M E M O

Blockchain technology can provide efficient infrastructure for payment services

1. Summary

During 2021, the company ZTLment ApS (ZTLment) conducted a test in the Danish Financial Supervisory Authority's (DFSA) regulatory sandbox, FT Lab. ZTLment uses blockchain technology to offer companies to settle business-to-business (B2B) payments in real time using e-money issued on blockchain. ZTLment's payment solution is integrated on platforms that digitise the processes for concluding and documenting purchase agreements between a buyer and a seller. Blockchain technology ensures transparency of completed transactions.

ZTLment's proposed business model builds on Algorand's blockchain and supports e-money payments issued by the Icelandic e-money institution, Monerium. When Monerium issues e-money to a blockchain, it is done in the form of e-money tokens (EMT). ZTLment has developed the software that communicates with Algorand's blockchain. In order to make payments with ZTLment's solution, users must download ZTLment's app, which forms a so-called non-custodian wallet.

The test performed in FT Lab shows that blockchain can support activities covered by the Danish Payments Act (DPA). The test also shows that blockchain can provide an effective alternative to payment services that make use of the traditional payment infrastructure in relation to settling payments in real time. At the same time, the test shows that payment services using blockchain as infrastructure differ significantly from existing payment services using the traditional payment infrastructure. This is described in more detail below.

In this orientation the DFSA has taken the opportunity to inform the market broadly about the impact of the use of blockchain in payment services under the DPA. The orientation is based on the test in FT Lab as well as the DFSA's ongoing work on this area.

Blockchain is the technology behind crypto assets such as Bitcoin and Ethereum. Blockchain can be described as a "common register" in which transactions made with crypto assets between accounts associated with the blockchain are recorded. A crypto asset is, in the sense of the word, an asset, and the specific crypto asset represents the rights attributed to the asset.

Crypto assets can therefore be many other things than Bitcoin. EMTs are electronic money issued on blockchain, which is covered by the DPA. EMTs differs from Bitcoin, which is not considered funds in the sense of the DPA.[1]

The DPA[2] regulates payment service providers and imposes different rights and obligations on users and service providers. Providing payment services requires an authorisation from the DFSA. It is the assessment of the DFSA that providers using blockchain to offer a payment service may be subject to the DPA. Providers using blockchain to offer a payment service should therefore contact the DFSA for an assessment of whether the solution requires authorisation under the DPA.

Blockchain itself, on the other hand, is not necessarily covered by the DPA if the blockchain merely functions as a piece of technical infrastructure. It is the DFSAs opinion that blockchain can serve the same function as clearing systems and technical services providers that support the provision of payment services, both of which are exempted by the DPA.

Blockchain is a decentralised technology. This means that a user of a blockchain-based payment solution may have to perform tasks that regulated companies will normally perform when using traditional payment services. A consumer or company typically has an account with a bank where funds can be received and deposited. The bank is obliged to guarantee users several essential rights, for example in the event of fraud. Using blockchain-based solutions, funds are received on the user's public key on the blockchain, which the user is generally responsible for creating, managing and storing. This means that there is typically no account servicing institution that is responsible to the user for the account kept. Therefore, when using blockchain-based payment services, there can be situations where the user bears the sole responsible for such matters.

Therefore, depending on how the blockchain-based payment service in question is designed, a user may be responsible for carrying out the tasks normally performed by regulated operators in the traditional payment infrastructure. Users may thus be at a disadvantage compared to when the traditional infrastructure is used, even if a regulated payment service is used to make payments from the user's account on the blockchain.

The DFSA expects that the current issues when using blockchain as an infrastructure for payment services, will be addressed at EU level, including in the upcoming review of the Payment Services Directive. Until then, users of such solutions should pay attention to how they are protected.

---

[1] Subject to the DPA, funds are banknotes and coins, scriptural money or electronic money. Bitcoin have previously been compared to glass beads because they do not have the intrinsic value that funds do. That is why they are not regulated at present either.
[2] The Danish Payments Act (law number 2710 of 6 January 2022) implements the Payments Services Directive (2015/2366 EU).

In this briefing, the DFSA has only taken a position on the regulatory management of payment services using blockchain as infrastructure, on the basis of the DPA. The DFSA has not taken a position on other types of services offered using blockchain. The DFSA has assessed the solution only on the basis of the DPA and not other requirements that may result from the legislation in other areas of jurisdiction. Moreover, the review does not involve a detailed technical assessment of specific blockchains. For example, the DFSA has not made a concrete assessment of the stability and security associated with the use of blockchain.

2.   Introduction to blockchain

A blockchain, or more precisely Distributed Ledger Technology (DLT), can generally be described as a ledger of transactions. The ledger is a database shared between and maintained by an unspecified number of operators. It is also called a peer-to-peer (P2P) network of data centres (nodes), where the nodes both store and maintain existing data, as well as continuously contribute to verifying and including new data on the ledger. The dataset (blockchain) is the ledger on which transaction data is recorded. The nodes are the users/computers that operate the network. In this way, you can always see all the transactions that have been completed in the register. Blockchain therefore contributes to transparency.

Blockchain is based on asymmetric cryptography that includes the issuance of a public and a private key (the key pair). The key pair is generated using cryptographic techniques, and is, among other things, a necessary input in relation to the verification of the transactions to be completed on the blockchain. The public key can be compared to a customer's account number in a bank, while the private key can be said to represent the customers right of disposal to the funds associated with the public key. As a user, you therefore need both a public and private key in order to receive and transfer crypto assets.

The blockchain has a protocol (consensus mechanism) that sets out the rules by which the network operates. The aim is to ensure that the credibility of the network is not compromised. Different consensus mechanisms are used across blockchains, such as Proof-of-Work (PoW) and Proof-of-Stake (PoS). Common to them is the fact that they give the nodes, which actively operate the blockchain, an incentive to do it properly.

## 3. Blockchain as infrastructure for payment services

ZTLment's test at FT Lab has shown that the way payment transactions are conducted in the traditional payment infrastructure differs in many ways from the way transactions are conducted, when blockchain is used as infrastructure.

The main difference lies in the fact that the traditional payment infrastructure has a need for central and trusted operators who bind together all the operating parties. Central parties are necessary to ensure that the underlying funds of a payment transaction between independent account-servicing institutions are effectively transferred. Blockchain, on the other hand, can serve as an efficient decentralised alternative to this. This means that several of these key operators are not necessary to complete a transaction.

Figure 1 below illustrates a generalised process for how a payment transaction can be completed, cleared and settled in the traditional payment infrastructure and on blockchain. The traditional payment infrastructure requires several systems to interoperate. For example, if a user pays an invoice through its online bank, which is a payment instrument, to a payee who is a customer of another bank, the payment process is as follows:

1. The payer enters payment information into the online bank with his bank, including the amount of money and information of the payee.

2. The payer's bank completes the transaction – often through its data centre. In practice, the bank communicates a message through the payment infrastructure messaging system (e.g. SWIFT) to the payee's bank that a payment transaction is being initiated.

3. Following the dissemination of information on transactions between data centres, payments will typically be cleared. This happens in the clearing systems.

4. Once the clearing has been completed, the transactions are settled. This is done by the payer's bank crediting the payer's account in its internal systems (the data exchange), while the payee's account is debited by the receiving bank. In addition, there is a final settlement between the account servicing banks in a central bank.

Figure 1 - Traditional payment infrastructure and blockchain
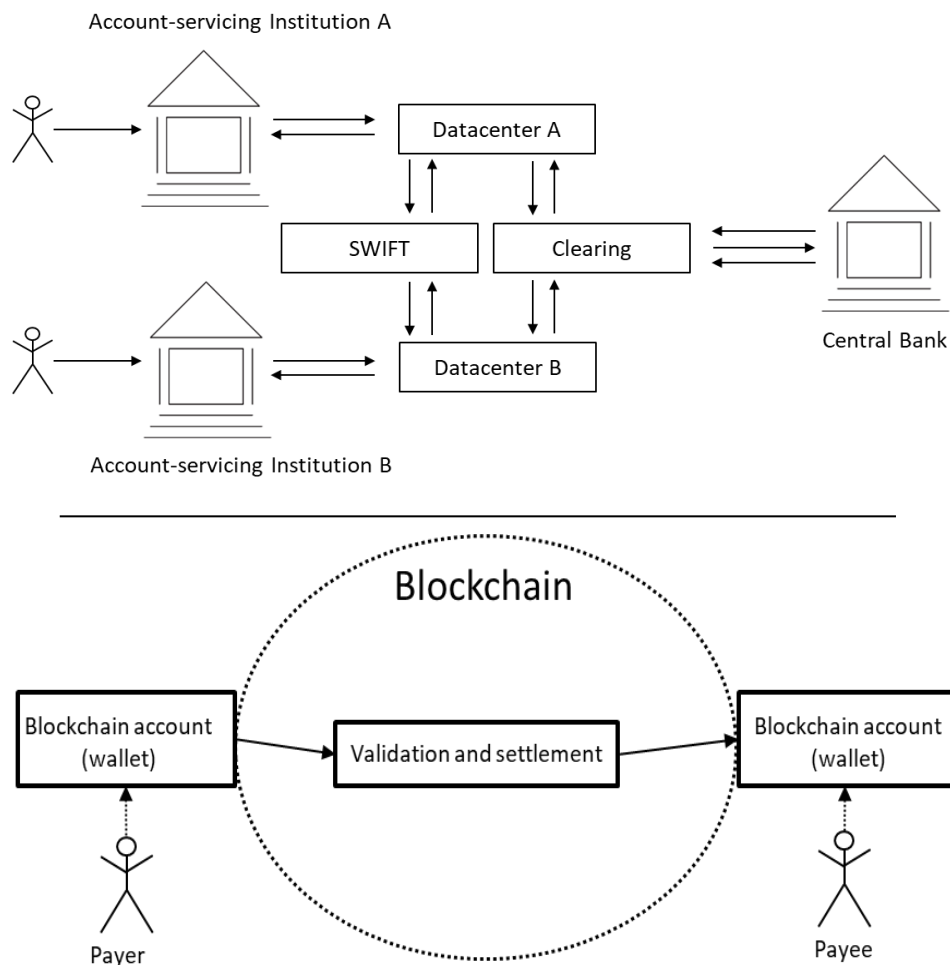
Note: The figure sets out generalised examples of payment infrastructure.
Source: The Danish Financial Supervisory Authority.

The figures illustrate the different operators and systems that appear in the traditional payment infrastructure and in services using blockchain as infrastructure. The blockchain technically handles the role of data centres, banks' internal systems and clearing systems in the traditional payment infrastructure.

The test with ZTLment specifically showed that blockchain can handle the same task as the traditional payment infrastructure, but in a new way. Unlike the traditional payment infrastructure, where each account-servicing institution has its own internal systems in which the amount of funds associated with the individual accounts are kept up-to-date, the blockchain constitutes a "common register" in which transactions between accounts linked to the blockchain (in this case e-money payment transactions) are recorded.

Therefore, all operators wishing to transfer funds on the given blockchain must have as their starting point an account associated with the blockchain. The blockchain consensus mechanism ensures that initiated transactions are validated and recorded. Transactions are recorded and settled only if they comply with the terms of the blockchain's underlying protocol. Blockchain can therefore be used to settle payments and serve as a decentralised alternative to the role of both account-holding institutions and the traditional payment infrastructure.

3.1. Blockchain as payment infrastructure is not covered by the Danish Payments Act

The DPA and other financial legislation regulates legal persons subject to law. This creates a challenge in terms of regulating decentralised services, like a blockchain where such legal persons cannot be identified.

However, the DPA also exempts various services from regulation. For example, there are a number of services that are part of the traditional payment infrastructure but are not regulated under the DPA. More specifically, transactions made by clearing systems as well as technical service providers, which support the provision of payment services are excluded.

The DFSA considers that it is not the purpose of the DPA or the Payment Services Directive that providers of technical infrastructure should be covered by the DPA. The DFSA therefore also considers that blockchain is generally exempt from the DPA in the same way as clearing systems and technical service providers, provided that the blockchain alone constitutes the technical infrastructure that supports the provision of payment services. The key of the assessment is that a blockchain only *records* a transaction. It is an external party that builds solutions on top of the blockchain that can be considered *to complete* a transaction. This is done by this external party communicating the transaction to the blockchain through its solution.

3.2. Providers using blockchain in their solution may be subject to the Danish Payments Act

As a result of the test with ZTLment, the DFSA concludes that the proposed business model constitutes a payment service that requires authorisation under the DPA, even if the solution is based on blockchain. More precisely, the business model requires authorisation to issue payment instruments and to execute payment transactions.

It is central to the assessment under the DPA that ZTLment specifically offers users of the solution to execute payments with funds (e-money) and not other types of crypto assets. Funds are notes and coins, scriptural money or electronic money. Not all crypto assets constitute funds under the DPA. Transactions with Bitcoin and Ethereum, for example, are not currently covered by the

DPA. However, these transactions may be covered by the upcoming Markets in Crypto Assets Regulation (MiCA) and the forthcoming revision of the Payment Services Directive.

Today, similar services are offered with crypto assets that do not constitute funds under the DPA, typically by so-called wallet providers. In general, providers of services on blockchain that can be equated with payment services should bear in mind that they may offer regulated activities if the activities are carried out with crypto assets that can be characterised as funds.

Therefore, it is also important for the DFSA to emphasise that contractual relations can be crucial for whether, and if so how, a provider should be regulated according to the DPA. It is essential whether the provider offers users the option to execute payments by using the provider's service. In such cases, the provider's service is likely to constitute a payment service. This requires authorisation from the DFSA.

For example, if a provider offers a user a service that allows the user to initiate payment orders using a set of procedures agreed between the provider and the user, it offhand requires permission to issue payment instruments, even if blockchain is used as infrastructure. It is the provider of the solution that can be used to launch payment orders with funds issued on a given blockchain that is covered.

In order for a payment transaction to be completed and executed in practice, the transaction must be communicated to the blockchain. The blockchain is responsible for the settlement of the payment transaction. The message given to the blockchain that a payment transaction should be registered on the ledger, constitutes the act that actually causes the payment transaction to be settled. The DFSA considers the message conveyed through the provider's software to the blockchain to register a transaction to be the act that actually causes the payment transaction to be recorded and executed in practice. A provider whose software integrates into a blockchain and thereby in practice ensures that the blockchain registers and settles a given payment transaction must therefore be authorised by the DFSA to execute payment transactions.

It also matters for the division of responsibilities whether the provider has a contractual relationship with the blockchain on which the provider bases its solution. A payment service provider is responsible to the user for the service provided. This applies regardless of the type of technology or subcontractors used by the provider to provide the service to the user. The provider must therefore pay general attention to which subcontractors it uses to provide the payment service and how the contractual arrangements are constructed in relation to the allocation of responsibilities.

3.3. Payments initiated by payment instruments as an example

During the test, it became clear that the payment value chain, when blockchain is used as infrastructure, differs from the payment value chain in the traditional payment infrastructure. As an example, the payment value chain for a traditional payment instrument, such as a debit card, is compared to the payment value chain for a payment instrument on a blockchain below.

The use of a regular debit card for payment in shops means that the payee (the store) has an agreement with an acquirer of the debit card. The role of the acquirer is to ensure that the payee can receive the funds from the payer when the debit card is used. In practice, the payer will use the debit card at the store's payment terminal. The software of the payment terminal and the payment terminal operator collect the information about the payment transaction in question and pass it on to the acquirer, who subsequently ensures that the funds are transferred from the payer's account to the payee's account in practise. The actual settlement and clearing of the payment transaction is done using the traditional payment infrastructure, in the same way as for account transfers described above.

As a starting point, it is not necessary for an acquirer to be included in the payment chain when payment instruments are used to transfer funds on a blockchain where both the payer and the payee have an account on the blockchain. This is because all activities carried out with the payment instrument will be recorded directly on the blockchain using the consensus mechanism. It is not necessary for several central systems to act together, as in the traditional payment infrastructure, or for an acquirer to collect and disclose relevant payment information. Payments on a blockchain can therefore best be compared to account transfers between two accounts in the same account-servicing institution, where only the internal systems of the institution need to communicate.

3.4. Decentralised solutions can put a user at a disadvantage compared to payment services using the traditional infrastructure

As a starting point, a blockchain supports the settlement of so-called Peer-to-Peer (P2P) transactions. When using payment services using blockchain as an infrastructure, the user will not necessarily obtain all the rights arising from the DPA or other regulations.

This is due to the fact that several operators, which usually appear in the traditional payment infrastructure, do not necessarily appear in the payment process when blockchain is used as infrastructure. In practice, this means that the user must carry out a number of tasks himself, which will normally be carried out by a regulated company. It will therefore be up to the user himself to ensure a number of conditions normally handled by a regulated company.

Traditionally, payments between payment accounts held by account-servicing institutions typically take place at a financial institution. The legislation lays down a number of obligations for the account-servicing provider to ensure adequate protection for customers. This is different from cases where block-chain is used as payment infrastructure. Here, the user is generally responsible for keeping the account on the blockchain where the payment is initiated from or received on. Even if the user uses a regulated payment service provider to initiate a payment, there is not necessarily a provider behind the user's account on the blockchain.

As a result, the user does not obtain the same protection as a user who creates an account with an account-servicing institution. For example, in the event that the account is hacked, the account-servicing institution must reimburse the payer for the loss. This is not the case for decentralised solutions where the user creates and is responsible for its own account on the blockchain. Therefore, these types of solutions may put the user at a disadvantage compared to using a traditional payment solution where a regulated company manages the account for the user.

Furthermore, as a payee, it should be noted that an acquirer is not necessarily a part of the payment process when blockchain is used as an infrastructure, because the technology eliminates the technical need for such services. An acquirer is obliged to ensure that the payee can receive his funds under the DPA. Therefore, if a payee does not have an agreement with an acquirer, these rights do not apply.

The DFSA expects that the future EU regulation on crypto assets, as well as the upcoming evaluation of the Payment Services Directive, will attempt to address the challenges that blockchain may pose. Until then, users of such solutions should pay attention to how they are positioned.

4. Further work by the DFSA on blockchain

ZTLment's test in FT Lab has demonstrated a concrete example of how blockchain technology can support the provision of a payment service. The technology's use in the financial sector is generally increasing, and the DFSA expects this development to continue. Going forward, we will see several different types of financial business models using blockchain.

It is therefore essential to ensure that the regulatory management of blockchain adequately ensures consumer and investor protection and financial stability without hindering innovation. The DFSA is actively involved in the development of new regulation in this area, where technology neutrality is a key focus point. The Commission's proposal for a Regulation on Markets in Crypto Assets (MiCA) is one of the first concrete regulatory measures in this area. Going forward, changes to existing regulation, such as the upcoming review of the Payment Services Directive, will also have to deal with the technology.

Although the technology has the potential to support new and smart financial services, all the nuances and risks associated with the use of blockchain remain uncharted. The DFSA is therefore setting up a new working group for blockchain and decentralised finance (DeFi). The task group will support the general knowledge, supervision with and risk assessments of the DFSA in this area. In addition, the working group will provide input to the preparation of new regulation and support the DFSA's contribution to new European regulation.