Februar 2019

Blockchain
The Future is Built on Blocks

KROMANN
REUMERT

Blockchain
The Future is Built on Blocks

Chances are that blockchain-like technology will soon embed itself into the core of our society – and have a vast systemic impact on everything from democracy to monetary structures that date as far back as Ancient Greece. In this insight we introduce the main concept of blockchain technology and provide you with examples that serve to demonstrate some of the many possibilities presented by this technology and the vast impact it may have. In doing so, we touch upon the legal issues of using blockchain technology.

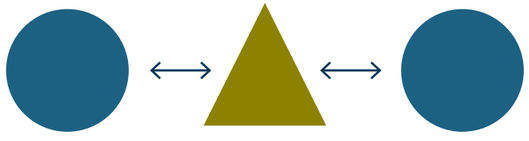
Blockchain is already used in both industry and government, mostly as a showcase for handling less complex processes. However, the number of cases that are trying to puncture the complexity and bureaucracy of existing processes is rapidly increasing. These new processes are not without challenges; the structures being challenged reflect old paradigms where third parties are used to provide the trust necessary for transactions to take place. But a blockchain can now provide that trust.

Trust and transactions

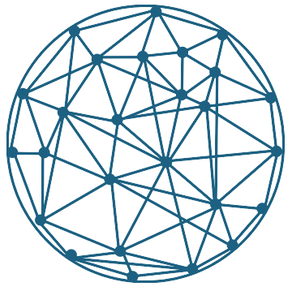
Trust used to be something bestowed upon a person based on his or her reputation, or family's reputation. A reputation for truthfulness, respect, and timeliness with agreements would lead to further access to values and assets. This type of trust – local trust or reputational trust – worked, and still works, for many transactions carried out in life.

The industrial revolution created a need for larger transactions, which led to methods for scaling trust, and to the foundation of the institutional trust underpinning all larger transactions in today's society. These transactions take place with the help of one or more intermediaries – a private or a public organisation such as a bank or law firm. Now, recent developments in technology have made it possible to create a new category of trust: distributed trust.

Distributed trust, or network trust, is found in companies like homestay broker Airbnb and GoMore – a Danish rideshare ing service. These businesses thrive on complete strangers staying in one's home or riding along in one's car – both examples directly countering our childhood learning to beware of those we do not know. But these are examples of how we are increasingly willing to trust complete strangers, based on ratings and reviews in the trust networks that are at the heart of these business models. Distributed trust is now being further fuelled by the ability to use a trusted blockchain network, which eliminates the need for trust between parties – as the blockchain network is the trusted party. Consequently, people who have no reason to trust each other can conduct business without having to go through a formal institution or neutral central authority.



Institutional trust
- **Closed**
- **Centralized**
- **Top-down**



Distributed trust
- **Open**
- **Decentralized**
- **Bottom-up**

Blockchain – is it a trustworthy technology?

The Economist Magazine dubbed blockchain the 'trust-machine' back in 2015. It is a well-chosen name, as the information underpinning the system – the ledger – is secure, transparent, and distributed to all its participants. Instead of having a central database, it is a decentralized database in a network spread across multiple entities ('nodes'). This means that every participant has access to the same shared data, in real time and at all times. Due to the cryptographic proof and consensus mechanisms, this data cannot be tampered with, so everyone knows it can be trusted. The data are immutable.

When making a bank transaction in the current financial system, the bank acts as a trusted third party – validating the transaction between the sender and the receiver. But blockchain negates the need for a third party, as its consensus mechanism ensures the transaction is validated by mathematics. In short, the trusted third party has been replaced by unalterable cryptographic proof – thus eliminating the need for a trusted third party. The blockchain is maintained by computers, nodes or mines, which store data and make the cryptographic proof. Nodes make the network run, and in return they get paid through an incentive system based on transaction fees paid by users and by the mining of new coins.

The transaction validation has already served as decisive proof in a court of law. However, the authority of any database depends on the quality; false data in equals false data out, which may affect the evidential value of a blockchain.

By way of example, construction work and IT development often involve issues about coordination with subcontractors and about the project plan as amended from time to time. Such "who knew what when" problems can be addressed using blockchain technology. Each amendment would then be put on the blockchain and require each contractor's acceptance. In the case of a subcontractor claiming ignorance of certain amendments to such project plan, reference to the cryptographic proof, i.e. the "fingerprint", can serve as proof in a court of law.

MAIN CRYPTOGRAPHY FEATURES

Hashing: A cryptographic hash function is a function that calculates a unique number (fingerprint) from a message (seed data). It is (a) a one-way function, meaning that a hash can be calculated based on the seed data, but the seed data cannot be calculated based on the hash, and (b) collision free, meaning two data seeds will never have the same hash.

Signature: A signature is made by asymmetric encryption with a private and public key. The private key is used to sign a message calculating a signature, which ensures only the person holding the private key can sign. The public key is used by recipients of the message to validate the signature. By taking the signature, the message, and the public key, the validity of the message can be determined, ensuring the message has not been tampered with.

This allows for a digital fingerprint to be added to any piece of data, a fingerprint which may be strong enough to be used as proof in court.

Bitcoin and beyond

Blockchain began with Bitcoin. Bitcoin emerged in the wake of the 2008 financial crisis, through its unknown inventor – or inventors – under the pseudonym of Satoshi Nakamoto. It was meant as a response to the existing banking system, through a 'be your own bank' idea, where people could store their own money in Bitcoin – a digital currency owned and governed by individuals. Bitcoin as a digital currency still acts as the reference point for blockchain and digital currencies, but it has also been the subject of speculative investment. This is a reminder that the technology is still in its infancy, but the concept of using cryptocurrency is gaining credence across the world.

Bitcoin also spawned the general term 'blockchain', which now covers all related technology within the field and not just a simple data structure.

Blockchain is a Distributed Ledger Technology (DLT) whose core strength is that data are decentralized across nodes and validated by a consensus mechanism, which makes it secure and, in some cases, provides anonymity.

Another example of DLT is Direct Acyclic Graph (DAGs), which is a different data structure than blockchain. Other consensus mechanisms are introduced for DAGs including voting algorithms, as opposed to mining, which is the power-hungry method that is used for consensus in Bitcoin. Voting algorithms is a much more efficient method in regard to power consumption and speed. The DAGs are thought to be one of the more long-lasting DLTs, as they address many of the issues found with blockchain.

Public and private blockchains

Another aspect of blockchain is governance and ownership of the network, and thus its data. Well-known blockchains like Bitcoin, Ethereum, Ripple, and many others are publicly governed, whereas other business blockchains are private.

On private blockchains, the possibility of review and audit is limited, as data access may require permission, which in turn requires access authentication. On public blockchains, anyone can run a node and thus access the ledger to review and audit it. Anyone can make transactions on the chain, even parties who do not have nodes. Therefore, no access authentication is performed, and no permission is required.

For public blockchains, replicas of the ledger are stored on each node. There is no central "original". All copies of the blockchains are equally valid. This decentralization ensures high immutability of data. Private blockchains can be distributed between the participants (a sort of semi-decentralization) but may also be completely centralized. Intrinsically, this means that the ledger is more limited in its distribution, which compromises the high immutability of data. On the other hand, it also allows the owner(s) of a private blockchain to correct errors or change entries due to e.g. court orders, bankruptcy, or other events that happen but cannot be accounted for without consensus on a public blockchain.

Private blockchains are therefore generally cheaper and faster than public blockchains, making them ideal for most business purposes, while public blockchains offer more security and openness, which is more appropriate for ideas such as a decentralized land registry, international currency, and wider democratization ideas.

THE MAIN CHARACTERISTICS ARE LISTED HERE:

	Public	Private
Centralization/Purpose	Decentralized: peer-to-peer	Semi-decentralized: good for business to business
Access authentication	None	Authentication required
Data Permissions	Permission-less	Permissioned data access
Advantages	• Supports anonymity and is non-discriminating • High immutability of data (security) • Trustless environment: not dependant on trusted third parties	• Supports legal entities • Higher performance • Better scalability • Efficient governance model

From a legal perspective, the choice of public vs. private is essential. A private blockchain will allow you to set up a governance structure that can correct faulty data and account for legal enforcement, leaving 'scars' on the blockchain.

Smart contracts

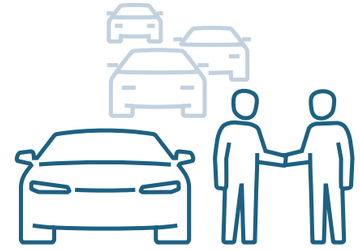
While undisputable trust in data is a cornerstone of DLT, another solid pillar is the ability to make deterministic computer programs which are executed on the chain. These programs are known as 'smart contracts'. Confusingly these are neither smart, nor contracts, but they make it possible to program contractual conditions into a piece of blockchain code that, once executed, cannot be stopped and will always do exactly as programmed to do. The International Monetary Fund (IMF) believes blockchains could reduce moral hazards and optimize the use of contracts in general.

The blockchain ensures that smart contracts are secure and cannot be tampered with. But, it is up to the programmers of a smart contract and those entering into a smart contract to determine if it corresponds to the agreement underlying the smart contract. A common use for smart contracts is when money is programmed to be released only when pre-defined conditions are met – such as in this car sales example:

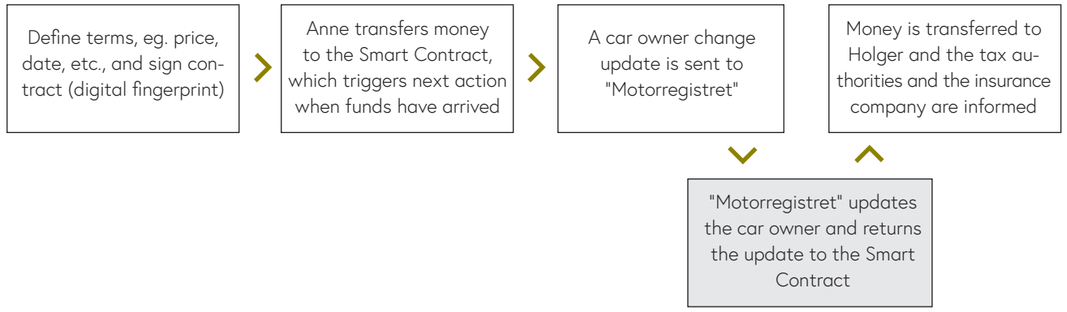
SMART CONTRACTS FACT BOX

Blockchain-based smart contracts are deterministic computer programs that are deployed and run on a blockchain and are automatically executed when pre-defined conditions are met.

A CAR SALE EXAMPLE



Anne buys a car from Holger



Smart contracts can support the simultaneous exchange of services very efficiently – making it less complicated to trade. However, smart contracts will not replace regular contracts on a general scale. Coding parts of a regular contract as a smart contract provide an automated way of ensuring concurrent consideration. However, smart contracts are not well-suited for legal standards such as 'fundamental breaches of contract' or 'material defects', nor will a blockchain always be sufficient to create the necessary legal documentation. Often the smart contract will have to interact with the real world through an oracle (an intermediary ensuring that what is inserted into the smart contract is true) or with other databases for documentation purposes. This is something that must be worked into the blockchain solution and its governance documentation.

Blockchain in action

We will now look at some examples of how to use blockchain and pinpoint the related legal issues:

1. A good example of using blockchain solutions is the handling of property and land transactions. Sweden's land-ownership authority, Lantmäteriet, started testing its own blockchain solution in 2016 and began trial transactions in 2017. The solution is now technically ready. The benefit is that real-estate transactions, from signing the contract to the sale being registered, become paperless. The parties do not need to be located in Sweden to sign, so a transaction can be largely frictionless and much faster than the 3-6 months that is typical in the current system. Lantmäteriet estimates yearly savings of SEK 5 billion, once operational. Full introduction is currently being held back, however, since legal hindrance regarding digital signatures has not yet been removed.

2. 'The TradeLens Blockchain Shipping Solution' by IBM and Maersk, which is being tested in production now, is an example of blockchain and smart contract technology that has the potential to revolutionize the world's global supply chain. It is a collaboration between the two companies in a bid to spur and ease international collaboration within international shipment, using open standards and APIs. Blockchain and smart contracts are the foundation for the applications on top, which handle certain processes e.g. dealing with all documents.

   More than 70 participants are already enrolled – including global container carriers, port and terminal operators, customs authorities, freight forwarders, and Beneficial Cargo Owners (BCOs). They can all now access information applicable to them – including an audit trail in real time on each container with relevant data such as temperature. Overall, the transparency and efficiency of the global supply chain have vastly improved; one case shows 40% reduced transit time for packaging materials to a production line in the US saving millions of dollars, and BCOs can always get live data on their shipments. However, quite a few legal considerations must be made in such a set-up, for example i) competition law issues such as merger control, access to the platform and no coordination effects, ii) fulfilment of multiple jurisdictions' legal requirements to the shipments handled on the platform, iii) safeguarding of data protection legislation, and iv) legal enforcement, including choice of law and venue.

3. In the world of banks and exchanges, SEB and NASDAQ have joined forces to build a trading platform for mutual funds based on blockchain (chain.com) targeting the Swedish fund market. The process is currently handled by different intermediaries through manual documents, different systems, and phone calls, which makes it very inefficient and non-transparent. The blockchain-backed solution aims to make the fund market transparent for its participants and to vastly increase efficiency. Such a solution must be compliant with relevant financial regulations as well as securities and competition laws.

4. Insurwave – a joint venture between EY and Guardtime – is a private and permissioned blockchain for insurance. Maersk is a pilot customer on the chain, while engine and hull insurance is the product in question. The main problem Insurwave seeks to solve is that, currently, the marine insurance value chain is very cumbersome and inefficient – thus unsatisfactory for customers. More than 40% of the insurance premium is an overhead on transaction costs, which is caused by a non-transparent, highly transactional value chain involving many stakeholders and intermediaries. Insuring a vessel today takes upwards of 100 document transactions, which is a sequential and manual process. This means that no-one has full transparency nor a holistic view of risk. It also means the administrative burden is very high, with 75% spent on insurance contract administration and 25% on risk management – although it should be the other way around to create value for the customers.

   By using Insurwave, EY and Guardtime want to accomplish a transparent and efficient process with fewer intermediaries, where administration such as document flow, invoicing, and payment is handled automatically. Moreover, they want to improve the general value process by providing real-time data on vessels, so insurance can be made on current data instead of static demographic data. This makes pro-active risk mitigation possible, instead of the current passive process where risk materialization is handled only when there is an actual claim. The governance of such a system must ensure that all the handled documentation and deeds are enforceable contracts valid in a court. The setup must further be compliant with financial regulations.

5. Voting is a much-touted use case of blockchain. This is still in its infancy but started with small cases. A mobile voting platform is being tested in West Virginia for 2018 general elections, whilst Nasdaq in Estonia used blockchain-based voting for shareholder voting in its annual general election. Naturally, such a system must fully comply with the applicable company law as well as data protection regulations

Legal issues to be aware of

Using blockchain does not change the law – anyone using it must still comply with competition law and data protection law. They must also ensure they have a valid and enforceable contract. The documents setting out the governance of a blockchain are therefore essential from a legal perspective. It is vital to understand how the blockchain and related smart contracts are intended to work to identify the legal issues and the proper handling thereof.

Every case has its own characteristics, but the following legal issues are always worth considering:

a) The governance documentation setting up the blockchain must give a clear legal basis for enforcement of the agreements made – a valid agreement, clear choice of law and venue, and in many cases also the possibility to identify your counterpart. In a private blockchain, the possibility to allow for regulation that can change the blockchain should also be considered, e.g. to enforce a court decision or remove faulty data.

b) Data protection is a key issue, especially within the EU due to the very high fines. The use of blockchain can make it difficult to apply the fundamental concepts of data controller and data processor, as it is not always clear who controls the data. Furthermore, some of the basic rights of data subjects, such as the right to be forgotten, work directly against one of the core values of a blockchain – the immutability. Anonymization of the personal data may be one way to solve the issue, but pseudonymization will not be enough and the possibility of making an identification based on other data points must be taken into consideration. Other solutions could be to set up the blockchain so that it cannot contain personal data (potentially with a side chain for storing personal data), or through the governance of private blockchains to allow for changes that leave 'scars' in the blockchain.

c) Competition analysis can be necessary before setting up a blockchain. Many blockchains allow anyone to see what has happened earlier in the blockchain, which means competition sensitive information may be visible to rivals. This, as well as other issues – e.g. restrictions on making horizontal joint ventures – need to be dealt with.

Perspectives and Kromann Reumert's advice

Blockchain and Distributed Ledger Technology as a whole are still in their infancy, and – whilst the technologies hold the promise of a massive change to our current systems and structures – these changes are still years away. It requires adoption, testing, and supporting legislation and legal practice – for users, businesses, and states.

A sector bound for further disruption is the financial services industry. Here, private and central banks and government need to work out how to deal with e-money, the legal status of cryptocurrencies. This might be an area where changes driven by the new technical possibilities are more imminent.

For start-ups and smaller businesses, blockchain-based structures can fuel more efficient collaboration and higher efficiency when raising capital. These structures do, however, raise questions of data ownership, competitive issues, data privacy, securities laws, and so on, which must be taken into consideration.

And then, as with everything else enjoying hype and attention, it is important that blockchain and the related technologies are only applied when there are sound reasons and a legal basis for doing so. Blockchain technology has come to stay, and its field of use is solely going to be extended from here. Kromann Reumert's technology team has vast experience in advising on the newest technologies and trends, and we can guide you on your company's blockchain adventure.

Kontakt

Torben Waage
Partner

Mobile: +45 40 61 08 86
Direct: +45 38 77 45 60
tw@kromannreumert.com

Amalie Paludan
Attorney

Mobile: +45 20 19 74 04
Direct: +45 38 77 42 59
amp@kromannreumert.com

KROMANN REUMERT

At Kromann Reumert, we set the standard. Together. We provide value-adding solutions and advisory services with dedication and focus. We are driven by our four core values: quality, commercial understanding, spirited teamwork, and credibility. We are Denmark's leading law firm with offices in Copenhagen, Aarhus and London.

COPENHAGEN
SUNDKROGSGADE 5
DK-2100 COPENHAGEN Ø

AARHUS
RÅDHUSPLADSEN 3
DK-8000 AARHUS C

LONDON
65 ST. PAUL'S CHURCHYARD
LONDON EC4M 8AB

LAW FIRM
KROMANNREUMERT.COM
TEL +45 70 12 12 11