval of the loan so that the agent and the Seller can be confident that the Buyer has the ability to pay.

10. Prior to signing the purchasing contract, the agent again checks the Seller and the property with Lantmäteriet. The agent also often checks that the Buyer actually has a loan commitment with the bank

New solution: The Buyer's bank is given access to the property via the app and the bank can check the property there. Information about the condition of the property, inspection report etc. can be included in the app or linked to the app.

11. Often four copies of the contract are created, one for the Seller, one for the Buyer, one for the agent and one for the Buyer's bank.

New solution: The necessary information is registered in the app, e.g. date of possession and purchase price in digital fields, which reduce the risk of the contract being incorrectly formulated. Signatures are provided in the app using Telia ID or another ID solution. Everyone involved can retain a copy of the agreement and the verification record in the blockchain in their mobile phone or computer for extra security. The contract cannot be lost or falsified. If anyone wants to print out a paper copy, it is easy, but it is then just a copy that is only valid for the time when it is taken out. The contract is also shared with Lantmäteriet, which registers the pending property title at no cost until the final verification record for the transfer (bill of sale) is distributed. The information about the purchase price and the property can be made public, which provides security for the Buyer and Seller and is important information for entities like Sweden's national statistics bureau and central bank.

12. The contract is sent by the Buyer to the Buyer's bank, often by regular mail.

New solution: The Buyer's bank can see the signed contract in the app and does not need to send it.

13. The bank sends credit documents to the Buyer, often via regular mail.

New solution: The credit documents can be attached to the app and signed directly when the purchasing contract is written up. ChromaWay's technical solution makes it possible to make the credit documents accessible only to the Buyer and the Buyer's bank. If the Buyer does not want to display how much is being borrowed to other parties, access to the credit documents can be encrypted or sent outside of the app.

14. The Buyer signs the loan documents and also writes a payment order to the bank to pay a down payment into the agent's escrow account.

New solution: The Buyer can sign the loan documents as well as the payment order for the down payment directly with signatures in the app.

15. The Buyer sends the loan agreement to the Buyer's bank via regular mail. The Buyer's bank receives the loan documents and pays the down payment to the Agent.

New solution: The loan documents do not need to be sent via regular mail because the bank gets a digitally signed copy of them directly when the purchasing contract is written.

16. The Buyer's bank receives the loan documents and pays the down payment to the Agent.

New solution: The bank can pay the down payment to the agent directly at the time of signing the contract, because the Buyer signs the payment order digitally.

17. If there is a condition that has to be met like an inspection of the property by the buyer, the property may be inspected by the Buyer.

18. The agreement becomes binding if there were conditions in the form of inspection.

19. The agent pays the down payment to the Seller, while deducting the agent's fees.

20. After this step, the main thing remaining is to actually sign the bill of sale, transfer the possession of the property and make the final payment. This is of-ten done roughly 3 months after signing the purchasing contracts. During this time the mortgage deed transfers can be prepared and signed following the process for mortgage deeds described in that section of the report.

21. Closing: The agent rechecks the property and the Seller in the database of Lantmäteriet to ensure that there aren't any problems that would prevent the sale the property.

New solution: With the new solution, this is not needed. The pending property title is already granted. If no changes have been made, this is displayed and the next stage can be processed without further changes or checks of the contract or real estate.

22. The Buyer and Seller sign the bill of sale at the agent's office. The Buyer signs for the mortgage deed on the property.

New solution: In the new solution, this is done with digital signatures and digital identification. The risk of incorrect formulations in the bill of sale is minimized since the necessary information is already there and any new information is entered digitally and verified automatically.

23. The purchase price is paid by the Buyer's bank to the Seller's bank. Often this payment is made via a direct deposit where the Seller's bank and the Buyer's bank confirm that the transfer has been made.

24. The Buyer, Seller, as well as the agent each save a copy of the contract and write one for the Buyer's bank, and the Buyer may now take possession of the property.

New solution: With the future solution, the contract is already available in the app. If anyone wants a physical copy of the contract they can print it out. The copy also has a verification code that is registered in the blockchain.

25. The Buyer's bank goes into the database of Lantmäteriet and takes over mort-gage deed in the mortgage deed registry of Lantmäteriet.

New solution: With the mortgage deed application everyone involved in the mortgage deed transfer has already signed this contract. If and only if all requirements are fulfilled for the land title to be transferred to the owner will the mortgage deeds be transferred to the buyer's bank.

26. The agent sends the Bill of sale to the Buyer's bank.

New solution: The bill of sale and documentation for the mortgage on the property is already accessible to the bank via the app.

27. The Buyer's bank sends the application for the property title along and a new mortgage (i.e. increase in the mortgage beyond the existing mortgage deeds) to Lantmäteriet.

New solution: This information is already accessible and distributed to Lantmäteriet in steps 11 and 22, and in the mortgage deed application.

28. Registering the property title: Lantmäteriet grants The Buyer a Property title, and it is registered in the land registry.

New solution: The pending property title is already granted and the process of verifying the agreement can proceed more quickly through automated decisions because the risk of incorrect formulations in the bill of sale is reduced when this is done using digital fields.

29. The Buyer's bank is granted a new mortgage deed, which is registered in the mortgage deed system.

30. Lantmäteriet decides on any service charges and stamp duty.

31. Lantmäteriet is paid via an automatic payment account for the title and the mortgage.

32. Lantmäteriet notifies the Buyer's bank, i.e. the title applicant, by regular mail that the title has been granted.

New solution: Lantmäteriet's record of the property title and the mortgage is shared via the app and all parties can see that the title has been granted.

33. The Buyer's bank notifies the Buyer that the title has been granted and the transaction is performed via regular mail.

New solution: This step is not needed. Information about the property title goes directly to the Buyer, Seller, agent, Buyer's bank and the Seller's bank via the app.

Summary of possibilities with the new technology

The future process example includes a number of improvements. The time between when the purchasing contract is written and when the pending property title is registered with Lantmäteriet can be reduced from 4 months to a few days. Eventually, this could take place more or less in real time. The Buyer is granted the pending property title, and the property cannot be sold a second time by the seller.

The information that is needed for the bill of sale is already registered in the system for the most part. Therefore, in practice, the buyer and seller sign the same information upon taking occupancy. The risk that the property title will not be granted is sharply reduced since the system can ensure that the information that is required by law is included in the system and is required by the system before the parties are able to provide their signatures.

In fact Lantmäteriet may actually automate the land title registration. If no other transactions or changes have been made in the property Lantmäteriet can execute the registration automatically since the manual checks that are necessary have already been made. Lantmäteriet wants it to be easy for citizens and stakeholders to do things correctly, and this is considerably easier in a digital system.

Digital signatures provide a significantly greater level of assurance that the correct people will be filling out the correct documents. Since digital signatures are provided with the same application at several instances, the risk of errors and fraud is reduced. The process involves multiple contact points and multiple signatures by the parties involved. This increases confidence in the system since it is more difficult to manipulate the system over a long period of time.

In addition, the purely manual portion of sending paper by mail is streamlined and made more secure. All of the parties can save the digital files and verification records of the entire chain of events digitally. Paper copies can be printed out if desired, but the process saves a lot of documentation.

Mortgage deed process

The current process for mortgage deeds is very complicated. It involves a lot of processes, and physical documents are still a common component even though digital mortgage deeds are becoming the norm. Below is an overview of the current process. Currently the process may involve as meny as 36 steps to complete a transaction. With the blockchain the same process can be significantly impoved and uncertainty of current state reduced. The transfer of mortgage deed will be transparent and executed by the contract. The following process is reduced to 7 steps.

A new proposed process for mortgage deeds

As a preliminary example of how the mortgage deed process could look in the future the below steps are described.

1. The real estate owner choose the manager of the contract and whether the contract involves a sale of the real estate or if it is only a transfer of mortgage deeds without the sale of the real estate. In this use case there is a real estate transaction.

2. The manager of the contract which will receive the mortgage deed, usually the Buyer's bank, checks the current state of the mortgage deeds for this particular property. The bank thereafter enters all the details of future holdings of the mortgage deeds, their priority, possible secondary holders, and the public keys identifying these holders in the contract. In most cases there will be only the bank holding the mortgage deeds. If there is a need to increase the level of mortgage deeds additional deeds are registered as well.

3. When all the details have been entered into the contract each person and bank, which is giving away or receiving a mortgage deed signs the contract in the application. Everyone here confirms that they will be the holder of the contract or they will give up their mortgage

deed. However, this will only be executed if and when the land title is transferred.

4. When everyone has signed, Lantmäteriet registers that the transfer of the mortgage deeds will be legally finalized if and only if the land title is successfully transferred. The steps above will normally take place between the signing of the purchasing contract and the signing of the bill of sale.

5. The actors who are involved in the real estate transaction process finalize that process and sign the bill of sale. Ideally there are no changes in the real estate contracts and Lantmäteriet can automatically register the land title with the new owner. Lantmäteriet then also finalize the transfer of the mortgage deeds when the real estate transaction has been granted. This connection between the real estate transaction contract and the mortgage deed contract may be automated in the future but will require manual work in the first solution.

6. Lantmäteriet calculates the fees and taxes for the transaction in the mortgage deed registry and sends the invoices.

7. The application will transfer all existing mortgage deeds. If there are new mortgage deeds needed they will not be given to the new holder of these deeds before the payment of the taxes for these new mortgage deeds is completed.

As seen in the example, the mortgage deed process is significantly improved and simplified. Today the Buyer's bank, which is to receive the mortgage deeds, may sometimes have to wait 6 months because the bank holding these mortgage deeds doesn't release them. The banks themselves have asked for a solution to this problem. They want the transfer of the

mortgage deed and the transfer of money to be dependent on each other. The process described would solve that problem.

The Buyer's bank doesn't have to worry about when they receive the mortgage deeds. The Seller's bank has had to sign the contract before the payment is made to them. Payment is conditional on the mortgage deed transfer.

The process also prevents the possibility of having to reverse mortgage deed transfers if a land title is not transferred.

# An overview of the IT architecture

The solution in short

In an initial stage, the database of Lantmäteriet remains intact. Updates to the land registry are retrieved from the blockchain and are then also checked by Lantmäteriet. Registration in the blockchain is digital and based on the legal requirements, which minimizes errors in the information.

The blockchain for the transactions is open source and is checked by Lantmäteriet, and other nodes running the blockchain. The chain of authorization, signing with a Telia ID, etc. can be edited in the administration interface, but any changes will be visible to all parties to prevent fraudulent changed of the contract/application. The blockchain saves the verification records of documents such as the bill of sale and the purchasing contract, all signatures etc. Storing the original documents and their verification records can be performed by an external party, but can also be stored digitally by each party in the agreement, the bank, buyer, seller, agent, etc. The documents and verification records are then stored in multiple locations, which creates redundancy. The verification records are also summarized in an external blockchain and/or transparent to the public, which means that all of the parties can feel secure that they can recreate and demonstrate the chain of events on their own, in the event that the other parties suffer a breach of data or similar event.

Technical overview

There are seven parts of a blockchain solution that can be considered to be standard, at least in the case of private blockchains. These components are described below.
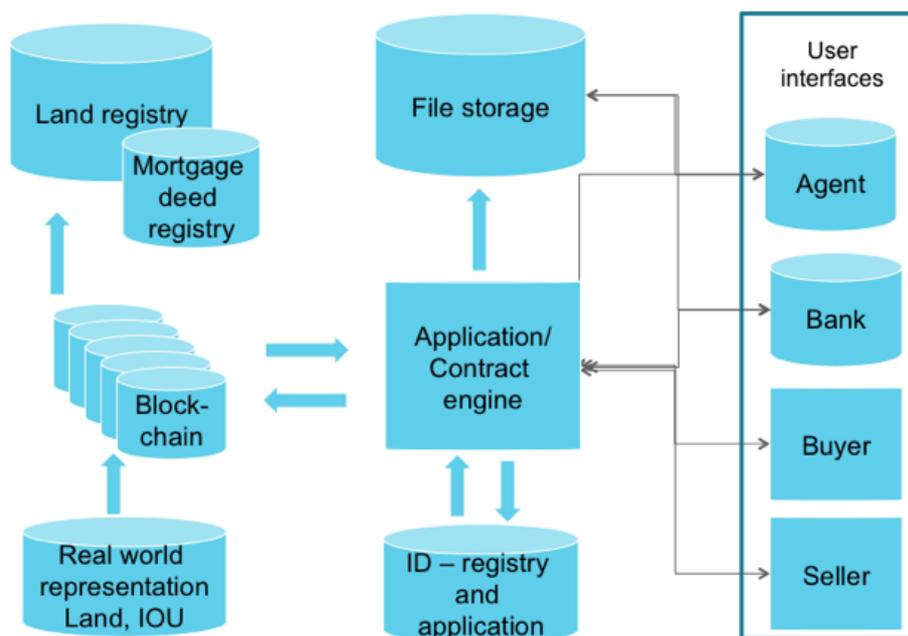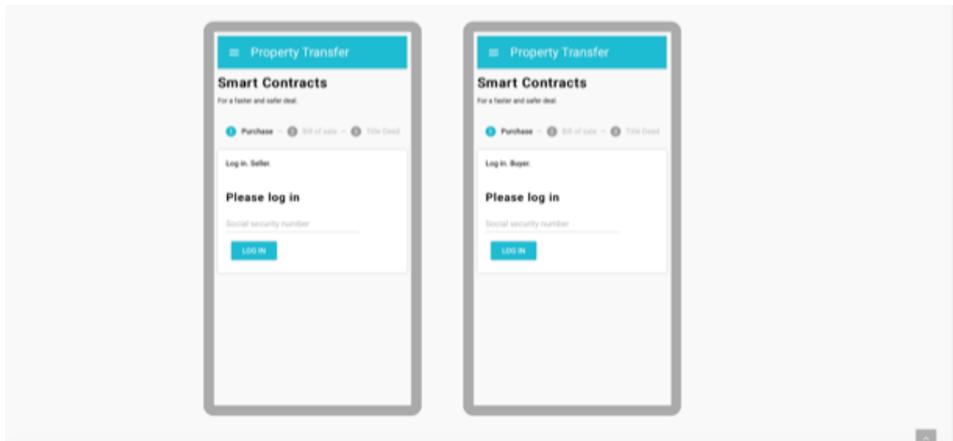
User interfaces

The user interfaces are designed for different users. There are three main categories of user interfaces.

End-users - typically the buyer and seller of real estate

These users are expected to use their mobile and a dedicated app for the solution. The real-estate agent can assist them in setting this up. These users will see the state of the contract and when they are in turn to take action. They will also be able to store the details of the contract as they see fit.

**Professional users – typically banks, agents, Lantmäteriet**

These users will be able to see the contract in a professional interface, and the application will ideally be integrated with their own systems and processes. These users will act as professionals and employees of an organization and in most cases represent the organization and not themselves. Their user interface will be adapted to their needs.

Contract administrators – typically Lantmäteriet and the architects of the solution

These users will administer the contract for the other users. The setup of the contract can be revised and changed quite easily at this point in time. In a launched solution the software/application edition in use has to be fixed and changes overseen by all partners running the blockchain.

The administration interface looks like this:
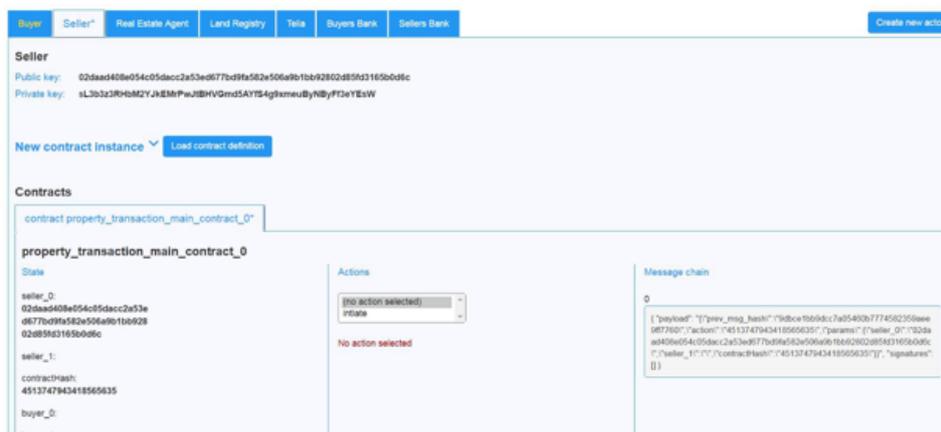
The administration user interface has four important sections

1. **The top bar:** Here the different actors are seen. The manager of the contract adds the actors; in the case of the real estate transaction it is usually the real estate agent. In the case of mortgage deeds it is usually the buyer's bank.

2. **The left column:** To the left the fixed properties of the contract are seen these are typically contract date, real estate identity number, the public keys of the actors involved in the contract, the price, the date of transfer etc.

3. **The middle:** In the middle there is selection of possible actions and below the different fields to enter or sign. Like the price entered. This is where the actions which progress the contract appear.

4. **The right column:** To the right are all the messages which are posted to the blockchain. Exactly these messages can also be seen with other messages from other contracts in the blockchain.
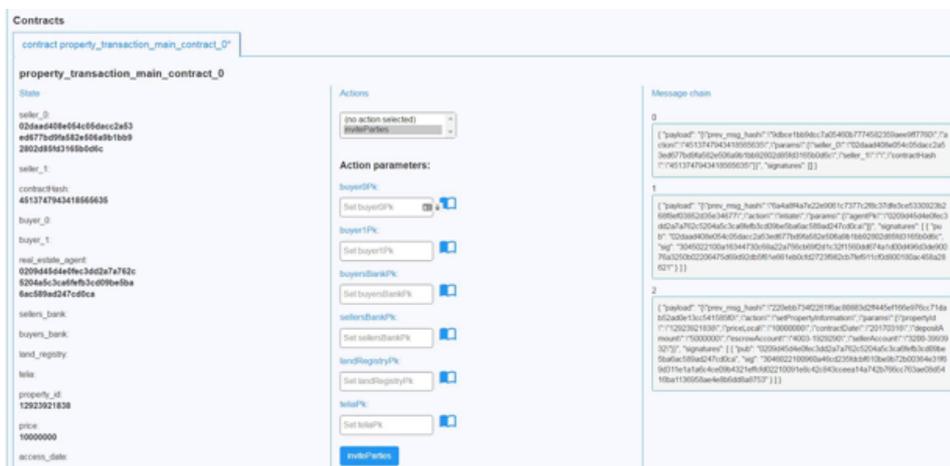
In this overview there has been two more steps taken and the messages to the right have become three. More information around the contract is now fixed in the left column.

The file storage

Each actor can make the file storage of contracts by herself. In almost all cases the blockchain will not contain all information, but instead contract verifications, hashes. The original files have to be stored separately. This can be made in the cloud or at the choice of the bank, agent etc. In a public blockchain the data storage has to be kept small so that the entire

data set doesn't become too large and slow to transfer over the network/internet. After eight years of operation the Bitcoin blockchain is a more than 100 GB. In our case, low network overhead and the low cost of storage means that realistic restrictions are much less burdensome than those of the Bitcoin network. The data that will be stored on the blockchain is primarily the content of the contracts, the data required for consensus among the participants, and other information like the closing price, the day of actual transfer of the property, and the public keys of the participants. It is possible that eventually the full purchasing contract and bill of sale will be stored in the blockchain as well.

File storage may not be handled jointly, but can be arranged according to the needs of different actors. The data storage will save a lot of work for real estate agents, banks, Lantmäteriet and the buyer and seller since they won't have to maintain a physical archive.

The blockchain

The blockchain is the part where the transparent transactions are recorded and stored. This is equivalent to the distributed ledger. The nodes decide what is going to be committed to the blockchain. There may also be nodes that are not part of the validation process but simply store the record.

In a public blockchains such as Bitcoin and Ethereum, anyone is allowed to be a node and keep a copy of the ledger. They can be a node which verifies and accept transactions and information that is going to be stored in the blocks. or they can simply keep a record of what is committed to the blockchain by the others. In practice those who want to be nodes which verify transactions need substantial processing power to have the chance to be part of the system. In our case the blockchain

is permissioned which means that only trusted partners are allowed to validate transactions and blocks.

Land registry, mortgage deed registry

The current database for the land registry contains a lot of information about the real estate. This data can be understood as metadata. Information can be obligations or rights for the property in relation to others, such as the right to use water or roads for another property. All this data will not be stored in the blockchain in the proposed solution, but may be in the future, or may be verified in the blockchain and stored elsewhere.

To access this data agents, banks etc. still need to contact Lantmäteriet through existing systems. The transactional data will be retrieved from the blockchain to the land registry.

The registry of mortgage deeds will, for legal reasons, be similar. The difference here is that the blockchain will store all relevant data. There is no metadata, which is only found in the mortgage deed registry. It will therefore be possible to use the blockchain as the actual mortgage deed registry over time without major changes in technology or processes, at least if physical mortgage deeds are transferred into digital.

Application/contract engine

The application or contract engine is a key element of the solution. The most well known blockchain solution for applications is Ethereum. In Ethereum the contracts are called distributed applications. The applications are run on the blockchain by all nodes, they are distributed.

In the proposed solution the contracts are not run on the blockchain – they are confirmed in the blockchain, we can say their verifications are embedded in the blockchain but the entire application is not run by the blockchain network. The contract is like a middleware running on the end-user's hardware. Some people believe this is a larger risk, but with the blockchain any changes in the contract can be observed. Manipulations are easy to identify and there is no central point of failure for the system.

The ID and authorization

The actors who are going to authorize the different steps in the process have to be identified. This is one of the major challenges for digital solutions. In the case of Bitcoin, possession of the correct private key is sufficient authorization to spend the associated bitcoin. The problem with this is that the storage of the key becomes crucial. Most consumers are not capable of securely storing their private key in the long term. If the private key is lost or stolen all Bitcoins can be lost.

Making an ID-solution and securing the adoption of the ID-solution may be the most difficult problem for the solution to be used in a widespread way globally. The ID-solution has to be adapted to the country, law, process, and culture. The eIDAS project in the EU is an example of an effort to standardise eIDs across a wide area.

While the ID solution is a major concern, the blockchain is also an enabler of ID-solutions. It is rather simple to add levels of security of an ID solution with the blockchain. For example if a public authority or a person wants higher security in the form of a copy of a driving license it is easy to make a copy and add that to the contract in the blockchain. The flexibility of the ID-solution is easy to adjust with the blockchain.

The real world representation

In the case of cryptocurrencies there is no need for a real world interpretation of the digital units. It's an open market, which decides if the digital units have a value, and apart from that value it has little meaning. In the case of a colored coin an issuer decides if the colored coins represent Euros (as in the case with LHV Bank) or any other financial asset. The real world interpretation may, however, be other things than financial assets and land. Many people who have heard of this project have thought that we are trying to implement a solution for digital transfer of land, similar to Bitcoin transfers. This is not the case. Digitally representing all of the packages of land in Sweden so that they can be traded directly on the blockchain without involvement of Lantmäteriet, agents or banks is not the ambition of this project. And there are no such plans for the future either.

Rather, this implementation focuses on digitally representing the processes by which property is transferred between parties. The contracts represent the identities of individuals, organisations, and property such that it is possible to authoritatively connect the representation in the contract with its real world correspondent. It is necessary to have an organization, in this case Lantmäteriet, to assign the representation of the property so that it can be identified in the blockchain. Any contracts related to a particular property can therefore easily searched and tracked by a unique ID.

Other information such as promissory notes can also be represented in the blockchain. It may not be Lantmäteriet who assigns the real world representations of all digital identities in the contract. It can be another public authority, a consortium of banks etc.

The result

The end result is a secure process for real estate transactions and mortgage deeds with the following characteristics:

1. All involved actors will have a digital file representing the agreement of ownership of the real estate, mortgage deeds and the transaction process. These files can be stored in the cloud, locally, or some other method of the actor's choosing.

2. The authenticity of the process, the signatures, the file confirming ownership, mortgage deeds etc. will be secured with a blockchain. The Swedish Lantmäteriet will store the blockchain with the proofs, but the blockchain will also be stored and validated by other actors. It will therefore be easy for authorised third parties to verify information. These third parties would usually be actors who are part of the process: banks, buyers, sellers, real estate agents etc.

3. The records and files that should be public according to Swedish law will be public and those which should be confidential will stay confidential.

4. There will be no bearer instrument stored on the blockchain in the current implementation. This precludes the risk of such authoritative documents being lost, stolen, or tampered with. Bearer instruments could be implemented in the future, but it should be noted that doing so entails risks and legislative uncertainties that require further investigation.

5. The only way to steal a property is through entering a new real estate transaction process with stolen or forged identification. The security of the ID-solution can be improved according to the requirements of the system in question. More stringent identification procedures (photos of physical ID-cards, biometric identification, multi signatures, etc.) can be easily implemented.

6. The current process is designed to involve Lantmäteriet, real estate agents, buyers, sellers, and banks. These are the parties involved in most real estate transactions in Sweden. The process can be redesigned to involve other actors such as notaries, insurance companies and local public authorities.

The next step

The development of an IT solution using blockchain technology for real estate transactions is a long term project that is best implemented in stages. The first stage was a proof of concept. This second project has been the building of a testbed with working technology. The solution has not yet been subjected to scaling, optimization, and integration development.

The continued project:

The plan is to further look into the solution and the requirements for a potential launch.

Technical environment

A list of requirements in terms of the IT environment with servers, storage, nodes that verify the blockchain, local storage in the mobile phone, in the cloud, etc. These can then be drawn out, designed and tested to ensure the proper IT architecture, and to further check the processes and security of the solution.

Technology and process integration

The project will also need to integrate with existing systems and processes, primarily banks and real estate agents, and the Land Registry in order to ensure that the service works with the partners involved in the process. Further process improvements can then be identified too.

More partners and partner projects

The international interest in the project has been impressive. The project

team has met, and discussed the solution with public authorities from more than 10 countries already, aside from several large conferences and presentations, including the Land and Poverty conference arranged by the World Bank in March 2017. A lot of companies, primarily banks, have also been very interested. This has resulted in more than 100 meetings with representatives from organizations from around the world. Media coverage has been very widespread. The project would benefit from more partners and other teams working on similar projects to stimulate development and learning. The project team sees a good value in getting more partners and other projects up and running.

Legal conditions and lobbying

Further lobbying, investigation and innovative solutions to allow for a digital process with digital signatures is a key element to secure the realization of the value of the project.

Ownership and governance

The operation of a blockchain is a joint responsibility. The appropriate governance and incentives for operation has to be set up. The ambition is to make the solution open source to a large extent. Still, ownership of the software and hardware, and a framework for potential external partners for cloud solutions, storage, network etc. has to be outlined. There are many possibilities to develop new solutions and services with the use of the data and platform developed. Conditions for this has to be discussed, and the process for decicion on changes investigated.

Participants in the project

Lantmäteriet
Mats Snäll, project owner
Jörgen Sannagård
Susanne Forsberg
Tobias Lundberg

Kairos Future
Magnus Kempe, senior project manager

Telia Company
Björn Hallare, project manager for ID-solutions
Magnus Leonhardt
Lauri Immonen
Vincent Vanot
Henrik Sund
Peter Lewandowski

ChromaWay
Jörgen Modin, project manager for technical solutions
Ludvig Öberg
Henrik Hjelte
Alex Mizrahi
Kalle Rosenbaum

SBAB
Jim Petersson
Henrik Ljung
Catharina Carlsson

Landshypotek Bank
Merete Salmeling
Claes Fransson

Disclaimer
This report is a best guess and an effort to explain this very interesting technology and the future of real estate transactions. The report is a simplification of many things and may not be fully accurate in the eyes of the participants or the organizations they represent. No one takes responsibility for the content or the interpretations of the report. We look forward to learning more about the technology and its implications for society. Magnus Kempe is the author of the report.

Contributing organizations

Lantmäteriet

Lantmäteriet produces geographic databases and maps and is charged with helping ensure confidence in the ownership of properties and the long term sustainable use of Sweden's land and water. Lantmäteriet has roughly 2000 employees across 60 cities. Lantmäteriet's head office is in Gävle.

ChromaWay

ChromaWay are pioneers in blockchain technology and have several times been ranked as one of the world's leading companies in the field. The company has its main office in Stockholm and employees around the world.

SBAB

SBAB's business concept is to provide loans and savings accounts to individuals, housing societies, and real estate companies with creativity and care. SBAB was founded in 1985 and is wholly owned by the Swedish state. The company has ap-proximately 350,000 customers and 500 employees. SBAB has the most satisfied mortgage customers in 2014, 2015, and 2016, as measured by SKI (Swedish Quality Index). Learn more at www.sbab.se, www.twitter.com/sbabbank, www.facebook/sbabbank.

Landshypotek Bank

Landshypotek Bank's fundamental mission is to finance the investments of farmers and foresters. The bank offers savings to those that wish to save with good terms and conditions and that love the countryside as much as we do. The bank is also now opening opportunities to offer mortgage loans to homeowners outside the major cities. Landshypotek Bank has about 170 employees at 19 locations in Sweden.

Telia Company

Our 21,000 talented colleagues serve millions of customers every day in one of the world's most connected regions. With a strong connectivity base, we're the hub in the digital ecosystem, empowering people, companies and societies to stay in touch with everything that matters 24/7/365 - on their terms. Headquartered in Stockholm, the heart of innovation and technology, we're set to change the industry and bring the world even closer for our customers.

Kairos Future

Kairos Future is an international consulting and analysis company that helps companies understand and shape their future. By analyzing trends and the world around them, as well as innovation and strategies, we help our customers see the big picture. Kairos Future was founded in 1993, our main office is in Stockholm, and we have representatives and partners across the entire globe.