**PAGE 1**

**Blockchain-inspired technical solutions for accounting, auditing, and taxation**

A collaborative project between FAR, Skatteverket, Kairos Future, Visma, SEB,

Fortnox, and FAR’s members PwC, Deloitte, Grant Thornton, and KPMG.

January 2019

**PAGE 2**

**Summary**

This report summarizes the result of a project in which FAR, Skatteverket (the Swedish Tax Agency), Kairos Future, Visma, SEB, Fortnox, and FAR’s members Deloitte, PwC, Grant Thornton, and KPMG have participated.

The purpose of the project is to identify challenges with today’s operations linked to accounting, auditing, and taxation. And to then describe these challenges, along with possibilities for solving them with the help of digital information chains, such as blockchain.

We want to demystify blockchain, and make the technology, and the principles it has contributed, more accessible and understandable by all. It stimulates more learning and the development of new thoughts, processes, systems and—in the long run—more fun and value-generating work in the branch of accounting, auditing, and taxation, as well as among companies.

The overall challenge is creating trust in digital processes, actions, identities, etc., among all parties involved. We want to increase efficiency, decrease risks and make it more difficult for companies to make mistakes, both conscious and unconscious. We also want to do this without compromising anonymity.

The most common approach to solving these challenges today is collecting more data in central databases. Doing so, however, often involves security risks and creates challenges in terms of both integrity and anonymity.

In *The Economist,* blockchainis described as a “trust machine.” One result of the project is that we regard the technology as a set of tools that can be combined in different ways to create trust. That is to say that it isn’t a technology and, in particular, not blockchain that is being proposed in the solutions.

The result of this project is five proposals for solutions within the following areas:

1. Digital receipt processing
2. Personnel registers
3. Realtime/SINK (Special income tax for people living outside Sweden)
4. Proxies
5. Company information services

For three of the above areas (*digital receipt processing, personnel registers,* and *proxies*), we believe that the proposals described in this report are very good solutions for creating social benefits. When it comes to SINK, there are a couple of dependencies on other processes that need to be investigated, and possibly resolved, before a solution can be realized. For the fifth solution, *company information services*, there are a couple of countries that have interesting solutions for different types of data. There is a need to identify which different groups of data should be in focus, as well as a need for better knowledge of those solutions that exist today in other countries, and their advantages and disadvantages.

In conclusion, the result is very promising. We consider it very likely that social benefits can be created amounting to well over ten billion SEK per year in Sweden alone, in a five- to ten-year perspective. It is deemed important that we continue to investigate and work further with new processes, law, and technology in all the five identified areas.

**PAGE 3**

**Contents**

**Summary**

**Introduction**

Purpose

Contributors

**Blockchain-inspired technology**

Share control, build trust.

**Trust from honor, control or dissemination**

Decentralization of value

Deconstruction of data

Share the parts

**Method and selection of solutions**

**Digital receipts**

**Personnel registers**

**SINK/Real-time**

**Proxies**

**Company information**

**Other support services**

**Technical explanations**

**PAGE 4 - 5**

**Introduction**

This is a report that summarizes a project that focused on exploring the possibilities of blockchain technology, as well as other technology that can be said to be inspired by blockchain. The starting point has been to identify solutions within the areas of accounting, auditing, and taxation. The hypothesis is that we can streamline and facilitate work among companies and create social benefits.

Blockchain technology has been said to signify some of the most socially viable opportunities in recent decades. The dollar can be replaced as the world’s currency, gold can be replaced as reserve currency for central banks, the world’s trade flows can be controlled safely, and virtual companies can act in the markets controlled by technology beyond the reach of nations and legislators. However, it has now been ten years since Bitcoin was launched and, so far, only the value of cryptocurrencies has come close to the visions promised.

But was *The Economist* wrong when they called blockchain “the trust machine?” Perhaps not. But in the interpretation of *trust machine,* too much focus has probably been placed on worldwide technology, indeed a single blockchain. In the project, we have tried to look at the possibilities with the new technology, but have focused on seeking new possibilities rather than using blockchain technology in its entirety. One term used in this report is “digitalized information chains,” a term that can be interpreted as “technology that does not allow data to be manipulated but, rather, it is followed like in a chain.” Since technology provides opportunities to create trust, this is something we have been curious about. In the project, we even tried to hold our ambitions at a reasonable level, which maybe differentiates us from the perspective held by others working with blockchain technology. We are satisfied if we succeed in saving a couple billon SEK per year in Sweden, something we believe is fully possible.

Our basic hypothesis is that blockchain has highlighted a number of technical tools that can be used to solve old problems in new ways. By gathering a group of curious people from a couple key actors working within accounting, auditing, and taxation we may be able to identify new opportunities to increase trust, reduce risks, save time and money, as well as to decrease both conscious and unconscious errors.

**Purpose**

The purpose of the project is to identify challenges with today’s operations linked to accounting, auditing, and taxation. And to then describe these challenges, along with possibilities for solving them with the help of digital information chains, such as blockchain.

The aim is that the participating organizations will be able to identify more opportunities for solutions to today’s problems, and thereby be stimulated to develop new technical solutions with the purpose of producing digital information chains that can be of great benefit.

The ambition is also to spread knowledge of these solutions to more organizations and individuals. We want to demystify blockchain and make it accessible and understandable for more. It stimulates increased learning and the development of new thoughts, processes, systems and —in the long run—more fun and value-generating work, both in the relevant industries and in the business sector at large.

**PAGE 6**

**Contributors**

Contributors to this project have included FAR, Skatteverket (the Swedish Tax Agency), Visma, Kairos Future, Fortnox, SEB, as well as FAR’s members PwC, Deloitte, Grant Thornton and KPMG.

**From the project team, contributors have included the following:**

Karin Apelman, FAR  
Dan Brännström, FAR  
Camilla Carlsson, FAR  
Lena Henriksson, FAR  
Bengt Skough, FAR  
Göran Sundin, Skatteverket

Therése Allard, Skatteverket  
Pablo Dias Taguatinga, Skatteverket

Björn Erling, Skatteverket

Patrik Lindmark, Skatteverket

Eric Thorén, Skatteverket

Patrik Cardell, Visma

Jennie-Ann Karlsson, Visma

Håkan Runquist, Visma

Henrik Olsson, PwC

Jonas Hagström, PwC  
Lars Alm, Fortnox  
Cesar Nilsson, Fortnox

Fredrik Nilsson, KPMG  
Jens Gullfeldt, Deloitte

Magnus Folkesson, SEB

Johan Hörmark, SEB  
Magnus Kempe, Kairos Future

**PAGE 7**

**Interviews and workshop invitees:**

Amey Rajput, Tech Mahindra

Anna Eriksson, DIGG

Annika Follin, Bolagsverket

Christian Landgren, iTeam Einar Persson, iTeam

Jesper Granlund, Deloitte  
Johan Bergsten, Bolagsverket  
Jürgen Sûvalov, Estonian Information System Authority  
Lars Åke Lundberg, IT and telecom companies/Svenskt Näringsliv

Martin Runosson, Aspia  
Olle Kinnman, Deloitte  
Patrik Nilsson, Företagarna  
Roger Fagerud, DIGG  
Zizzi Marten, Tech Mahindra

**Limitation of Liability**

No organization or person is responsible for the contents of this report. The report is largely, but not exclusively, written by Magnus Kempe. In the report, the word “we” is used in reference to the project team, even if the project team does not take responsibility for or is not in agreement over the formulations contained in the report.

The legal obstacles that exist when it comes to putting possible solutions in place have not been investigated. The report does not claim that the various solutions fall within current legislation. The report is intended to be a source of inspiration in the continued work with the opportunities that blockchain-inspired technology offers.

**PAGE 8**

**Blockchain-inspired technology**

The word blockchain became widely known following the publication of a White Paper describing the construction of Bitcoin. There, it was described how groups of encrypted data, block, is linked together in a chain. Since the combination of some known and lesser known technologies showed a number of revolutionary possibilities, after a couple of years, blockchain became a technology concept. In this project, we want to get inspired by the opportunities blockchain has revealed, but also consider possibilities where blockchain technology is not used in its entirety. We are more interested in social benefits and opportunities than using a technology that can be described as blockchain.

There are a lot of different opinions when it comes to establishing what kind of technology a blockchain should consist of in order to be considered blockchain. For example, sometimes the term “Distributed Ledger” or Distributed Ledger Technology (DLT) is used. Blockchain has contributed to extraordinarily interesting discussions around law, technology, and philosophy. In the first part of this report, there are some views and perspectives inspired by blockchain. When it comes to the solutions described, however, we try to take a pragmatic approach. We use a technology for which we have strong support for claiming that it works, regardless of what it is called.

A basic principle in the project is that we try to identify opportunities with technology that is differentiated from the extremes. The general view is that the two extremes are blockchain and a central database.

These terms can be defined as follows:

**PAGE 9-10**

1. Blockchain: In the extreme case, blockchain is an openly distributed database. That is, all databases participating in the network have the ability to see and verify all registered information, and the information is the same in all databases.

2. Central database: In the extreme case, a central database is a single database that collects and verifies all information.

These two approaches also have links to control, where the former can be described as “code is law,” i.e., there is no need for legislators since the technology itself regulates what results are generated for different machines, people, and organizations. For example, no legislator can prevent money from being paid out in Bitcoin. At least that is the ambition of the system. In Sweden, the view of the government is essentially positive, and the need for an established infrastructure, where the legislation does not apply or cannot be defended, is probably less compared to other places, at least in the coming years.

The other alternative is to instead centralize the information, i.e., an authority or company collects all the information and then makes an assessment of how, for example, a law should be interpreted once the (increasingly complete) information has been collected. The disadvantage of this system is that if the government or company or individuals are given the ability to collect complete information, people lose much of their integrity and privacy. The large amounts of data that are collected and analyzed become the basis for power that can be abused by both the holders and those who, in one way or another, come across the information. One step that’s been taken towards regulating this danger is the General Data Protection Regulation (GDPR) and USA’s

equivalent, California Consumer Privacy Act of 2018. In practice, however, these regulations are too cumbersome and insufficient to achieve their purpose. Furthermore, the interpretations of these laws are currently not clear since there are not yet any legal cases. One example of this is the fact that there are many interpretations of what can be regarded as personal information, and what cannot. One indication is the fact that pseudonymization is not allowed, but anonymization is allowed. The regulations slow down some of the problems with personal information in parts of the world, but do not prevent them. There is also a risk that smaller, less scrupulous nations with poorer protection for people and company’s data can develop better services, for example better AI, with better access to data. An overly strict interpretation of GDPR will make it more difficult to compete with nations and companies that can more easily develop better technology. Blockchain technology, the encryption technique, and the opportunities the technology has brought to light indicates that there are great opportunities to combine the best of two worlds, i.e., secure data, anonymization, and, at the same time, control and advanced analysis services like AI.

In the aftermath of the large price drops that occurred for cryptocurrencies in 2018, it can be tempting to brush aside the technology and believe that we probably don’t need to learn anything about blockchain. We hope that this report widens the perspective and stimulates more learning about the different technologies and approaches that blockchain is built upon. Many of these technologies are likely a prerequisite for building a world where democracy, private life, etc., can continue to exist as we see them today.

The growing dependence upon the internet as societal infrastructure is a further reason why it is important to seek out opportunities to secure this infrastructure with encryption technology, where blockchain is one example. There is a growing threat against the internet in the form of connected computers and, not least, other things besides computers, that which is usually called the internet of Things (IoT). Today, it is difficult to verify whether the connected devices are being manipulated. All of these connected devices are, therefore, at risk of being hacked and can then attack the internet through, for example, overload attacks.

**PAGE 11-13**

The basic thesis is that there is an increased need to collect and share parts of data, but we need to use the new technology that exists to do this in a wiser way. Blockchain technology has paved the way for a series of new innovations and ideas that cannot wait any longer to become reality. The hypothesis from the start of this project was that there are several different user cases that can save billions of kronor every year in Sweden alone, and in several cases, this can be relatively easy to realize.

**Share control and build trust**

“We must move beyond transactions and to more meaningful relationships. Must achieve right balance of being in touch and in control. The paradox is that the more we are in control, the more out of touch we are. The more we give up control, the more we become in touch.”

AG Lafley Chairman, President, CEO of P&G at ANA conference Masters of Marketing 2006

If AG Lafley were to hold a similar speech today, he would probably say: “The more we give up control, the more we build trust.” Blockchain technology and the broad group of other technologies we have identified as interesting in this project are built upon the same principle. By giving up control, we build trust. One concrete example of this is the principle of public access to official records. By making it possible for citizens to request meeting minutes, decisions, documents, etc., from public actors, public actors are divested of some control. Normally, they cannot refuse to disclose material that is requested. It reduces their control, while at the same time increasing confidence in the public sector. Mismanagement can be detected relatively easily.

In a closed system with full control, citizens and journalists can have a considerably harder time detecting evidence of errors and crime. At the same time, a loss of control comes at a price. It may therefore be inappropriate to share complete data. Digitalization has made the principle of public access to official records worse than before in certain situations. Sensitive personal data can, for example, be sold at a larger scale for a lower price, compared to before. Neither is the data of private companies subject to the same requirements of openness as authorities. For example, private companies can maintain secret board minutes. In this case, society has deemed the gathering of complete data as competition sensitive, risky, and an infringement of privacy. Instead, information is requested by different authorities. With this safeguard in place, it becomes more difficult for companies to misbehave. Yet another control device is the auditor’s inspections. By forcing a company to let a third party review their financial reporting, the company is thus forced to relinquish control. In this way, we develop more confidence in the companies that are reviewed. Even a traditional agreement is an example of how we relinquish control, by signing a contract and letting a copy of it stay with another party. It becomes easier for the other party to prove what has been agreed upon in the contract, and trust increases.

**Digital information can be manipulated**

In the digital world, we have trouble proving a course of events. If an individual actor has full control over data, that data can be manipulated. For this reason, we usually do not accept signatures that have been signed with digital letters. Anyone who has a digital contract can manipulate its contents, e.g., by switching out the names or other terms, amounts, dates, or similar. In other words, the principle of public access to official records is not enough for creating trust in digital documents and processes. However, modern encryption technology, where blockchain is an example, has different solutions that enable us to achieve this trust.

In practice, we need to supplement and regulate the transparency. We do not want all to make all actions and events in our surroundings transparent for everyone and we want to ensure authenticity. This means that if we receive a public document or contract that is digital, we need to be able to verify that it is genuine. If, for example, a protocol from a meeting about an authority is possible to manipulate, transparency around that protocol after the fact does not generate the same confidence. On the other hand, we can ensure authenticity and additionally easily gain access to the protocol, creating trust and the opportunity to demand responsibility.

**PAGE 14**

**Trust from honor, control or dissemination**

In her excellent award-winning dissertation and book, *The Force of Words: Political Oaths in Sweden 1520-1718*, author Sari Nauman describes how oaths are used to create trust between regents and subjects. Nauman describes how much weight was given to oaths, their oral pronouncement, the context, and witnesses to the oaths. The situation resembles those described in the Game of Thrones. An oath is not something people take lightly. People who break their oaths have lost the trust of others and it is very serious. Nauman also describes how

poorer trust and the regent’s absence due to war, among other things, contributed to the increasing importance of written documents that the regents had signed. Control replaced trust. While honor was crucial for trust in the 16th century, society has, ever since, increasingly relied upon written documentation rather than people’s oath, honor, and good will. Even today, witnesses must be present in courtrooms and often testify under oath, but the importance of written documents and their formulations have undoubtedly increased in recent centuries.

There is an ongoing discussion about false news, source criticism, etc., that can be attributed to digitalization. The term “post truth” was named the International Word of the Year by Oxford Dictionary in 2016. Data is spreading at a rapid pace today and verifying both the content and the sender is often difficult, not least because information is spread over larger geographical areas. In the digital world, dissemination and awareness have become more important for trust. This has, however taken place at the expense of control and authenticity. We therefore see a greatly increased need to ensure just that.

**PAGE 15**

Blockchain technology is based on encryption technology and comprises the possibility to ensure just that. Blockchain technology can, for example, answer questions like, “What is authentic, and according to whom?” Today’s increasingly powerful AI technology and genetic engineering have brought ethical questions much more to the forefront about AI, for example. Perhaps this means that in the future we need to work more with questions of honor, ethics and morality. It is not straightforward, however. Perhaps society is already moving in a direction where people will attach greater importance to the sender’s character and opinions than the authenticity of the message.

*(ILLUSTRATION TEXT):*

Honor + Control + Dissemination + Trust

Overall, transparency, authenticity and dissemination seem to contribute to increased trust. Trust reduces transaction costs. According to some researchers, modern economies consist of almost 70 percent transaction costs.1 In other words, the potential societal benefit of increasing trust among actors, processes, data, and more is very large. Blockchain can strengthen confidence primarily by contributing to control and authenticity, something which the digital world has problems with today.

**PAGE 16**

**Dematerialisation of value**

In his book, *Reframing Business: When the Map Changes the Landscape,* Richard Normann, a well-known Swedish management researcher and author says that some of the most important carriers of societal values and companies are on their way to becoming dematerialized. Some examples of that which is increasingly valuable today are symbols, brands, algorithms, information, data, knowledge, and relationships. All of these things are weightless. Two major consequences of this development are, according to Normann, componentization and mobility. Componentization means, for example, that the price can be separated from a product, something that has paved the way for new price comparison services. A brand can be separated from a product. A known car brand can therefore sell licenses to use its brand to other products in different geographical areas. This was not possible in a world where the car's value was merely the product and not the brand, which was the case when the car could not be driven in several parts of the world simultaneously. When software is the most important part of the engine, temporary upgrades can be sold remotely, which is much easier than taking the car to a workshop and changing the physical components of the engine—not to mention replacing the entire engine.

**PAGE 17**

**Deconstruction of data**

Blockchain and modern cryptography have made dematerialization even more sophisticated, and society has begun to grow aware of the value inherent in the deconstruction of data itself.

A clear example of this is the separation of identity from identification. In the analogue world, a person making a statement or signing a contract must be physically present in a particular place. When the telegraph came, we could communicate over a distance, but we couldn't be sure of

who was on the other side. Nowadays, with cryptography, it’s possible for an individual to identify themselves without being present. An achievement that is extremely valuable and something that is becoming increasingly common on the internet.

**PAGE 18-19**

As a technology, blockchain has proven its value in the deconstruction of data, but also in the division of different parts of the deconstructed data.

Instead of sharing all of the data, we can share when the data was created. For example, it can be practical to be able to prove what time the data was created, and it is valuable to be able to do so without needing to share all the data with a central database.

Distinguishing identity from identification is just one example. We can now deconstruct data in a number of different ways:

* When was the data created? Example: A picture of a car accident that is sent to an insurance company, a patent application or a personnel register at a restaurant.
* Is the data manipulated? Example: Accounting with a company, or an employment contract.
* Who has validated the data? Example: Was the task validated by a certifier, a trusted data center, or is it possible to validate by some third party?
* Is the data verified by an authorized organization or individual? Example: Without knowing who it is, only the authorized person or someone who is qualified to submit the information.
* When will it be possible to access the data? Example: To prevent information, such as a test answer or money, from being shown or spent too early.
* Has anyone looked at the data? Example: To know if someone has looked at a patient record or secret information in a company vault.
* Is there version management, a unique record of any changes to this document/task? Example: The latest version of the law, a current information on F-tax bill, space for ROT and RUT deductions.

• Is the data unique? Example: To make ensure there are no copies of financial assets or a package of drugs.

**Share the parts**

With blockchain, the value of sharing data with others has become clear, especially sharing only a few selected parts of the deconstructed data. If two parties sign a contract, both of them benefit from storing the evidence of the contract with an outsider. This can now be done without sharing the actual contract, but rather just showing proof of it.

**An incorrect illustration of central databases and blockchains**

(ILLUSTRATION TEXT):

**All information is shared**

Database/node

Database/node

Database/node

Database/node

Database/node

**All information is gathered centrally**

Central Database

**PAGE 20**

Today, many people think that we can either share complete information or no information at all. It is a rough and very unfortunate simplification. Not only is blockchain the only solution for sharing data in a smart way, it has clarified the technical possibilities and value of sharing selected parts of data. We can, for example, with help of technology, share evidence (a digital fingerprint) of a contract as well as the time, place of its conclusion, etc., but not the contract itself. Trust and data security can, in this way, be achieved simultaneously.

**PAGE 21**

[Image only]

**PAGE 22-24**

**Method and choice of solutions**

The method for the work was based on seven workshops in the project team, and a number of smaller meetings for in-depth discussion and interviews, etc.

During the work, 19 potential problems and opportunities were initially identified, which were grouped into five areas. These were:

• Identities and properties  
• Digital transactions and data events

• Accounting and auditing  
• Tax liability   
• Standards and comparison for reporting

Within these five areas, five possible sub-areas were then selected which were deemed as valuable, and also presented a reasonable potential as areas where good solutions could be worked out.

1. Digital receipts

2. Personnel register   
3. SINK, special income tax

4. Proxies   
5. Company information services

For three of the above, solutions are already considered to be sufficient enough today to be able to build technical pilots and proceed with investigating legal issues, etc. in more detail. For the other two, a little more analysis and brainwork is still required.

Developing in parallel with investigative work in order to speed up development processes has become more common in business, especially within digital development. Terms like "design thinking,” work with prototypes, and beta tests are examples of this.

**Social benefits**

The starting point of this project was to identify solutions we believe can generate great social benefits. The benefit is assessed according to three criteria: the value created, the cost of achieving the value, and the time required to realize the value. Several of the actors involved in the project are rather risk averse. The cost of a wrong step made by authorities, banks, and auditors can be large. At the same time, it is important to emphasize that a project that generates five billion SEK in social benefits per year is valuable to implement. One year's delay implicates a loss, or loss of profit, of five billion for society.

**Technology, law, and process**

The project focuses on learning and innovation. Detailed knowledge of law, processes, and technology has not been in focus. In the very general proposals for technology, adaptation to laws and regulations, as well as current and future processes, we have taken social benefits into account. If a law change is required, we are aware that it takes time and delays the solution. What is presented is a qualified guess of what we should do to achieve the value we want to achieve within a reasonable time. In some cases, technical solutions can also be built that can be applied already before new legislation is in place.

We cannot know with certainty in advance what the final interpretation of laws and regulations will be. As information, we can mention that we have at least identified issues such as the principle of public access to official records, eIDAS, GDPR (anonymization, pseudonymization, factual basis, the right to be forgotten etc.), issuance of receipts, originals of receipts, the Accounting Act, transfers of proxies for declaration agents, etc.

To understand the solutions, it is of course valuable with a certain knowledge of law, processes, and technology. When it comes to technology, a review of the most important concepts is provided at the end of the report. If you as a reader are familiar with what a hash, a merkle tree, and a Certificate Authority (CA) is, you probably don’t need to read that part.

**Description of the solutions**

The descriptions of the solutions follow a similar structure. Initially, we describe today's situation and what we want to improve. Subsequently, we describe, in general terms, a process that we’ve deemed suitable as a starting point. Finally, there is a description of thoughts and suggestions regarding governance and law, ID, as well as the storage of data. We judge these three areas as particularly urgent to sort out since they are difficult, not least because they are areas where many blockchain projects tend to fail.

**PAGE 25**

[Image only]

**PAGE 26-28**

**Digital receipt management**

**What value and benefits can be created?**

With ongoing digitization, digital receipts have become highly requested. Cash register legislation makes it possible for the cash register to produce an electronic receipt. In order to still handle digital data, companies have taken a photo of the paper receipt and used the digital copy of the receipt in their accounting. In these cases, the company still has to save the original receipt for a period of time. Registering and saving paper receipts requires great resources and makes modern workplaces difficult, as many work partly or wholly at a distance or, for other reasons, take trips and have expenses from hotels, trains, taxis, restaurants, etc.

The reason why digital receipts that are a copy of a physical receipt are not accepted without qualification is essentially that they can ease fraud and make tax inspections more difficult. Furthermore, digital receipts can be copied and one and the same receipt can be used for deductions and, for example, reclaiming VAT within several different companies. It is also easier to change a digital receipt if the receipt is allowed to be in any format. For example, it is easier to, without detection, add an extra zero in a Word file than to a paper receipt.

Today, there are legal requirements for both digital and physical receipts. These regulate, among other things, manufacturer-certified cash registers and the functions that a cash register should have. Cash register legislation allows the manufacturer-declared cash register to produce a digital receipt. However, the current legislation requires that an employee who wishes to deduct expenses for outlays and a company that wishes to deduct expenses and VAT must save the original receipt in the bookkeeping, i.e., in the original file format for digital files and in paper format for paper receipts, which has made practical management complicated. Unfortunately, the introduction of digital receipts, for that reason, has drawn out the time involved in trade and among companies. However, there are companies that have begun issuing digital receipts.

The discussion on digital receipts has touched on a number of different areas, such as "black boxes" for cash registers, automatic posting in bookkeeping, real-time time reporting, etc. Ultimately, the solution proposed in this report has the potential to facilitate most of these issues. For this to be possible, the starting point is that receipts are not only digital, but also independent of format, i.e., if it is a PDF or similar format. That is to say that it is the digital information that is central, not the format.

The solution consists of secure receipt management and is based on two important insights.

1. A receipt in itself has a very limited value. There is no greater harm created if someone steals a digital receipt. For example, it is often possible already today to get a copy of old receipts from the point of sale.
2. The Swedish Tax Agency (Skatteverket) and other stakeholders are primarily interested in whether a receipt has already been expensed, and thus has previously affected the accounts in the same or another company. Even companies would like to know if a receipt has already been used for compensation of an employee on a travel account, or by another company.

The greatest benefit of a digital receipt is probably the reduction of administration and work for companies and their employees involved in reporting and the transferring of paper receipts to digital form at the same time as the paper receipt is to be archived. Since a completely digital solution also enables automatic posting in bookkeeping to a greater extent, a considerable amount of work input can be saved.

Fully digital management of receipts, which also enables automatic posting, is expected to generate a value of more than ten billion SEK per year in Sweden. The solution described can be central to achieving this. If the solution is also used for invoices and counteracts VAT fraud, for example, the potential is even greater. The possibility to collaborate with other countries can also increase and contribute to a reduction of international VAT fraud. In the EU alone, VAT fraud is estimated to amount to more than 300 billion SEK per year.

**A software/service and architecture for digital receipt management**

The solution is intended to handle the following situations:

• Enable digital storage of digital receipts.

* Reduce the risk of mistakes and fraud with manipulated receipts and receipts that are expensed several times.
* Facilitate digital transactions and event data and enable real-time reporting and automatic posting in the accounts.
* The process can be extended to also include invoices, and thereby reduce risks of VAT fraud, not least with a future international solution.

**PAGE 29**

**Overall** **architecture**

**DIGITAL RECEIPT REGISTRATION**

*(Illustration text, left side):*

Simple "CA" for receipt issuers and expensing companies

Business system

Registration application that checks in receipts

Cash terminal

Check out system

Selling company

Receipt

*(Illustration text, right side):*

Receipt hash register matches issuance against cost entry

Employee

Business system

Registration application that checks out receipts

**Process**

In accordance with that which is stated in the delimitation, the views described in this report do not reflect something a person or organization takes responsibility for. Both ID handling (CA) and the receipt register in this solution may lie with the Tax Agency or another authority. In this specific case, the Swedish Tax Agency has been particularly keen to emphasize that it is not a position held by the authority, that information should be collected.

**PAGE 30-32**

**Step 1: Transaction**

The seller receives a payment and issues a receipt. The format of the receipt can be optional. The goal is, of course, that all receipts should be completely digital, but in order to enable the system to be implemented faster, existing solutions must be legally valid during the transition period.

**Step 2: Registration of the receipt in the issuer’s cash register system**

The selling company retrieves data on the issued receipt's content from the cashier terminal/computer. The content consists of two parts: A unique ID that is linked to each receipt, and information about the transaction, i.e., date, time, amount, VAT, items purchased.

**Step 3: Registration of receipt hash at the receipt hash registry**

The information obtained from the receipt described above is encrypted as a hash. A public key, or similar code, is also added to the hash which the company has registered with a party similar to a certificate authority, CA, i.e., someone who links the code and the company. Since receipts have a low value, the management of these keys can maintain a suitable and cost-effective lower level and companies that want to register receipts can use large amounts of keys if they wish. The receipt hash register now has a hash of one receipt and a code that another database (CA for receipts) can attach to a company (i.e., the company that registered the receipt). Note that the original information itself does not exist in the receipt hash register.

**Step 4: Expense receipt registration**

The employee who has had an expense, e.g., a train journey, registers the digital receipt and submits it to their employer. The employer, or the employee, records the information in the business system. Since no physical receipt is needed, the receipt can be saved digitally. Registration and posting can also more easily be carried automatically by a system or someone in an accounting department or accounting firm. Automatic posting is easier if the receipt is issued in a digital, machine-readable format.

**Step 5: Registration of a receipt that is expensed by the receipt registrar**

The information obtained from the receipt described above is encrypted as a hash. Since the receipt content is the same as the one registered by the cash register’s owner, the hash will be the same. A public key or code is also added to the hash, which is linked to the expensing company in a corresponding manner.

**Step 6: The receipt registrar matches the issuer’s hash with the expensing company’s hash**The receipt registrar now has a hash of a receipt and a public key for the issuing company. This hash can then be marked as "used" when an expensing company registers the same hash. The receipt registrar does not know anything about the content but can validate that the same receipt that has been released and expensed.

**Governance, law, etc.**

**Governance**

It is central to the architecture that a common registry is created for the registration of the encrypted receipt verifications. If the common register collects complete data, i.e., the receipts themselves in their entirety, the database becomes, altogether, an extremely large and significant safety risk. Today, there are a number of countries, even in Europe, that are moving in this direction, i.e., to create complete databases with sales and delivery data. In the proposed solution, however, it is possible to abandon data without the ability to recreate it, since it is encrypted as a hash.

In order for the registrations not to be completely unidentifiable, unique dispatchers are also needed. There is therefore a need for a system that can register the users and link them to the respective companies. This will therefore require private and public keys, or company-specific codes (or any other digital identification system.) The companies can choose to have many keys and extra transactions can also be sent in to hide the amount of receipts that are registered. The Swedish Tax Agency should have access to the common register since unknown registries cannot exist. It is possible to store these in a blockchain, but it is probably easiest if the Swedish Tax Agency is the owner of the registry or, in any case, has law-controlled access to the register in a fixed format.

Integration with the public registry is preferably done machine-to-machine, with an API that the respective business system suppliers integrate.

**ID**

It advantageous if ID management is handled separately, as it otherwise makes it difficult to analyze the database and any data connections. In other words, ID management can be managed by other actors. There are a number of different ways to further conceal information, but one must be aware that this is considerably safer, with less complete and less valuable sales data than what many other countries, including Sweden, Norway, and the EU are about to build elsewhere.

**PAGE 33**

**Storage**

Storage of receipts, i.e., the original information, takes place in the respective business system or storage connected to them, such as the cash register system. In this case, the requirement to store receipts in their original format needs to be interpreted as or changed to be based on the receipt’s content rather than format. As long as the content is recorded in the common register, the receipt registrar, it is considered to be an original. Whether this is consistent with current legislation is unclear. If new legislation is required, however, it will not be needed for existing management. What would be required is the enabling of this procedure in order to fulfill the requirement of original storage.

GDPR is not considered a barrier to this solution. It is not certain whether this system requires blockchain technology in the form of merkle trees or consensus algorithms. If a need arises for time stamping, for example, i.e., establishing a time schedule for the registrations, it will continue to be possible to delete old data.

**PAGE 34**

**Personnel Register**

**What value and benefits can be created?**

A legal requirement for personnel registers has been introduced in a number of industries in Sweden. The purpose has been to reduce the incidence of illegal labor.

A personnel register can be kept manually (in book form). It should then be bound, and the pages should be pre-numbered. This means that you cannot use loose paper or, for example, a spiral notebook. The Swedish Tax Agency has developed a manual personnel register that can be used, but a personnel register can also be kept electronically. The requirements for what should be recorded in the electronic personnel register are the same as they are for the manual version. In the program, all events must be logged so that it is clear who has made a change and when. The system must also be designed in such a way that the Swedish Tax Agency can review the data back in time. Within the construction industry, there exists a more advanced ID management system which the industry has developed (ID06). In this case, we have limited ourselves to looking at the restaurant industry, but the application is general for industries lacking ID verification.

The value of the solution is considered to consist primarily of reduced illegal labor and simpler handling for the companies who must fulfill requirements for a personnel register.

**PAGE 35-36**

**A software/service and architecture for personnel registers**

The solution is intended to handle the following situations:

* The process is primarily intended to create a routine for registering digital verifications of personnel registers, regardless of format.
* This means that, in principle, it becomes impossible to alter the content of the personnel registry while, at the same time, all the data in the personnel registers remains anonymous, i.e., impossible to decrypt.

* Yet another advantage is that it can become easier to verify the history of a personnel register during a tax inspection.
* A notification of a failure to register can also be sent to companies already the same day if desirable, which reduces the risk of forgetting registration.

The value of the solution is based on the assumption that any cheating with illegal labor can be reduced and it can become easier to distinguish between situations where incorrect reporting has occurred based on pure mistakes, rather than deliberate cheating.

**Process**

**Step 1: Establishment of personal register**

Every day, the personnel register is filled in the same way. Of course, it is an advantage if the personnel register is digital, but it is possible to have a regular notebook, i.e., any format can still be accepted according to existing legal requirements.

**Step 2: Registration of a verification**

From the restaurant's business system, time reporting system, or similar solution where the personnel register is retrieved, the names of those who have worked and when is published. It is also possible to solve this in cases where the personnel register is analog. In this case, an app is used in a phone. With it, a photo is taken of the personnel register every day. A verification, i.e., a hash, of the file/photo is registered together with a code that identifies the person who registered the verification. The registration is made in a predetermined blockchain, or merkle tree.

**Step 3: Notifications**

If no registration occurs, a notification will be sent to the company, e.g., a restaurant, stating that the personnel register needs to be registered.

**Step 4: Tax inspection**

If the Tax Agency is to complete a tax inspection, the mobile or software that has registered the verifications can be easily checked. The personnel register that has a verification in the blockchain is the one that is compared with the personnel working at the restaurant. It is impossible to manipulate the personnel register since then it would not be in agreement with the verification. It is also easy to check, for example, last month's registrations. For example, it is easier to assess whether a missed registration is due to an accident at work or if it is systematic. Tax inspections can possibly be directed to those companies/restaurants that have not made registrations, but this presupposes that the blockchain with the personnel register verifications (the hashes) is available in some form.

**Governance, law, etc.**

**Governance**

The central part of this solution is that taxation of the personnel is secured in the digital information chains of the taxpayers themselves but, at the same time, that the risk of data being manipulated decreases further.

**PAGE 37**

One requirement is that those who keep the registers have procedures in place to ensure which restaurants they hold verifications for. That is to say that it is sufficient that there is no risk for several different registers for the same restaurant. The ownership of the solutions can therefore be completely private. The restaurants do not need to share the personnel registers with the registry holders either, but only encrypted verifications.

**ID**

It is possible for restaurants to make several registrations of verifications on the same day. For example, if someone gets sick and a replacement is brought in. However, at least one registration per working day must occur. In order to ensure that only one registration per company occurs, an ID is needed, which is linked to that specific company. This ID can be agreed upon with the company collecting the registrations, e.g., a public key can be sent from the application while the private key is retained. If someone steals a key, it is easy to make a new one.

**Storage**

The original files must be stored digitally, but only need to be stored locally. The personnel register can be kept on paper, but the photo taken of the register needs to be digital. This photo is also what needs to be saved. In this case, a review of the conservation rules of the personnel register may have to take place.

**PAGE 38**

**SINK/Real-time**

It has been discussed in various contexts that, over time, accounting, internal and external accounting, tax payments, and more will take place closer to the moment of the transaction. Ideally, this can be done in real time.

The benefits of this are many:

1. It facilitates on behalf of businesses, which benefit from a better decision-making basis and a higher degree of control,
2. it makes accounting and auditing more relevant,
3. it eliminates the need for preliminary tax payments
4. it ensures tax payments already at the time when tax liability arises.

Relatively complicated legal rules can be handled quickly in digital automated chains.

At the same time, looking at the current situation, the distance from real-time tax reporting is large. Today, tax is generally reported monthly, every three months, or even on an annual basis.

Digitization is, in itself, a good basis for being able to report in real time. Expanded opportunities for automation and machine-to-machine communication, as well as expanded opportunities for intelligent systems for automatic risk management, remove the manual tasks that previously needed to be carried out in order to, for example, compile and manage different types of tax accounting, payments, etc.

**PAGE 39**

[Image only]

**PAGE 40-41**

**The situation today**

* Routines among companies today vary in quality. The work is slow and often involves manual handling, which means both uncertainty and risks. The work can therefore give a skewed picture of the company's position and the information often lags behind reality.
* There are different truths at different times. Both the annual report and other reporting currently have an obvious weakness in the fact that they are drawn up well after the financial year has ended. In a world where real-time is in high demanded, the annual report loses its relevance. When the time period between the end of the year and the publication of the annual report is long, it becomes unclear what is being audited. What did the company look like at the designated moment, and is that picture still relevant?
* Today, accounting takes place afterwards, which impairs control and the direction of operations. Many other services are suffering when the published accounting lies far behind the actual events in time. Credit assessments, assessments of the company's solvency, etc., become worse.

**Alternative approaches**

In order to achieve real-time reporting and real-time taxation, we can work with different approaches:

* Facilitate the digitization of cash handling, invoicing, reporting to authorities, risk management, accounting, and auditing. By promoting digitalization, better opportunities are created for making real-time reporting a reality.
* Introduce a final tax fixation closer to the moment of the transaction in several taxation areas. The tax already works in several areas to directly determine the moment of the transaction, such as, for example, VAT, excise duties, employer contributions (in connection with salary payments), and SINK.
* “Split-payments” mean that tax payments are made directly to the Tax Agency, at the same time as payment is made to the person who shall be paid, e.g., a supplier or an employee.
* The companies that have good control over their business develop better and have lower risks. Those that can demonstrate better processes should be able to gain benefits in their business and receive loans, insurance, better payment terms, etc., more easily. Real-time accounting can therefore be run naturally, both by companies, their customers, and suppliers.
* The ambition is that through automation, digitized information chains, and real-time accounting and payments (e.g., through so-called split-payments), relatively complicated legal rules and complicated operation rules and risk management models for taxation can be managed quickly and safely in digital chains. It assumes that data and processes cannot be freely manipulated. This can enable a situation, which was previously sought to be achieved through regulatory simplification, without opening up the risks and economic distortions that simplifications of the legal rules can open up. Managing companies’ taxation situations can be easier and more predictable.
* For the state, risks surrounding tax payments that occur later than the transaction date are reduced.

**Real time–a first step with SINK (Special Income Tax)**

A first step towards achieving real-time reporting is to focus on tax situations where the tax is fixated at the moment of the transaction.

**PAGE 42-44**

It would also be interesting to find a user case that does not become too extensive in a first step, but which, at the same time, offers substantial potential for economic gain for both individuals and authorities.

SINK, Special Income Tax on non-residents, is a suitable area for several reasons. Special income tax is paid by people who are normally liable to tax in another country, but who, for example, work temporarily in Sweden for an amount of time sufficient enough for tax liability to arise. SINK is also paid for by Swedish pension recipients living broad, for example.

It is, in other words, a tax that does not apply to a very portion of the population. Another reason is that the tax is final at the time of the transaction, even if it is a tax on income. SINK is paid as a flat percentage, of 25% on gross salary, without basic deduction or progressivity. Ordinary taxation of work (income from service) is taxed afterwards, the person can declare and then the tax deductions that the employer has made are matched against the final tax, and tax that is to be paid or reimbursed can occur. There are basic deductions, other possible deductions, austerity tax on higher income, etc. However, SINK is ready at the moment of payment. That which remains after the salary has been paid minus the deduction for SINK is the accounting and payment of the tax to the Tax Agency from the employer.

In other words, even though it is a tax on work, there are no deductions, no equations or adjustments of the tax after the end of the year. The income in Sweden is, however, often a tax basis for the tax authority in the employee's home country, where it is an income that’s usually included in their ordinary employee income taxation. The tax paid in the home country can, depending on local legislation, be adjusted with respect to the SINK that is paid in Sweden (one can deduct Swedish tax paid on the estimated foreign tax, or that particular income may be exempted from providing basis for tax).

A number of issues have been addressed through joint discussions within the group:

* Can business systems (payroll systems) handle payment orders/accounting?
* Yes—there are already systems developed for SINK that handle rules about time, etc.
* SKV can help distribute sample rules via API.

• Can accounting information that corresponds to the employer declaration at the personal level be submitted with a payment?

* Yes - there is currently a limited amount of characters that can accompany a payment (ex: SWISH).
* However, the international system for payments has been improved and it will soon be possible to add an XML file to the payment “payload”—the entire report can be submitted with the payment.
* Can the accounting information be made available digitally/automated/securely?
  + Yes—through, for example, solutions with the register for the international exchange between tax authorities.

**What value can be created?**

* When tax liability arises, it is good if the tax is paid as soon as it can be finalized. Since tax is a prioritized requirement, and board members are jointly responsible, it is an advantage for many parties if large tax debts are not accumulated in companies.
* We primarily view SINK as a first step towards reporting and paying taxes closer to the time of the transaction. In the long run, such management can contribute to:
* Easier access to updated data on companies, and the organizations’ position can improve the basis for decision-making and existing services, as well as enable new ones. This, in turn, will ease working capital management, liquidity management, borrowing and insurance, etc.
* Sharing of data with different stakeholders is easier when it is updated and secure.
* Accounting that can be retrieved from the system as needed, or at least takes place closer in time to the interim financial statements and annual report, is necessary in order for these to maintain their relevance.
* In the long run, there may be more relevant ways of reporting, for example, on an as-needed basis instead of at certain time intervals, which are governed by predetermined rules.

**PAGE 45**

**Process**

(Illustration text):

A new process around SINK with split-payment and distributed information on paid tax (without registration)

Phase

The tax authority in the home country

Workers residing abroad

Employer

Business system company

Bank

Tax Agency

Operational logic (rules) delivery via API

25% of the salary is reported and paid to the Tax Agency

Payment order TAX

Payment order SALARY

Data as XML in Payload

Blockchain/DLT regarding paid SINK

Operational logic for SINK is running

The business system divides the salary into two payment orders

The employer pays in a split-payment function. The transaction is noted publicly (person and tax)

75% of the salary is paid to the employee

The employee is taxed correctly in their home country

The foreign SKM records the data and taxes the employee, including the correct deductions for paid SINK

**PAGE 46-47**

**Step 1**

Payroll systems or other business systems incorporate applicable rules for managing SINK from the Swedish Tax Agency's API.

**Step 2**

The employer pays wages in a split-payment function. The business system goes through its own and the Swedish Tax Agency's regulations, states that the salary must be taxed according to SINK legislation and divides the salary into two payment orders. Information about the taxation statement is added to the payment in the form of an XML file.2

**Step 3**

The payment order for salary goes to the bank and is executed. The payment order for SINK tax goes to the bank together with the related information. The bank executes the payment order on behalf of the Tax Agency and forwards the related information. The information is supplied to a secure register (blockchain/DLT) by the Swedish Tax Agency. The tax is now fixed and paid.

**Step 4**

The register is made available to foreign tax authorities and the taxable person. The foreign authority adds the information to the employee's income taxation. The employee can check to see whether the information is correct, already in the register.

**Governance**

The Swedish Tax Agency and advisors potentially have a key role in developing accepted solutions for updated interpretations of machine-to-machine regulations, for example, via APIs. Question marks may therefore arise regarding interpretations of tax amounts, tax liability, and more.

*1 The information attached to the payment replaces the registration information for SINK decisions and employer declarations at the individual level. The information thus entirely fulfills the person and employer's accountability towards the Tax Agency. Nothing further is required.*

**ID management**

ID management today involves, among other things, creating a coordination number (corresponding to a Swedish personal identification number for non-residents whose Swedish residency is not to be registered) for the employee. The process for creating coordination numbers lies with the Tax Agency. However, the process today is taking too long since it is manual. It is therefore necessary to create conditions for the automation of this process within the Tax Agency.

A system for creating a code that can decrypt a SINK decision is sent to the individual. However, they do not have to be linked to the code, but rather the code is a decryption key. The decryption key can be given to the tax authority in the home country for the employee to receive correct information about the Swedish income and the tax in the oppression of their income declaration.

**Storage and accessibility through automatic international information exchange in real time**

A possible desirable ambition is that the Swedish Tax Agency's interaction with foreign tax authorities can focus on each authority retrieving data as needed. At present, it is the tax authority that has the information that sends large amounts of data to other tax authorities based on the data owner's assessment of what may be interesting for which foreign authorities. The exchange takes place on the basis of international agreements between the governments and EU directives. This development requires international collaboration.

If blockchain/DLT is set up:

1. The taxpayer themselves can retrieve their information from, and
2. The foreign tax authorities can simultaneously retrieve information from their taxpayers. Then we turn around the information exchange so that the actors retrieve what they need, instead of the Swedish Tax Agency sending the information that they think the parties need. The exchange of information between tax authorities can then take place in or next to real time (making it accessible).

**Share information between authorities**

Information about work permits for people coming from a non-EU country is available today at the Swedish Migration Agency. The Swedish Tax Agency needs to verify this information to be able to approve a worker for SINK. A system that makes it easier for Swedish authorities to retrieve information from other Swedish authorities would, therefore, be valuable for this solution.

**PAGE 49**

[image only]

**PAGE 50-51**

**Proxies**

**What value and benefits can be created?**

We believe that proxies can be managed in three different ways:

1. As a central service for proxies that are established or accredited by one or more authorities. An investigation of this was completed by several authorities under the direction of the Swedish Pensions Agency in 2012. It was deemed valuable but complicated to establish a national service.
2. As one or more applications or pieces of software that can be used by different organizations as desired. An authority, an interest organization can accredit these, but it is not necessary.
3. As a service for different individuals to gather information about proxies linked to them in the same way as "My messages.” A special function such as "My proxies” can be established. The "My proxies" service could be extended to include a more general service, "My documents,” for valuable documents. For such a service, it is advantageous if authorities establish, or at least approve or accredit, the service.

The greatest benefit can probably be found in streamlining and securing the work involved with proxies at banks, companies/organizations, and the companies' accounting consultants and auditors. Those who draw the greatest benefit will also be quickest to utilize a new solution, especially since they are professional users and therefore may be forced to introduce the processes by their employers. The work of developing a solution can also be initiated by a smaller group of companies, banks, auditors, and others, and the service may also be implemented without government decision. The starting point is therefore to begin with the needs of the banks and accounting consultants. In the end, it turns out that the solution for proxies very well may begin to be established with that starting point, but that it is relatively easy to also consider authority proxies, such as declaration agents, and proxies for citizens in general.

The value of the solution is deemed to be significant, especially since the solution can form the basis for several different types of proxies and authorizations. The solution can be used to manage any right, authority, proxy for any person, organization, device or entity. The solution can also be used in situations where the proxies or rights are signed on paper or other formats, for example where digital identification or signatures may not be used.

**A software/service and architecture for proxy management**

The solution is intended to handle the following situations:

1. The auditor requests a complete list of proxies to verify that purchases, agreements, etc. have been signed by authorized persons. This is the auditor's duty when auditing.
2. A person wants to prove that the person in question has power of attorney and that the power of attorney is valid but, also that the person may represent/act as their agent in a given situation.
3. An accounting consultant, company, or the bank wants to get an overview of which valid proxies exist, who the proxy holder is, and who the proxy giver is.
4. A proxy shall be terminated, for example, in order for a person to terminate their work as an accounting consultant for a company, or because a proxy is to be revoked.
5. An accounting consultant is going on holiday and needs to hand over their authority to represent the company to someone else.

**PAGE 52**

**Overall architecture**

PROXY SERVICE

*(illustration texts):*

Blockchain, Verifications

Application for closing, transferring, and checking validity

Tax Agency - Storage

Accountant - Storage

Business & Proxy Provider - Storage

Accounting agency & Proxy holder - Storage

Bank - Storage

Application for digital signing of authorizations with codes for rights

E-identification + signature

**Process**

The establishment of the proxies takes place in the usual way in the digital world, i.e., a digital file containing the contents of the proxy is signed with a digital ID and a digital signature is attached to the proxy. The proxy is now valid. The idea here is that the validity is simultaneously controlled by an external register in the blockchain. The proxy is valid if, and only if, the necessary status of the authority is registered in the blockchain. This is formulated in the proxy, i.e., which public keys have the right to terminate the proxy, as well as to which public keys the proxy may be transferred (if any).

**PAGE 53-56**

**Step 1**

The proxy is established digitally, which includes the period of validity, who the proxy holder is, who the proxy giver is, the extent of the proxy, i.e., what it can be used for. Both the proxy giver and the proxy holder fill in their own public key which gives permission to terminate the proxy. Several public keys may be registered, since there may be interest in giving more people and organizations the right to terminate and/or transfer the proxies.

**Step 2**

The proxy is signed digitally with an approved eID, e.g., mobile bank ID or Freja eID, and an approved signature, e.g., from CGI is tied to the proxy.

**Step 3**

The proxy is registered in the blockchain for proxies, but only as a hash, i.e., a digital fingerprint for the proxy. Alongside the hash are public keys that have the right to terminate the proxy, which should at least be present with the proxy giver and the proxy holder. The process is now complete and the proxy can be used.

**User case:  
1. The auditor requests a complete list of proxies to verify that purchases, agreements, etc. have been signed by authorized persons. This is the auditor's duty when auditing.**

**Solution:**

The auditor requests a list of all proxies the company has and their digital fingerprints, hashes. The hashes for the proxies are checked against the blockchain via a simple API that only needs to check that the proxies have not been terminated. If they have been terminated in the blockchain, the auditor needs to check when it was done and that the proxies were only used when they were valid.

**2. A person wants to prove that the person in question has power of attorney and that the power of attorney is valid but, also that the person may represent/act as their agent in a given situation.**

**Solution:**

The representative shows the proxy - e.g., to the bank. The bank makes a strike in the blockchain via a simple API and can confirm that it exists and that it is still valid.

**3. An accounting consultant, company, or the bank wants to get an overview of which valid proxies exist, who the proxy holder is and who the proxy giver is.**

**Solution:**

One prerequisite is that the employees have prepared requests about proxies and their validity by submitting the public keys that the respective accounting consultant, bank employee, company employee, etc. have registered in proxy cases. Each organization can choose whether the private keys should also be stored centrally. On the organizational level, one can then check all valid and completed proxies that are registered.

**4. A proxy shall be terminated, for example, in order for a person to terminate their work as an accounting consultant for a company, or because a proxy shall be revoked.**

**Solution:**

Anyone wishing to terminate the proxy enters an interface that is connected to the blockchain and registers the private key that belongs to the public key, which is tied to the proxy in the blockchain. The person with the private key has the right to terminate the proxy, and it is therefore then registered as completed and can no longer be used. Note that this right to terminate the proxy can reside with several persons and organizations. For example, it may be possible to terminate a proxy for both an accounting consultant and their employer.

**5. An accounting consultant is going on holiday and needs to hand over their authority to represent the company to someone else.**

**Solution:**

There are a few different ways to solve this. Usually, an accounting consultant wants to be able to hand over a proxy during their vacation, for example, and then be able to become a proxy holder again after the holiday. A little different logic is required in this situation, since the private key cannot be published and then used again. Already with the proxy’s establishment it is probably necessary from a legal standpoint to assign the role as possible future proxy holder. In other words, it is determined which person can become proxy holder during the holidays already at the time of establishment. A public key, also given to this person, is then linked to the hash of the proxy in the blockchain. These people can then, in turn, transfer the proxy between them. It is possible to solve with encryption even without revealing the private key. A very important feature is that this makes it possible to ensure which person has the authority to represent the company at each occasion and that it is only one person at a time. Given that the proxy, already at the time of its establishment, has several proxy holders, it is not to be regarded as a traditional transfer of proxy. Proxies for declaration agents can then possibly be activated for another person, even though, according to law, a transfer is not currently permitted. This is because it is not a transfer but, rather, an activation of an inactive proxy. Of course, this cannot happen if it is regarded as a circumvention of legislation. The assessment is that the legislature intends to limit transfers of proxies to people who the proxy giver has not accepted or approved. In this case, the proxy giver has approved the proxy holder in advance, and even set the conditions.

**Governance, law, etc.**

**Governance**

The core of the architecture is that the authorizations themselves are separated from the blockchain. In the blockchain there is a merkle tree that saves validity information about the proxies. Since the information in the blockchain cannot be identified, neither the person who owns the private keys or the contents of the proxies are flexible governance issues.

It is conceivable that companies, banks, accounting consultants, ERP system providers, and others may provide this architecture as a service. The important thing in architecture is to ensure that data cannot be manipulated. There are still advantages to managing the database as a blockchain since it is the blockchain that creates redundancy and reduces the risk that any individual can acquire a monopoly with the database as a basis.

**PAGE 57**

**ID**

A very important part of the solution is to distinguish between the establishment and termination of a proxy. The establishment of a proxy requires very high security. We do not want proxies to be created by unauthorized persons. For this reason, secure identification and signatures are needed. For the private keys, security is not as crucial. The only use of the private keys is to terminate proxies. Therefore, no CA Certificate Authority is needed for the management of the public and private keys in the blockchain. Management of the proxies’ validity, i.e. activation and termination can, however, be handled with private keys that are generated locally. This management can be viewed by banks and accounting consultants as business-critical and be managed with high security. But for individual proxy givers, there is no danger if a public key linked to a proxy falls into the wrong hands. The proxy can be terminated, but it cannot be used in any other way than intended.

**Storage**

Storage of the proxies, i.e., the original information itself, can be done very flexibly. It is possible to store these in a cloud service, on a regular computer, or in a structure together with professional actors and many proxies.

The storage of the database itself, with verifications, should be a merkle tree and preferably a blockchain.

**PAGE 58-59**

**Company information**

The management of company information is interesting from several perspectives.   
•The companies are interested in reporting in a simple and standardized way - and preferably only one time. The once-only principle is an objective for authorities to make it easier for the companies. This principle has also become law or practice in several countries, such as Estonia and Norway.

• It can also be interesting for companies to be able to share information in an effective way with other actors besides authorities, e.g., to make it easier to get credits, be able to make purchases with good payment terms, etc.

• For many different actors, it is also interesting to take part in information about companies in a simple and standardized way, in order to feel safe with their counterparts, ensure compliance with legal requirements, compare data, and more.

• Data that has been reworked and sold can also advantageously be based on an infrastructure that is quality controlled and transparent. The area grows with demands from legislators, e.g., for Environmental, Social, and Governance reporting (ESG), various sustainability aspects, other types of certifications, etc. Also compare with "Integrated reporting,” a concept in accounting and auditing where soft factors, such as sustainability reporting, are increasing in importance.

In all of the above situations it is, of course, also important that the handling can be done with high quality data, high IT security, and with an appropriate degree of anonymity for both the data provider and data seeker.

The various applications discussed so far in the project are:

1. Standardized reporting of company data to authorities.

Standardization of reporting is an issue that the Swedish Companies Registration Office (Bolagsverket) is actively working on, among other things, through the Nordic Smart Government collaboration.

As far as standards for company information are concerned, blockchain technology and other encryption technology as such are not something that creates a greater advantage that we know of, and it is therefore reasonable to let the conclusions drawn from the collaboration within Nordic Smart Government become clearer in terms of what they want to achieve and how, before attempting that area proposed by this project group.

2. A coordination service for basic data available on companies

A coordination service for basic information about companies where there already exists a reporting obligation to authorities, and information that companies want to share is considered to be both valuable and a good start.

3. Holistic identification of organizations with different forms of data

The collection of broad information about companies can be seen as an overall solution for collecting and sharing different forms of data where legal requirements exist and where, for other reasons, it can be valuable. The estimate in this proposal is relatively extensive, with the previous point being a first step. One possible starting point is to place emphasis on establishing the structure and basic information, i.e., item 2.

4. A service for comparing companies within the same industry

This type of service can be based on public data and should be able to be created, but is probably dependent on other parts being in place so that data from, e.g., The Swedish Companies Registration Office, SCB, and the Swedish Tax Agency can be coordinated and, in some cases, may also be made anonymous. We believe that it is better to start with point 2 and thereby create the conditions for this at a later time.

5. A service for consolidating data from different companies, for example, before for the acquisition or merging of companies. Generally speaking, this leads to the same reasoning as in point 4.

**PAGE 60-61**

**What value can be created?**

Already today there are companies working to provide services of this nature. It is therefore important to consider what a similar service would supply.

1. One reason may be that the responsibility for ensuring that information is correct and updated is often a responsibility of the authorities and that the responsibility can become more unclear with an intermediary.

2. Another reason is that authorities have increased requirements on themselves to make data available. Concepts such as "open data,” "open source,” and "open science" are increasingly emphasized in reports and regulations, both in Sweden and the EU. It is therefore appropriate that information which already exists with the authorities be made available in a more open and accessible manner in the future.

3. An available infrastructure for different types of data enables new services. Banks are now required to set up APIs, according to PSD2, in order to facilitate third-party services using bank data. It is reasonable that public data be made available to facilitate third-party services, at least in a corresponding manner.

4. It is an advantage if the service is open for building services, where companies and other parties can also expand and add information about their own organizations, or for those who want to sell data.

5. With the introduction of GDPR, it may be advantageous if the infrastructure is owned, managed, or reviewed by one or more authorities. It can clarify the right to store the underlying data.

An encyclopedia for basic information in standard formats may include, for example:

* F-tax
* Information about how I want to be invoiced. Here, Finland's high proportion of digital invoices is interesting and perhaps Sweden can be inspired? Can access to digital billing information be made easier?
* Payment information
* Certifications, ESG, Certified Tax Payer, Authorized Economic Operator at Customs. To be able to check certification, verify that it is valid and has been issued by the relevant actor.
* Warehouse operator Yes / No
* Voluntary registration or compulsory registration of information that may support assessment of others may possibly be part of a service. For example, as a way to show payment times for supplier invoices.

**Overview of possible architecture**

BUSINESS SERVICES

*(illustration text):*

Company information

Company registration

Tax Office

Credit assessment

Certification

Blockchain

Files not needed?

Application for access and consent

ID - register and management - Log file?

User interface

Company consent giver

Company readers

Auditor

**PAGE 62**

**Solution proposal/next steps**

There is not a complete solution proposal for this service. It is possible to build an infrastructure similar to the description above and, overall, we believe that it is possible to create great social benefits with a service in this area. However, we have not identified a single service that, in itself, justifies large investments. It is probably not enough just to have a service for checking whether or not "the company has an F-tax.” Rather, we have different types of data with different conditions, and therefore may require different solutions.

Essentially, we see two parts that need to be deepened.

1. What type of data and data management is desirable?
2. What solutions already exist in other countries, and what works well and less well with these solutions?

**Examples of data questions**

Whose data should the system include? Is it solely government-owned data? Is there data owned by the one who the information concerns? Is there data that is collected and owned by companies about other companies? Should the system make data accessible completely free? Should accessibility be limited in any way? Should it cost something to access the information? Should those who retrieve data be registered in the system? Should the collection of data be limited to those who have special legal backing for retrieving data? Should the system regulate who gets access to the data, so that the one who the data is about must first approve its collection? Should there be data that cannot be supplied, even with consent?

If a solution is to handle all of these questions, it will have to be large and complex.

**PAGE 63-64**

If we are contented with individual services it becomes, instead, more important that the cost of the individual service can be justified by its great value. We then need to ensure that there are organizations and people who want to use the service and who see advantages relative to the current situation.

**Role models in other countries**

Over the course of this project, we have learned that services exist in other countries which can serve as inspiration.

**The UK**

Experiences from the UK tell us that the usage of certain types of data increases markedly by making them available. It can be an example of making data freely available in a simple way. We do not know if the system can also handle data that should be limited in accessibility. It may be an interesting example to investigate further.

**Norway**

Norway is another country with a system that seems to work better than those in Sweden, when it comes to the handling of business information. Among others, there is a service called Altinn. The service acts as a portal and becomes a natural interface for many different types of data. Historically, Norway has also been successful at sharing relevant information between authorities. This makes it easier for companies since they do not have to report the same data in different formats to many authorities, which is the case in Sweden.

We do not know if the Norwegian management involves consent for retrieving information or how the security risks that exist with a central system are handled today.

**Estonia**

In Estonia, there exists a system for obtaining data between authorities called X-road. The solution is an important part of Estonia’s IT infrastructure. The system entails that a central authority oversees the system, but at the same time cannot control what data is transferred between authorities in the system. It stands out as interesting from a security point of view. Finland has now joined the solution and Estonia and Finland have jointly formed NIIS, the Nordic Institute for Interoperability Solutions. They work to create a service that makes certain data collection require prior approval. Even today, however, there is a log function that makes it so that actors retrieving data without legal support can be punished. It is probably enough to handle data that requires consent in many cases, but in order for the system to be used widely by authorities in the cases in question, it was, however, necessary to introduce mandatory legislation.

Overall, there are more and more examples of solutions in other countries. The Swedish Companies Registration Office’s work in the Nordic region with Nordic Smart Government probably has even more knowledge about the current situation. More work is needed with the material before we in this project can recommend any individual solution to proceed with.

**PAGE 65**

[Image only]

**PAGE 66-68**

**Other support services**

In this project, four support services have been identified that serve as a prerequisite for many other services. Most natural is probably the fact that that the new authority for digital management, DIGG, will be responsible for these services in the future, at least as coordinator or purchaser. Since DIGG is a relatively new and small authority, it can be perceived as many and big things. On the other hand, it is the project's assessment that these services are among the few that are most central to digitalization and that responsibility cannot be divided with many different authorities. Moreover, DIGG already has a responsibility or governmental assignment for three of these services.

The four services that should exist are:

1. A framework for eID services, with corresponding signature services. - Work is already underway on this issue, and the e-Legislative Committee has now become part of DIGG. See further information in the section on technology.
2. A service for addresses/digital mail for organizations and citizens - The "my messages" service has been moved from the Tax Agency to DIGG. While the issue of an identification service for organizations has both advantages and disadvantages, there are clear advantages to having a service for sending messages to organizations like the analogue world. For example, a personnel register service can monitor if someone has failed to update their personnel register and a message can be sent to a digital "mailbox" like "My messages" in the case that it is relevant. In the example of digital receipts, it may be a way to be able to send out new codes for the organization to register their receipts with, for example, if the old ones are missing or lost.
3. A communication service for efficient collection and sharing of governmental information - In the work with SINK, the need for an easy way to exchange information between authorities has been identified. The Swedish Migration Agency (Migrationsverket) has information on work permits which the Swedish Tax Agency needs in order to be able to make decisions about SINK. In the case of a company service, the issue of sharing information between authorities, as well as companies and private individuals, is central. - Around this issue, there is a governmental assignment and project where the Swedish Tax Agency, the Swedish mapping, cadastral and land registration authority (Lantmäteriet), the Swedish Companies Registration Office, and others are included and coordinated by DIGG. Within this framework, we can look, for example, at the Estonian X-road. The issue of sharing governmental information has many legal aspects to take into account. In terms of technology, it is an interesting solution that Estonia uses, and we know it to be the most widely used and well-functioning infrastructure for sharing information. Finland has now joined the system and has set up a separate organization to develop and operate the technology, NIIS. The technology encompasses many of the properties that characterize blockchain technology, i.e., private and public keys, hashes, merkle trees, and an infrastructure for peer-to-peer communication. However, it is not a consensus algorithm where databases have synchronized information. Above all, the central organization keeps track of whether the identities are approved and can receive and send requests. It also keeps a log of requests. The central authority, on the other hand, does not collect the information and cannot read what is sent within the network.
4. A notary service for legal validation of digital information - In addition to the above services, where work is already in progress and the responsibility is delegated, the need for a digital notary service is great. Presently, there are uncertainties when it comes to digital evidence and their legal effect, archival stability, and the interpretation of storage opportunities according to GDPR. An authority service would fulfill a very valuable need of being able to register "combination hashes,” i.e., top hashes of other blockchains and services. In practice, this is a blockchain or a merkle tree where licensed operators can register evidence (usually hashes), and possibly in exchange for compensation. The government-controlled service can guarantee legal effect, archival stability, and the requirements demanded by GDPR. At present, there may be uncertainty, for example, about whether a piece of evidence, i.e., a hash of a digital agreement may be saved even though when the agreement is drawn it is clear that the contracting parties wish to have digital proof, at least for a specified time such as the duration of the agreement. In the case of proxies, it could be valuable to be able to refer to the fact that the verifications confirming the proxy’s validity and termination are stored or confirmed in a government-controlled notary service. - This can be likened to registration with periodicals and local newspapers adapted for the digital world and its possibilities. - There are similar services at Guardtime, for example, but for the reasons mentioned it makes it easier to know the specific conditions according to Swedish law. There may also be an interest in saving more information in the notary service and a willingness to pay to be able to do so. Virtually all actors working with blockchain technology, who are faced with the question of whether there’s a need for a similar service, understand the value of this. For Swedish authorities, such a service could become an important infrastructure in order to, in turn, create secure systems for version management, original documents, and more. Something which, among others, the Digitalization Legal Investigation(SOU 2018:25) and a number of authorities currently regard as challenging issues.

**PAGE 69-70**

**Technical explanations**

To understand the solutions described in this report, there are some technical concepts that are valuable to know about. These are briefly described below.

For more in-depth analysis of the technology, it is recommended to start with the concepts below, PKI, Certificate Authority, Merkle tree, Hash, etc., and then search on the internet. A well-written book on encryption is *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* by Simon Singh. In other words, it is a proposal and recommendation to start by understanding encryption and then, afterwards, move on to blockchain.

Somewhat more detailed descriptions of blockchain technology, and its applications in Swedish projects, can be found here.

https://chromaway.com/papers/Blockchain\_Landregistry\_Report\_2017. pdf

https://www.kairosfuture.com/se/publikationer/rapporter/blockchain-use- cases-for-food-tracking-and-control/

**Private and public keys**

Traditional encryption has been built on the idea that there is a document, e.g., a contract, that is encrypted with an encryption key. The result is an unidentifiable message. Anyone who, in one way or another, gets ahold of the encryption key, or breaks the code, can recreate the original message. This encryption technique is called symmetric encryption. Anyone with knowledge of the encryption key can decrypt the message.

Private and public keys are a common way to generate codes with further finesse. We can know that someone has an encryption key - without them showing it to us. The one who does the encrypting does not have the same encryption key as the one who decrypts. This technology is called asymmetric encryption and has revolutionized the use of digital technology, such as the internet. There are a great number of contexts in the digital world where we want to know who is acting on the other side of the network. Some form of electronic identification, eID, is needed, regardless of whether it is an internal network or the internet.

Private and public keys are a solution to that problem. The person who is to identify themselves has access to a private key, i.e., a code with numbers and letters. The private key includes a special public key. The public key can be distributed freely, for example, on the internet. If Astrid wants to identify herself, Bertil can be certain that it is Astrid who has written a message, signed a document, or similar. Bertil knows that since a message encrypted with the private key can be decrypted with the associated public key. In other words, Bertil can decrypt the message using the public key. If the decryption is successful, he knows that there must have been a person with access to Astrid's private key who has encrypted the message - otherwise it would not have been possible to decrypt using Astrid's public key. The technology also works in the other direction, i.e., Bertil can encrypt a message using Astrid's public key - and only Astrid can read it with the private key. Bertil, on the other hand, cannot decrypt his own message, even though he made the encryption using Astrid's private key.

Since it is easy to generate new private and public keys, we propose this technology for some of the solutions in this report.

**PAGE 71**

**Certificate Authority, CA**

However, one problem remains in the example above. How does Bertil know whether the public key he has access to really belongs to Astrid? Maybe another person, we can call him Edvin, put out a public key and claimed it was Astrids? To guarantee that the public key belongs to Astrid, there is a Certificate Authority, often called CA. Its task is to keep track of which public keys belong to what individual. Note that the CA does not need to be able to access Astrid's private key. The CA can, on the other hand, claim that another key is Astrid’s and thus fool Bertil. Therefore, if someone hacks the CA, it’s a major problem because they will be able to claim that everyone else has incorrect keys. The security associated with CA is therefore central. The infrastructure that includes private and public keys, CA, etc., is sometimes called a Public Key Infrastructure (PKI).

In Sweden, identification with Mobile Bank ID is the most common, and the company Financial ID technology is the CA for these eIDs. However, there are several credentials that can be used by private individuals to identify themselves, i.e., they have legal backing as e-identifications, such as e-Identification from Telia. Now there is even an authority approval that can be provided, in the form of receiving approval as a Swedish e-Identification, which Freja eID has become.

As of September 29, 2018, eIDAS, an EU legislation for e-legitimations and trusted services is binding for EU member states. This means that all e-Identifications that have been approved under eIDAS will have to be accepted in all EU countries as approved e-Identifications. In order for it to be practically possible to integrate tens, if not hundreds of approved ID solutions, eIDAS has required each country to set up some form of ID exchange. The newly established authority for digital administration, DIGG, has been assigned responsibility for the e-identification board and has also built this type of exchange service. The switching service includes two parts. One for outgoing eIDs, i.e., identification using a Swedish eID that is to be used in another country. The second service exists in order to obtain an eID approval from another country that’s using a Swedish service.

In practice, the work of setting up these exchange services is not at all ready to the extent that EU legislation really requires. However, a dozen member countries seem to be well on their way towards establishing the system.

In addition to the functions in which responsible authorities already exist, there is value to being able to secure more information about an individual’s roles and powers.

This area covers issues such as the permissions, authorities, agents, proxies, positional proxies, and KYC (Know Your Customer) of individuals. In this report, we have generated a proposal for a solution for proxies. There are several examples of ongoing work on these issues, in addition to eIDAS. A few examples are:

* The issue of permissions is usually handled by today’s IT systems for each respective organization.
* The issue of KYC is something that is particularly valuable for banks and credit institutions. There is an ongoing project between the Nordic banks, with blockchain technology as support for making it happen.
* Handling by agents is an issue that will now to be investigated in a joint government project.
* In March 2019, an investigation will be presented that will look into the issue of a new Swedish government-owned ID which is expected to replace the driving licenses. But, until further notice, it is not an eID.
* There is Nordic collaboration around ID, NOBID

**PAGE 73**

**Signatures and trusted services**

In addition to eID, eIDAS also regulates trusted services or digital signatures. Besides the identification of a person, there is sometimes a need for proof that a person has been identified, and has signed, and that the evidence can be tied to a document, in practice, a digital file. For this purpose, a signing service is needed.

**A hash—digital proof**

Perhaps the most important technical component in what is today called blockchain technology, is the ability to create unique verification codes of digital files, i.e., photos, transaction lists, registers, contracts, videos, patents, etc. Verifications can be created by anything that can be stored as a digital file. The verifications make it possible to confirm that digital files have not changed, a function that is extremely essential. It is important because there are no reliable ways to know whether a digital file has been changed without encryption technology being used, which the owner of the digital file does not control themselves.

With help from an advanced "fingerprint algorithm,” any digital file can receive a unique verification 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 describing a digital document and re-calculates them according to a defined, but unpredictable pattern. Regardless of what data set the original file has, the result is always smaller code which always has the same format, i.e., number of characters.

**PAGE 74**

The hash was invented already in the 1950s, but its use has only gained momentum in recent years. The most important feature of a hash is that it cannot be reversed. In the same way that it is not possible to recreate a human from the limited information contained in a fingerprint, it is not possible to restore a digital file from a hash. Unlike encryption technology, which has been the only of its kind known for several thousand years, it is not yet possible to understand what the original file looks like, even for those who know the encryption algorithm. Compared to symmetric and asymmetric encryption, there is no decryption at all for hashes. You cannot restore the original file.

The hash can consist of 64 characters, which is far too little information to understand what an accounting file with an annual report looks like. If the accounting file is comprised of several megabytes, it cannot be reproduced with a few digits and letters.

The number of hash combinations is, at the same time, a larger number than a one with 64 zeros (since it contains letters as well). The probability of two hashes coincidently being the same is therefore practically zero. This means that the one who has the original file can recreate the hash, i.e., the fingerprint, but no one else. At the same time, the owner of the file cannot make a change without it being noticed by someone who has the original hash.

This feature is completely critical for the solutions described in this report. The proxy giver and proxy holder can, for example, share a hash in regard to their proxy without disclosing the actual contents of the proxy. Given that the content of a digital receipt is sufficiently comprehensive, it is not possible to understand the contents of the receipt based on a hash that is in a receipt register. The ability to be anonymous is crucial in these cases.

**PAGE 75-76**

**Merkle tree**

Let us assume that a proxy holder and proxy giver want proof of the contents of the proxy and that it has not been manipulated. They can then let a third party store a hash of the proxy. The disadvantage of this, of course, is that this third party, or any of their employees, can manipulate the hash. To eliminate the problem, the hashes are put into a sequence where each hash that is to be added forms a part of a new hash. In the proxy example, we take the first hash, no. 1, of proxy number 1. When a new proxy hash comes, no. 2, these two hashes 1 and 2 are taken and made into a new file which makes a “combination hash,” hashes 1 + 2. When a third proxy comes, we add the "combination hash" together with the new proxy, no. 3, and create a new "combination hash" (1 + 2) + 3.

The result of this procedure leads to the last combination hash locking all of the underlying information. If any of the proxies change, 1, 2 or 3, this hash and the combination hash will no longer be correct.

Since all of the new hashes entering the merkle tree use the last combination hash, we also get a timetable for all the information. We know that the last proxy, no. 3, will have its verification merged with a combination hash containing references to all previous proxies. Hashes 1 and 2 must therefore have been registered before hash number 3.

The timetable, or time stamping as it is sometimes called, is valuable because it enables us to know which proxy and which information on the proxy is most recent. In the case of personnel registers, it is also valuable to know when the personnel registers have been recorded. If an update is made, we know which version applies. If records of personnel registers have been made every day in the last month, this is easy to check. It is also not possible for the provider of the merkle tree to make changes, given that the combination of hashes is published at least once a day, for example. One of the most used actors in this arena is Guardtime, which collaborates with the Estonian authorities, the US Defense Department, Ericsson, Verizon, etc. They publish their combination hash, also called a top hash, in the *Financial Times* once a month.

**Blockchain**

What is usually intended with a blockchain is that the merkle tree should also be safe for manipulation and not be dependent upon a single database. Another reason is that there might be a possibility that the owner of the merkle tree prioritizes incoming hashes for their own gain, something which is very valuable in financial markets. If someone were to have the opportunity to register their stock trades before anyone else, it would be extremely valuable. Given that the combination hash is kept secret for a couple of days, it can also be possible to make a new tree and add new hashes and thus create a new timetable, etc. To avoid this problem, it may therefore be important to arrange the databases in a distributed structure where several actors can secure the order of the data, and ensure that it adheres to set rules, is not destroyed, and so on. This means that there are several databases that all contain the same merkle tree. Different systems for blockchains use special algorithms to ensure that all databases are synchronized. These algorithms are called consensus algorithms. When several actors are allowed to have a synchronized database with the merkle tree, confidence in it increases.

**PAGE 77-78**

**Public blockchains**

The blockchains mainly associated with cryptocurrencies are called public blockchains. This technology is not used in the proposals described in this report. A few problems that are sometimes highlighted with public blockchains are therefore not relevant. Examples of problems often addressed in connection with blockchains, but which are thus not relevant in our examples in this report are:

1. Energy consumption - public blockchains often use a technology called Proof of Work. This technology requires large amounts of energy.
2. Scalability - public blockchains have capacity limitations. It is not possible to register overly large amounts of data in these.
3. Transaction speed - public blockchains have difficulty with the speed of registering hashes and other information.
4. Deleting records - in public blockchains it is not possible to delete old information. This is because blockchains used for cryptocurrencies need to be clear about how many cryptocurrencies have been created since the blockchain started.
5. Theft and losses - stolen or lost private keys can mean that large amounts are lost. It is possible to lose private keys even in the solutions described, but the losses are, in these cases, small or non-existent.

Blockchain has been described as a trustless technology, i.e. a technology where you do not have to trust others. In practice, this has its origin in public blockchains such as Bitcoin or Ethereum where a sole individual or organization cannot change registrations made by the system. If you have sold your Bitcoin, there is no way to take back the money or remove the registration. A new transaction can be made, but the old one cannot be undone. The one who controls the private key that has access to the respective Bitcoins can spend these and when they are done, someone else gains the control. Ultimately, this means that everyone must rely on themselves for the storage of private keys, which is risky. Few people want their pension lost just because they lost a personal code, or the computer's hard drive was hacked or broken. Therefore, in the case of Bitcoin, most use a depository, an organization, that takes responsibility for storing these private keys, which in turn controls Bitcoin. When a depository is hacked by someone on the inside or outside, which has happened, the owners have a system for disputes in order to get their money back. This means that the rightful owners of cryptocurrencies have a great need for some form of insurance, law enforcement, or other protection, which, at least today, requires institutions in the rest of the world.

**PAGE 79**

(No image or text)

**PAGE 80**

FAR is the Swedish organization for auditors, accounting consultants, tax advisors, payroll consultants, and specialists. FAR contributes to the profession’s development through recommendations, training, and referral activities. FAR arranges courses, publishes books, regulations, and the digital service FAR online, as well as two journals - *Balans* and *Resultat*. FAR's mission is to help the profession create benefits for business and society. This is mainly achieved through: The development of good professional practices, skills development, and advocacy.FAR’s members, approximately 5,100, are authorized and approved auditors, authorized accounting consultants, tax advisors, authorized payroll consultants, and other specialists, for example, in the field of sustainability reporting.

The Swedish Tax Agency is for everyone in society. We want it to be easy to do the right thing - for example, when you pay tax, sell or buy a home, start and run a company, move or get married. Our assignment from the government consists of three parts: Contribute to a well-functioning society for private individuals and companies, Contribute to securing the financing of the public sector, Combat crime. This means that we work with taxes, public records, the marriage register, property taxation, estate inventory, ID cards, and the investigation of tax crimes. We are also a creditor on behalf of the government. We have more than 10,000 employees and have operations throughout the country.

Kairos Future is an international consulting and research company that helps companies understand and shape their futures. Through trend analysis and market research, innovation, strategy and software support for AI-driven analysis, external monitoring, and innovation, we help our customers turn the big picture into concrete action. Kairos Future was founded in 1993, our headquarters are in Stockholm, and we have offices and partners all over the world.