MASTER THESIS
COMPUTER SCIENCE

RADBOUD UNIVERSITY

Blockchain for post-trade settlement, clearing and custody of financial instruments

Author:
Sven Arissen
s4206363

First supervisor/assessor:
dr. Jaap-Henk Hoepman
jhh@cs.ru.nl

Second assessor:
dr. Zekeriya Erkin
z.erkin@cs.ru.nl

July 30, 2019

Abstract

A large amount of value is transferred on the financial markets everyday. The stability and efficiency of this system relies on a solid infrastructure for clearing and settlement of these trades. This thesis analyses what role the blockchain can play in these processes. Though the blockchain is not without its merit, regulatory and technical challenges will likely limit it to being at most evolutionary instead of revolutionary.

Contents

Chapter 1

Introduction

Over the past few years the application of blockchain technology [1] for projects in various fields has increased drastically. Though many applications can theoretically use a blockchain, this is not always the optimal choice. In some cases the previous system was simply old and "legacy" (or there was no digital system at all) and a newer system was necessary. Though the simple fact that the blockchain spurred the creation of a newer, better system is nice, there may not have been any need for a blockchain. A "traditional" centralised or distributed database with an application layer may have sufficed and might have been more efficient. There are also periodic news stories about blockchain projects being shelved because it was "a solution in search of a problem" [2]. Even cryptcurrencies like Bitcoin seem only moderately useful so far. Though intended as a currency Bitcoin is rarely accepted as a payment method and seems to be far to volatile to be used as a currency[1]. One area of interest for the application of blockchain is the post-trade process of trades in financial instruments.

For many people financial instrument trading will be primarily associated with exchanges like the New York Stock Exchange (NYSE) or Euronext Amsterdam. In reality the exchange plays only a small, if important, role in the full lifecycle of a trade. Part of that lifecycle occurs after the execution (creation) of a trade on an exchange. This is referred to as post-trade and consists of two steps: clearing and settlement. Settlement is the actual transfer of cash[2] and securities to its new owners. Clearing consists of various activities between the execution and settlement of a trade,

[1] Currency is supposed to be either a stable holder of value (like gold) (that way my salary is worth (buys me) roughly the same tomorrow as today), or a medium of exchange.

[2] In daily use "cash" is often used to refer to physical cash (coins and banknotes), in literature on trading in financial instruments it is used as a more general term, carrying a similar meaning to funds or money.

the details of which depend on the type of instrument that is traded. In chapter 2 we will provide a more extensive description of the current trading lifecycle focused on the post-trade steps. There is a great variety of financial instruments each with their own processes and regulations. The analysis in this thesis is limited to cash securities (equity and debt securities) and derivatives.

The current system is not without its flaws. There is a high degree of intermediation especially in the post-trade area, with corresponding costs. A study from 2015 by Oliver Wyman [3] estimates the total revenue for major post-trade actors (CCP, CSD, Custodian) to be at $5 billion for clearing related activities and $43 billion for settlement and custody related activities. In chapter 4 we will describe these flaws in more detail.

The blockchain is the underlying technology of Bitcoin [1]. Bitcoin was originally designed and developed by Nakamoto to have a decentralised payment system without the need for intermediaries (banks). In chapter 3 we will provide a more detailed look a blockchain technology.

A process focused on the transfer of ownership of certain specialised types of financial assets suffering from a high degree of intermediation sounds like the perfect use case for blockchain technology. In chapter 5 we will contain a more detailed theoretical analysis of the various advantages and challenges of using blockchain technology in this field. Followed by a more practical analysis based on a case study on a securities settlement system based on blockchain technology in chapter 6.

Blockchain technology is ultimately a tool in a toolbox; with its own inherent advantages and disadvantages. As such it is worth analysing if the current flaws of the process can be solved with other technological (or non-technological) solutions as well.

The intent of this analysis is to have an overview of the inherent constraints of the application of the blockchain to this area of interest and to analyse what advantages can be uniquely provided by the blockchain given the constraints we have to deal with. With this we can then provide an answer to the question: "In which way does a blockchain based solution add value compared to another, non-blockchain based, system for a post (financial instrument) trading infrastructure?".

Chapter 2

The capital markets

2.1 Financial instruments

Financial instruments are a specific type of financial asset. Assets comprise any sort of resource (in the broadest sense of the word) that can be owned by some legal entity or person: like real estate or commodities. The classical example of financial instruments are (financial) securities. The exact definition of what a security is varies by jurisdiction. In the US a broad definition of securities was defined in the Securities Act of 1933 [4] and the Securities and Exchange Act of 1934 [5]. In the decision on whether or not a particular instrument is a security these definitions are often supplemented with the Howey test [6] and the results of other cases. In the EU a broad definition of "transferable securities" as a subset of financial instruments is provided in the MiFID2 directive [7].

Securities can be broadly divided in two categories:

- Equity securities: a common example here are stocks. Equity securities entitle the owner to partial ownership of a company. This will generally entitle the owner to dividend payments and often also give them voting rights.

- Debt securities: a common example here are corporate bonds. Bonds are issued by companies or governments to collect money from investors against a periodic interest payment and a final principal payment. Debt securities generally entitle the owner to periodic interest payments and a final principal payment. Debt holders have priority over equity securities in case of a bankruptcy of the issuing

company meaning they have a better chance of regaining their investment if this happens.

Securities in Europe are often identified by an International Securities Identification Number (ISIN), a unique 12 character code. In the USA and Canada the CUSIP number is more commonly used to identify securities. Though technically not mandatory many reporting regulations require the use of a valid identifier such as an ISIN.

A third, somewhat different, category of financial instruments are derivatives. Derivatives are contracts with some underlying asset[1]. Important here is that these contracts are tradeable. A classic example is the "option" where two parties have a contract with one party having the right to buy an asset from the other at a certain price and date[2]. In theory these contracts can take on many different forms, but when traded on an exchange there will be a limited number of types of derivative contracts that can be traded.

Monetary assets (currencies) and participation in funds[3] are generally also considered financial instruments and come with their own financial market infrastructures and processes. The analysis in this thesis will be limited to (equity and debt) securities and derivatives. Cash does play a role in the trading of financial instruments (for most trades instruments are traded against cash), as such including cash in the analysis is useful. Any such analysis will be limited to the role it plays in financial instrument trading.

Bearer & Registered securities A distinction can be made between bearer securities and registered securities. Bearer securities entitle anyone that "hold" them to their benefits. As such these securities are not centrally registered and have to be presented when requesting benefits. Traditionally these bearer securities were physical certificates without any ownership information attached to them. This means that everyone "holding" the physical security was entitled to the rights associated with it. In recent years many of these physical securities have been recorded in digital book-entry form instead and have taken on a form that is (operationally) similar to

[1] These underlying assets are often securities like shares or bonds, but this is not always the case. Someone could create a contract stating that they will buy 100 potatoes against a price of €0.50 per potato at some point in the future. In this case the underlying asset is not a security, but a commodity.

[2] In the case of options, they can also elect to not exercise this right.

[3] Often referred to as: Units on collective investment undertakings.

registered securities. Bearer securities are unpopular with regulators as their anonymous nature makes it easier to avoid taxes and other forms of oversight. The 4th EU AML directive instructed member states to take measures to prevent misuse of these types of securities.
In the case of registered securities there will be a central organisation (registrar) keeping track of all current securities and their ownership.

According to a report by the ECSDA (European Central Securities Depositories Association) in 2016 [8] the usage of bearer shares in the EU differs per member state as it depends on member state law.

2.2 Primary and Secondary market

An important distinction to make when talking about the capital markets is the one between the primary and secondary market. The primary market concerns itself with the initial offering (or issuance) of a security; an initial public offering (IPO) being the obvious example. The exact process will depend on the type of security and the market chosen. In this case it will ultimately lead to transactions between an issuer and an investor.

After that these securities may be tradeable on the secondary market. Here investors will trade securities amongst each other. The issuer will generally not be involved except for corporate actions[4].

2.3 Capital markets

2.3.1 Pre-trade & Trade

The part of the process before a trade is "executed" concerns itself with order submission and matching. The exact flow and parties involved depends on the type of market on which the instrument is traded, which generally depends on the type of instrument traded. Brokers are active in all market types. They facilitate matching (finding a buyer for a seller and vice-versa) and price quotes (providing information on current market prices for an instrument), especially in less transparent markets. Brokers serve

[4] see: section 2.3.2

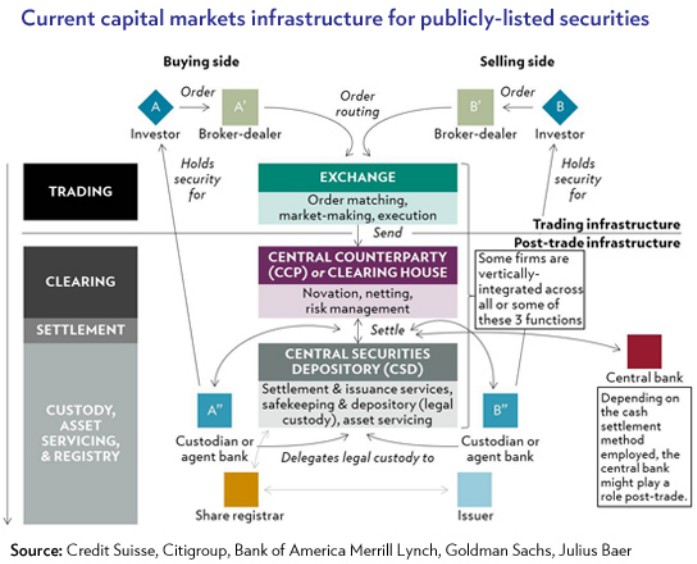


Figure 2.1: *Overview of the capital markets*

as intermediaries that trade on behalf of their clients, they generally do not trade on their "own book". Instead they execute orders on behalf of their client and do not trade for their own gain, earning money through fees instead. Some brokers combine their brokering activities with their own trading activities (often referred to as broker-dealers). Brokers also commonly provide market access for (retail) investors that can not directly access a market. Aside from retail investors which have market access via brokers there are also institutional investors like insurance companies, pension funds and investment banks. These institutional traders will often trade independently without a broker, though they may employ one in some cases.

Trading markets

Instruments are traded on one or more venues. A single instrument can be traded on multiple venues, this can give an issuer access to different pools of investors and promote liquidity of the instrument.

Exchange An exchange (also called a regulated market) is the classic example of a trading venue. This is a centralised venue for trading that will receive orders on registered instruments and match them according to a pre-defined rule book. Exchanges will deal with both issuers (primarily for IPOs) and investors. Exchanges have trading members that can trade directly on the exchange, non-members will have to use an intermediary (commonly a broker) to access the market.

Exchanges will have predefined rules on how orders are matched. These rules will be executed through automatic electronic algorithms, replacing the old system of brokers on the floor. They will have one or more order types: like limit[5] and market[6] orders and one or more matching strategies like continuous order book [7] or a periodic auction[8].

Over-the-counter (OTC) OTC refers to instruments not traded on a regulated trading venue. There is no central organisation listing prices and matching investors. Brokers and other intermediaries are important here as they provide price quotes and facilitate the matching process. The process of coming to a trade is generally handled via phone or email communication. More recently attempts have been made by regulators to gain more insight and oversight of these markets[9]. Transactions made in these markets in the EU have to be reported to a "trade repository", which maintains an overview of all transactions. These trade repositories also serve to increase transparency in general, providing other market participants with market data on markets that are traditionally less transparent. The emergence of online listing and matching platforms to find counter-parties has also increased the transparency of these markets. Derivative contracts are commonly traded on OTC markets. Many exchanges will offer the option to trade derivatives contracts, however these will be standardised contracts (in terms of type, dates etc.). Contracts traded on OTC markets can take on many different forms.

MTF, OTF & ATS Traditionally exchanges in the EU and US held a somewhat monopolistic position. There were only one or a few per country. To encourage more competition in this market, the EU (Multilateral Trading Facility and Organised Trading Facility) and US (Alternative Trading System) have introduced new types of venues. These are less heavily regulated and often have a lower barrier of entry

[5]For limit orders an investor provides an upper (for buy orders) or lower (for sell orders) limit to the price.

[6]Market orders will trade against the current market price without limits.

[7]In the case of a continuous order book incoming orders will be matched with existing orders in the book in the order they come in. If no match (or a partial match) is made, the order will be added to the book.

[8]In the case of a periodic auction, orders will be added to the book without matching for a certain period of time. When the auction is executed a price will be calculated at which the highest volume can be traded (the exact auction algorithm varies by venue).

[9]In the case of the EU this is implemented in various directives and regulations like: MIFID2 & EMIR, see: subsection 2.3.3.

for issuers. This allows many instruments that were formerly only traded OTC to be traded on trading venues instead. An MTF functions similar to a regulated market (it is non-discretionary) while an OTF allows for discretionary control. This means that an OTF may hold on to orders even if there are matching orders, if it believes it can create a better deal.

Execution No matter the type of venue used; eventually a buyer and seller will agree to trade or match in an order book depending on the type of market. Trade confirmations will be sent to the parties involved in the trade and the post-trade process starts.

2.3.2 Post-trade

Pre-trade and trading consists of all the actions up until execution. Execution of the trade is the creation of a legally binding agreement between two parties to exchange certain financial assets[10]. After this the assets still need to be exchanged. Until both parties have full ownership of their new assets there is a certain amount of risk that the other party can not meet their obligations at the time of settlement. The current infrastructure is focused on reducing the risks associated with this delay in settlement.

It is important for the stability of the financial markets that the number of failed trades is small. Even if we have Delivery vs. Payment (DvP)[11] and an investor does not have any risk of losing their assets; a failed trade is still a problem. If an investor wants to buy or sell an asset and the trade fails they are stuck with their assets. This may in turn mean that they cannot meet their own obligations in other trades leading to more failed trades. Depending on how connected a market is, this can have an epidemic effect destabilising the financial system.

The process after the execution of a trade (post-trade) is (broadly) split into two steps: clearing and settlement.

[10] In the case of securities trading this will almost always be cash vs. securities. In some cases it may be an exchange of securities vs. securities.

[11] see: section 2.3.3

Clearing

Clearing consists of several activities between the execution and settlement of a trade. The purpose of these is to calculate the actual obligations the counter-parties have to each other and make sure that any required assets are in place, so that a trade can be settled. In all cases settlement instructions are exchanged between parties. In some cases an additional step is included where the parties can manually confirm these instructions. These settlement instructions will contain most of the information contained in a trade, notably: quantities and prices of instruments, amounts of money, the identifier of the product and the identifiers of parties involved. In addition they contain settlement specific information like the accounts from which assets have to be transferred and the accounts to which they have to be transferred. Each party involved in the clearing and settlement process will individually submit their settlement instructions to the party responsible for settlement and they will need to be matched[12]. This process can fail if instructions do not match or if one party does not submit instructions at all. In these cases both parties will have to investigate which party is incorrect.

In many cases parties will not settle trades bilaterally, instead a third party will step in between the two parties. This party is known as a Central Counter Party (CCP). The CCP will act as the counter-party to both parties involved in the trade and will guarantee delivery and payment to either side. This reduces the risks for both parties, even if one fails to comply with their obligations the CCP will ensure that the other party receives its payment/delivery. This is done through a legal process called novation[13]. If the trade was executed on a trading venue the two counter-parties may not even be aware of each other as the CCP steps in immediately after execution using a legal process called open-offer[14].

The risks here are not eliminated but transferred onto the CCP. In exchange for their services the CCP will have fees and ask for a collateral (this could take the form of securities, money or other financial assets), which is commonly referred to as a

[12]This is not to be confused with the matching happening at an exchange, in this case the goal is not to come to a trade but to make sure that the required information matches on both sides so the trade can be settled.

[13]In the case of novation an existing bilateral contract is replaced with multiple new contracts with a CCP. The legal background is further described in a paper by Chamorro-Courtland, C. [9].

[14]In the case of open-offer no bilateral contract between the two counter-parties will exist at all. From the moment of execution both counter-parties will have a contract with the CCP. The legal background for this process is described by Chamorro-Courtland, C. [9].

margin. In the case of derivatives the collateral may be recalculated and adjusted over time as the period between trade and settlement is much longer and prices and market values can change over that period. The firms making use of a CCP's services will be "clearing members" of the CCP, pooling funds and other collateral into a single large fund that can be used for emergencies. In addition to the contributions by members the CCP is mandated to have its own reserves for emergencies (see Figure 2.2). Non-members will have to access a CCP's services through a clearing member.

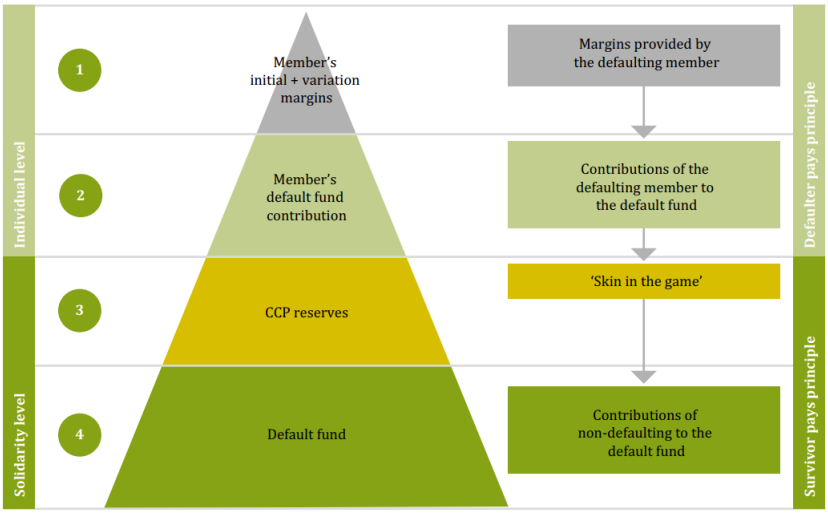


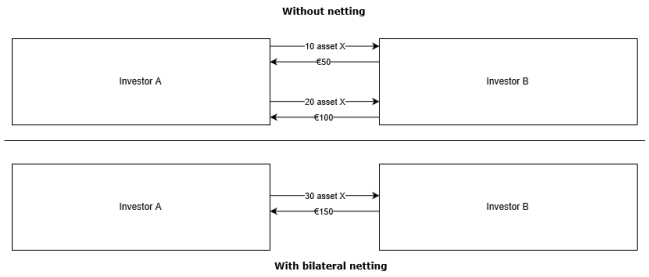
Figure 2.2: *Source: AFME*

In addition to serving as a central counter-party the CCP can opt to net trades. In this case it can calculate a member's final position over multiple trades and only settle these differences. This can reduce the amount of required settlements and thus increase efficiency.

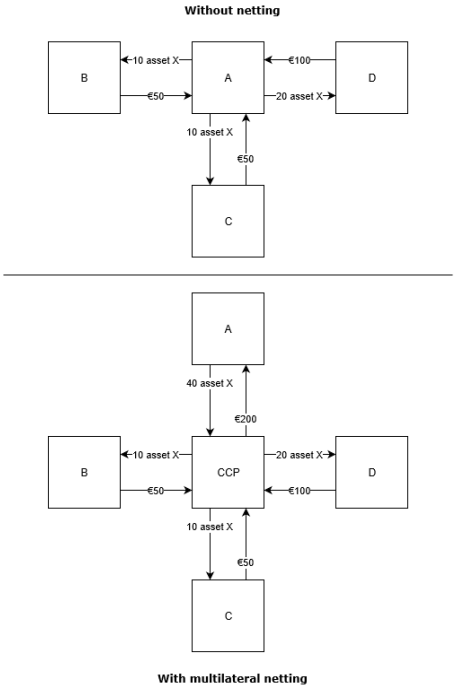
A simple example of netting without a CCP (bilateral netting) would be: investor A buys 10 of an asset from investor B, than later buys 20 of that asset to investor B, at the end (of the day) investor A would only need to make one transfer of 30 instead of 2 separate transfers (see Figure 2.3a).

An example of netting with a CCP (multilateral netting) would be: party A has 2 trades for 10 of an asset with parties B and C as well as for 20 with D, all with the same CCP. Normally A would have to individually settle with 3 different parties, however in this case it would only have a single settlement with the CCP (see: Figure 2.3b).

Exchange traded instruments will always be cleared with a CCP. For OTC traded



(a) Bilateral netting



(b) Multilateral netting

Figure 2.3: Netting

instruments it used to be more common to settle without a CCP. After the financial crisis steps have been taken by regulatory authorities in the EU to encourage the use of CCPs for OTC traded instruments[15].

Settlement & Custody

A trade has two dates. The transaction date when the trade was made and became legally binding and the value date (also called the 'intended settlement date', or just 'settlement date'). The value date is when the final exchange of assets will happen. The value date is generally written as: $T+x$. Where T is the transaction date and x a number representing the amount of days after the transaction date. For common securities (e.g. bonds or shares) the value date will generally be: T+1, T+2 or T+3[16,17]. For derivatives this is a bit more complex as it is possible to have multiple payments over a duration, leading to multiple clearing and settlement processes which are often significantly later than T+3. In the case of derivatives there are also two types of settlement: delivery and cash. In the case of delivery the underlying asset will be

[15] see: section 2.3.3

[16] These trades are also known as spot trades.

[17] Different jurisdictions may have different rules for this depending on the type of security.

delivered. In the case of cash settlement the price difference between the derivative price and current market price will be paid out[18].

There are two main parties involved with the securities settlement process. The first (and most important) one being the Central Securities Depository (CSD) and secondly the custodian. The purpose of custodians is to hold securities for safekeeping. In the past these could be paper securities (certificates), nowadays though these are mostly recorded in digital form. Custodians are most often banks. Their role is somewhat similar to what a normal bank would do for money[19]. Custodians traditionally operate in a certain financial centre and will service assets in that area. There are also global custodians which can offer custody services for many different financial centres. These global custodians will then have several sub custodians (local custodians) in each centre that will hold assets for that centre at a CSD (see Figure 2.4).

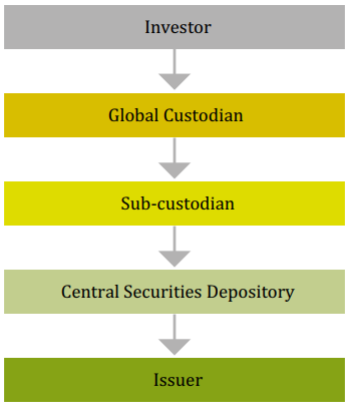


Figure 2.4: *Source: AFME*

A major difference between depositing money and having securities in custody is that in the case of depositing money the bank effectively borrows money from the account holder. They can then use it as they see fit, often to make investments or give out loans[20]. In the case of the insolvency of a bank, account holders may lose (some of) their deposit. Custodians are required to store securities segregated so they are not affected by insolvency and can not be loaned out without permission of the owner.

[18] Assuming investor A has a futures contract with the right to buy 100 potatoes at €0.50 per potato from investor B and at the settlement date the market price of a potato is €0.80; in this case a cash settlement means investor A receives $100 * 0.30 = 30$ euros from investor B.

[19] They do not have any ability to issue new securities though, while a bank can issue new money.

[20] This is a oversimplification of how money is created and loaned out, banks don't loan out existing deposits, but create new money when giving out a loan.

Custodians will often also offer general servicing of securities, handling settlements and corporate actions.

When two clients of the same custodian engage in a trade this is easy to settle for the custodian, it can be settled internally[21]. A simple book entry is all that is required for the securities leg of a trade. When more than one custodian is involved it becomes more complicated however. This is where the CSD comes in. A CSD is a custodian of custodians. CSDs are ultimately responsible for settling trades and the safekeeping of securities. Custodians will hold accounts with a CSD and when transactions with clients of multiple different custodians happen, the accounts at the CSD will be used. CSDs are considered a key financial market infrastructure and have their own regulatory requirements. In the EU the CSD regulation accepted in 2014[22] provides regulation for CSDs. CSDs generally exist at a national level. For example the main CSD for the Dutch markets is Euroclear Nederland.

Settlements involving CSDs still entail a simple book entry in the systems of the CSD. In addition to this the cash leg of a trade also has to be settled. In some cases this is handled by the CSD itself if it allows its participants to hold cash accounts with the CSD, in other cases accounts at a central or commercial bank will be used. If it turns out that a party cannot meet its obligations during settlement there are two options: either the trade fails or the party has to lend cash or securities[23] to meet its obligations. It can then later try to reacquire the borrowed asset to repay its loan.

CSDs are also involved in the issuance of new securities. When a new security is issued and registered at a CSD the issuer will choose the CSD where it is registered. That CSD will be responsible for holding these securities. They are responsible for checking that the number of securities in circulation matches what was originally issued. When a cross CSD transaction has to take place, it will generally be handled by one CSD having an account with the other CSD. The investor-CSD will hold the securities in their account at the issuer-CSD in a similar manner to a non-CSD participant. Participants of the investor-CSD can then indirectly hold securities at another CSD without being a participant of that CSD.

Participants themselves will also often hold omnibus accounts. This means that a

[21] In EU regulation this is called a internalised settlement and the entity doing so is a settlement internaliser: a non-CSD that handles transfer orders.

[22] see: section 2.3.3

[23] In the case of securities this is called short selling.

participant will hold a single account for all its clients and the CSD will be unaware of the underlying clients and beneficial owners. Participants will have their own books with accounts for their clients. Most CSDs will also offer segregated accounts, either by client or by beneficial owner. This distinction is relevant where the client of a participant is another intermediary. Some EU member states mandate the use of segregated accounts by beneficial owner. There will still be an intermediated structure, but the participants will manage multiple different accounts, a different account per beneficial owner.
According to a report published by the ECSDA in 2015 [10], the exact regulation of account segregation still differs per member state as it depends upon member state law. An exception will generally be made for CSD-links where investor-CSDs hold omnibus accounts at issuer-CSDs which will be allowed even if normal omnibus accounts are not allowed.

Both CCPs and CSDs have close ties to the various European exchanges:

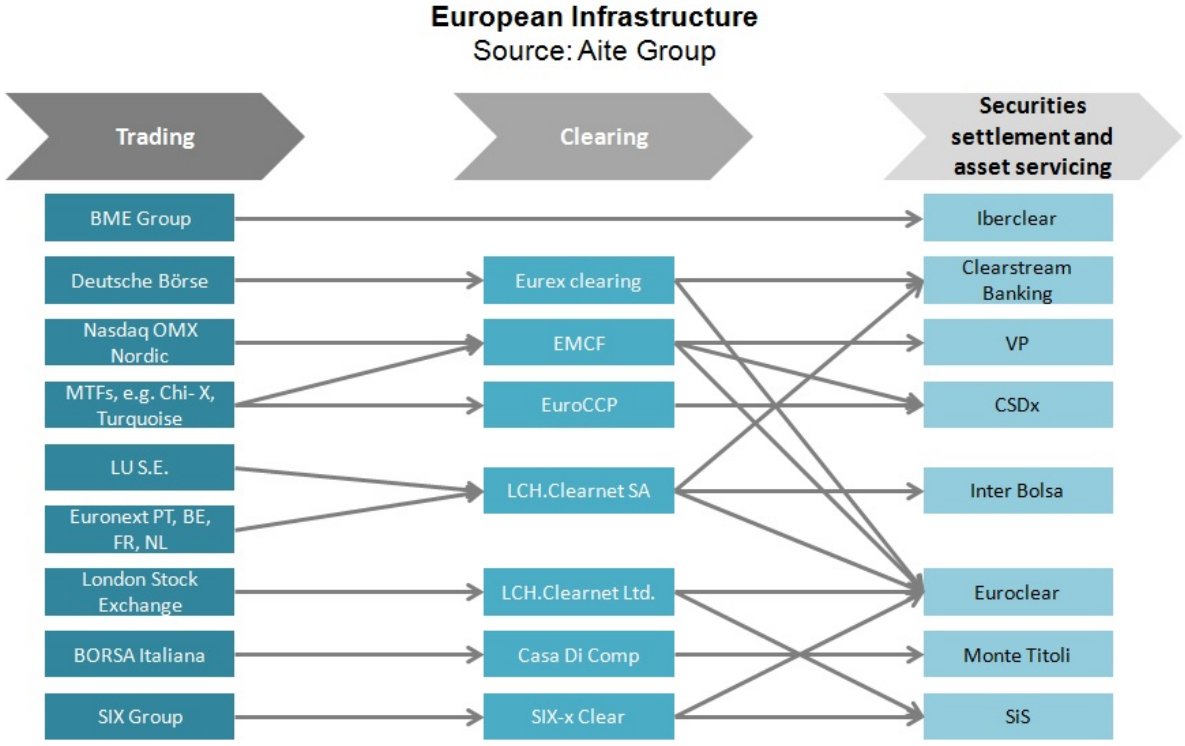


Figure 2.5: *Source: Aite Group [11]*

Registrar

In cases where the securities are registered (i.e. non-bearer securities) they have to be registered in a register. This register is different from the accounts held at a CSD. The register is leading when it comes to corporate actions and investors exercising their rights. The register holds the identities of the beneficial owners of the securities (the share/bondholders). In some cases it may not be the beneficial owner that is registerd, but another party acting as a "nominee". In practice the task of a registrar is often performed by CSDs who will maintain the register. The register can also be maintained by the issuer itself or an (issuer) agent acting on their behalf. If the CSD maintains the register it can enable (near) real-time updates of the register, though this is not mandatory. Registers can also be updated periodically or at request of the issuer. The registrar does not have to be the issuer-CSD: according to a report by the ECSDA in 2016 [8] the CSD is involved in the maintenance of the register in 76% of the European markets either as the sole maintainer or in cooperation with its participants which will have their own accounts for their clients. In the case of bearer securities the CSD may still maintain an "informal" overview of shareholders. However this is not a real register.

Corporate actions

Corporate actions are not a part of the settlement process, but are a task that's generally handled by registrars, CSDs, custodians and other intermediaries as part of their post-trade services. Corporate actions are all the activities affecting the holders of a security. One example of this is a dividend payment, for other examples see Figure 2.6. When a corporate action is issued the issuer of the security will inform the registrar. The registrar will then inform all registered or bearer holders of securities. These will then inform their clients, continuing on until the investor is reached. If the corporate action requires a response (e.g. in the case of voting) the investor will inform their custodian, who will go back up the tree until the registrar and finally the issuer is informed.

2.3.3 (European) Regulation

Most financial market infrastructures are organised on a national level. This chapter (and thesis in general) will focus primarily on the situation in the EU. The EU is not

Corporate actions on stock	Types of corporate actions
Distributions: CAs whereby the issuer of a security delivers particular proceeds to the holder of the underlying security without affecting the underlying security	**Cash distribution:** a distribution where the proceeds consist of cash only (e.g. cash dividend, interest payment) **Securities distribution:** a distribution where the proceeds consist of securities (e.g. stock dividend, bonus issue) **Distribution with options:** a distribution with options is handled as two events: i) a distribution of intermediary securities (see securities distribution above) followed by ii) mandatory reorganisation with options (see below) (e.g. optional dividend)
Reorganisations: CAs whereby the underlying security is replaced with proceeds	**Mandatory reorganisation with options:** a mandatory reorganisation with a choice of proceeds (e.g. conversion) **Mandatory reorganisation:** a reorganisation that mandatorily affects the underlying security (e.g. stock split, redemption) **Voluntary reorganisation:** a reorganisation in which participation is optional for the holder of the underlying security (e.g. tender offer)

Figure 2.6: *Source: T2S Special Series | Issue No 3 | January 2014 | Corporate actions in T2S [12]*

a nation, but much of the regulation for the financial markets has been moved from a member state level to the EU in order to create a shared and harmonised financial market in the EU. Much of this applies to the US and other countries as well, as many countries have based their regulation on the principles for financial market infrastructures (see section 2.3.3). Many of the roles described below (like CSD and CCP) tend to be more centralised and less fragmented in the US then in the EU. It is also important to note that depending on the specific instrument being traded and the parties involved the exact process and regulation may differ.

Principles for financial market infrastructures The principles for financial market infrastructures [13] (PFMIs) are a set of principles defined by the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) in 2012. These are a set of international standards that form the basis of much of the recent regulation by the EU (and also in e.g. the US). It contains guidelines and considerations on minimising various forms of risk to improve the stability of the financial market infrastructures (FMIs).

One of the considerations is the need for a clear legally defined moment of 'settlement finality' as defined in principle 8 of the PFMIs. This is the point at which a transfer order or transfer is irrevocable. This is important in the case of a bankruptcy as it needs to be clear whether or not a transaction will still be settled. It is important to note that this does not necessarily need to be the moment cash and securities are

exchanged. For the EU this is defined in directive 98/26/EC[24]. Aside from the legal basis another recommendation is for FMIs to have a clearly defined moment for settlement finality in their internal systems.

The PFMIs also recommends the usage of DvP (Delivery vs. Payment) in principle 12. It is defined in the PFMIs as: *"DvP is a settlement mechanism that links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding funds transfer occurs"*[25]. This does not mandate simultaneous atomic transfers of cash and securities (though that is one solution). The only thing that is important is that neither party should have the risk of not receiving their cash/securities[26].

Another recommendation is made regarding money settlement, as defined in principle 9. Which recommends using central bank money[27] to settle trades and only settle in commercial bank money[28] if settling in central bank money is not feasible. This is because of the higher creditworthiness of central banks (it is less likely a central bank will become insolvent).

Anti money laundering (AML) & terrorist financing The exact nature of AML regulation differs per jurisdiction. In the case of the EU it concerns directive 2015/849 [14](the 4th EU AML directive) and the amendment directive 2018/843 [15](the 5th EU AML directive).

The purpose of these directives is to combat criminal activity related to financial transactions including fraud, tax evasion and terrorist funding. It provides guidelines for 'gatekeepers' to the financial markets. Specifically in addition to applying to credit institutions (banks) as defined in Article 2(1) sub-paragraph (1), it also applies to financial institutions, as defined in Article 2(1) sub-paragraph (2). In practice this encompasses all parties involved throughout the lifecyle of trade. Specifically it includes parties involved in: "safekeeping and administration of securities" and "safe

[24] see: section 2.3.3

[25] DvD (delivery vs. delivery), in the case where securities are exchanged. PvP (payment vs. payment), where only cash is exchanged. And FoP (free of payment), where securities are transferred without payment, also exist and are similarly defined.

[26] This is known as principal risk.

[27] Central bank money means physical cash (coins and banknotes) and deposits held at a central bank. Holding an account directly at a central bank is generally only an option for FMIs like banks, brokers, custodians and CSDs. Central bank money is a central bank liability.

[28] Commercial bank money means deposits held at a commercial bank. In this case it is the commercial bank and not the central bank that owes the account holder money.

custody services" applicable to custodians and other intermediaries in the holding chain. "Participation in securities issues and the provision of services relating to such issues" and "safekeeping and administration of securities" apply to CSDs as well as registrars. The counter-parties in a trade will generally be financial institutions as well: such as brokers, investment firms or insurance companies, which are subject to the directive as well.

These institutions are required to take "customer due diligence" measures. This requires them to investigate new clients and the final beneficiary owners of those clients. In addition to this similar requirements apply to occasional transactions of a sufficiently large volume (€15000 or €10000 for cash) as defined in Article 11. In practice these volumes often apply to securities trades, T2S[29] for example settles 600,000 transactions per day on average with a total value of €578.07 billion, this gives an average transaction value of €963,450.

Measures taken for customer due diligence are defined in Article 13 and Article 20 and include: the need to identify the customer and where applicable the beneficial owner(s). This second requirement is applicable to companies, where it is important to determine the persons that are ultimately owning the company. Furthermore if a business relationship is started the purpose of the relationship has to be determined and should be used to monitor the behaviour of the client to determine if its behaviour matches what is expected from such a client. In addition to this it is mandatory to check if the customer or its beneficial owners are (or are related to) politically exposed persons (PEPs).

The directive provides room for member states to make exceptions for simplified or enhanced customer due diligence in certain cases. The exact implementation of this is left to the individual member states, but some examples are mentioned in the Annexes of the directive. Enhanced or simplified due diligence may apply depending on the country where the client/counterparty is from, low-risk countries are (among others): the EU member states. High-risk countries are countries with high levels of corruption or that have terrorist organisations operating within the country. Simplified due diligence is also applicable where technologies or products are used with a high

[29]T2S is a securities settlement system developed and operated by the ECB and several national central banks of EU member states. It is not a CSD itself but a common platform to be used by EU CSDs to create a more harmonised and standardised settlement system. Most CSDs in the EU use T2S for the settlement of securities.

degree of transparency of ownership. In contrast enhanced due diligence would be applicable where the product is inherently anonymous (traditional physical bearer securities would be an example of this) or new technologies/products are used.

Articles 25, 26 and 27 specify that obliged entities may rely on other obliged entities to handle their due diligence provided that those other entities apply due diligence as required by the directive. In practice this means that in large holding chains not all due diligence activities would have to be duplicated, entities are only responsible for their direct clients/participants. Full responsibility still stays with the original entity.

Amendment directive 2018/843 also contains specific references to virtual currencies as often seen on blockchains. Article 3(1) sub-paragraph (c) extends the list of applicable entities with virtual currency exchanges and custodian wallet providers.

Individual member states have their own specific implementation of this directive[30]. As such the exact requirements regarding customer due diligence differ per member state.

CSD regulation The CSD regulation (Regulation No 909/2014 [16]) concerns the settlement of securities ('settlement service') and specifically the role and requirements of CSDs. A CSD is here defined as: *'central securities depository' or 'CSD' means a legal person that operates a securities settlement system referred to in point (3) of Section A of the Annex and provides at least one other core service listed in Section A of the Annex.*

The three services of Section A are:

- *Initial recording of securities in a book-entry system ('notary service');*
- *Providing and maintaining securities accounts at the top tier level ('central maintenance service');*
- *Operating a securities settlement system ('settlement service')*

Article 3 stipulates that all transferable securities traded on trading venues are settled in a CSD and Article 18 specifies that only CSDs are allowed to operate securities

[30]For example: the Netherlands has the WWFT (wet ter voorkoming van witwassen en financieren van terrorisme).

settlement systems. All other financial instruments also have to be recorded in electronic book-entry form but do not have to be recorded at a CSD (the issuer itself or an agent acting on its behalf could fulfil that role).

The regulation provides guidelines for settlement. CSDs have to settle all trades at the intended settlement date. They are also responsible for penalising parties that cannot meet their obligations (i.e. parties that cause trades to fail). These penalties would at first be cash penalties, but could eventually lead to eviction of repeat offenders as defined in Article 7. It also limits the intended settlement date for securities traded on trading venues to T+2 in Article 5.

The regulation also contains a definition for 'settlement internalisers': *'settlement internaliser' means any institution, including one authorised in accordance with Directive 2013/36/EU or with Directive 2014/65/EU, which executes transfer orders on behalf of clients or on its own account other than through a securities settlement system.* This applies to custodians and brokers that will often settle trades between clients internally without the involvement of a CSD when holding an omnibus account at a CSD. The only requirement put forth by the regulation is a quarterly report of settlement activity to relevant authorities. It is worth noting that these parties will need to maintain accounts at a CSD if settling trades in transferable securities, as the CSD is ultimately responsible for maintaining accounts and executing transfer orders.

CSDs have to be authorised by the relevant authority of their member state[31]. CSDs are allowed to outsource their activities including their core activities to other parties as defined in Article 19, but will have to submit a request for authorisation if this is the case. This is also the case when they wish to establish a link with another CSD or if they want to establish a relationship with another settlement agent to handle the cash leg of a trade. Article 30 expands upon the requirements for outsourcing by putting forth some additional requirements. This includes the fact that the relationship between the CSD and its clients (participants and issuers) should not be altered, it should not impede authorities and supervisors in their tasks (third parties should cooperate with them) and the CSD should be able to properly manage its risks. There are two exceptions to the aforementioned:

- These requirements may not apply when the tasks are outsourced to a public entity

[31] For example the "Autoriteit Financiële Markten" (AFM) for the Netherlands.

- Other parties may record transactions if it is explicitly required by member state law

MiFID2 The MiFID2 directive [7] focuses primarily on the pre-trade and trading processes. Providing rules for exchanges and other trading venues and for investment firms and brokers. Its primary aim is to enhance investor protection and to improve the transparency and regulatory oversight of the financial markets.

MiFIR MiFIR [17] is the regulation that accompanied the MiFID2 directive. Like MiFID2 it focuses more on trading venues and investment firms, but also contains some articles that have relevance to post-trade activities.

Article 23 requires any trades in shares admitted to public trading on a trading venue to be executed on an authorised trading venue as defined in MiFID2. This effectively mandates that shares in any publicly traded company should be traded on a regulated trading venue and should also be settled at a CSD. A similar trading obligation is defined for certain classes of derivatives in Articles 28, 32 and 34. As of the time of writing (June 2019) this primarily concerns some classes of interest-rate swaps and some classes of index credit default swaps [18]. Article 29 also mandates a clearing obligation for the aforementioned derivatives. This means that these derivatives have to be cleared using a CCP.

EMIR The EMIR regulation [19] focuses on clearing by CCPs and OTC traded derivatives. The main goal is to provide stricter rules and more transparency for OTC trade derivatives and establish requirements for CCPs.

Article 4 mandates a clearing obligation for many classes of OTC traded derivatives. As of the time of writing (June 2019) this includes various classes of interest rate, equity, credit and foreign exchange derivatives [20]. This means these classes of derivatives have to be cleared by a CCP. Any other OTC derivative contracts not subject to the clearing obligation have to use appropriate risk-mitigation techniques including bilateral confirmation of the trade, exchange of capital and monitoring of market values of the contract.

In order to increase the transparency of the derivatives market which are traditionally very opaque as trades are primarily executed and settled bilaterally, the regulation also mandates a reporting obligation in Article 9. This requires all derivatives trades

to be reported to a trade repository so that trading venues, supervisors and other interested parties have insight into these contracts.

Similar to the CSDR for CSDs, EMIR requires all CCPs to be authorised and includes various requirements and rules for CCPs. These include rules regarding the outsourcing of their activities which are similar to those for CSDs. Specific to CCPs is the need for various forms of collateral to limit the risks it is taking on itself. These rules are defined in articles 41-48. It includes gathering margins from its members for individual transactions as appropriate for those transactions and also a default fund made up of contributions by members to be used in case of emergencies. A CCP also has to maintain a decent amount of its own capital as a final fallback.

Settlement finality Settlement finality[32] is an important concept to reduce systemic risk in the case of insolvency. The EU has defined when settlements are final in Directive 98/26/EC [21]. It defines finality as: "Transfer orders and netting shall be legally enforceable and, even in the event of insolvency proceedings against a participant, shall be binding on third parties, provided that transfer orders were entered into a system before the moment of opening of such insolvency proceedings as defined in Article 6(1).". In this context "system" refers to a securities settlement system. This means that a settlement will be considered final before actual transfer of cash and securities has taken place. This does not prevent failed trades in events where one counter-party cannot perform its obligations. It does prevent failed trades due to the insolvency of one of the counter-parties, provided that cash and securities are present. It also means that in cases where a CCP is used the CCP will have to perform its obligations as a central counter-party.

2.3.4 International standards

With all the parties involved, having standards for communication is important for the whole infrastructure to function efficiently. There are currently two main communication standards being used: FIX [22] for pre-trade/trade and SWIFT [23] for post-trade. There are also several standards for identifiers used throughout the trading process including: ISIN [24], LEI [25] and BIC [26].

[32] see: section 2.3.3

FIX FIX is primarily used to standardise communication in the pre-trade and trading segment, everything up to and including execution. It is used by brokers and other investment firms to send orders to brokers and trading venues. And by trading venues to send information on trade execution back to interested parties. FIX is a messaging standard, unlike SWIFT it is not a network. Users are required to setup their own connections and sessions.

SWIFT SWIFT is both a network and messaging standard for post-trade settlement. This is not just for securities settlement, but is also used for e.g. international payments. The messaging standard is an ISO standard: ISO20022 [27]. In addition the SWIFT Foundation also runs a proprietary network providing connectivity between parties. The SWIFT or BIC codes used to identify banks originate from SWIFT as it are the identifiers used by the network. The SWIFT Foundation is owned by a conglomerate of banks, it is a non-profit organisation.

ISIN International Securities Identification Numbers (ISINs) are unique identifiers for securities. The format is specified in ISO6166 [24]. Though not mandatory for securities, an identifier is required when reporting trades to various regulatory authorities. As such ISIN identifiers have become more common over time. The organisation which is ultimately responsible for the issuance of ISIN codes is the Association of National Numbering Agencies (ANNA). Though in practice this task is delegated to various National Numbering Agencies in individual countries. These agencies will often be that country's CSD.

LEI Legal entity identifiers (LEIs) are unique identifiers for institutions participating in the financial markets. The format is specified in ISO17442 [28]. This identifier is currently required for all parties involved in financial transactions in the US and EU, because the LEI is required when reporting transactions to the relevant authorities.

BIC Another identifier used to identify parties involved in post-trade activities is the bank (or business) identifier code (BIC), also known as the SWIFT code. The format is defined in ISO standard 9362. BIC codes are issued by SWIFT and are commonly used on the SWIFT network to identify parties.

Chapter 3

Blockchain

Defining "the blockchain" can be hard to do. There are many different applications that call themselves blockchains. So for this initial description we will focus on public permissionless blockchains like the one used by Bitcoin. This will be followed by describing various alternatives, like permissioned and/or private blockchains. It is worth noting that some argue that some of these different types of blockchains are not "blockchains", but are distributed ledgers instead and that the blockchain is one particular example of distributed ledger technology. Exactly when something is a blockchain is not entirely clear yet though.

A blockchain is at its simplest a decentralised and distributed data-structure. Traditionally data on the internet will be stored centrally with a single controller. An example often used is a bank, which controls your data (your money), what you can see and what you can do. Similarly CSDs keep and update the ledgers on ownership of publicly traded securities. By doing so they also control what you can do with your money (or securities). Similar arrangements can be seen in different fields. Even if you are cooperating with others, e.g. using Google docs, it is still ultimately Google who controls the data and determines how it can be used. This does not mean that the data is stored and processed on a single server. Popular applications will often use distributed databases spread over many nodes to improve performance and/or availability of a system. These databases will still ultimately be under the "control" of a single entity though.

The need for this centralised control (at least for financial applications and other applications that track ownership) is related to the double spending problem. When I own a physical object I can show it to others to prove that I have it and give it to them

to transfer ownership. That does not work for digital objects. I can claim that I own something even if I do not and create an infinite number of copies of some piece of digital data that I did own at some point. Traditionally this is solved by appointing a single party (or limited group of parties) to maintain an overview of ownership of a certain type of data. We can then ask that party to transfer ownership of this data. If more than one of these parties exist for a certain type of data, some form of interoperability is required to make sure that their respective ledgers stay in sync.

With a blockchain there is no such central party. Every participant controls its own node(s) and whenever some action happens each participant individually executes the steps necessary to update its local copy of the data. This allows us to maintain our own version of the ledger. This only works if all participants have the same (local) state. When new transactions that change this state come in, it is easy for every participant to check if this new transaction is correct according to the invariants of the application and to then apply state changes according to the rules defined in the application. Unfortunately due to the inherent unreliability of network connections (individual nodes may receive transactions out of order or not at all if they are offline) keeping all nodes consistent is a non-trivial problem.

Because of the unreliability of the network, maintaining a consistent state among a distributed set of nodes (computers or other digital systems) is hard to do. To illustrate this consider an example of three nodes (A,B and C) keeping a shared ledger of their ownership of some asset. Assume a starting state that is consistent among nodes where A owns 10 of this asset. If A were to then broadcast its intent to transfer 10 to B to both other nodes (or to one node which would broadcast it to the other), the resulting state would be consistent among nodes. Each node would individually update its state to assign the 10 assets to B and remove them from A. But if A were to send a message to B, specifying a transfer to B and at (roughly) the same time send a message to C, specifying a transfer to C, a choice would have to be made. Assuming that B and C simply act on the first message they receive the system would be in an inconsistent state as B and C both think themselves the owner of the asset. Even if they later receive the other conflicting message they will (in this naive setup) simply reject it as invalid. Solutions to this problem have existed for a while (in the form of consensus protocols which can handle various types of faults), but until the creation of Bitcoin these solutions always assumed a trusted setup with a limited set of nodes.

On the blockchain consistency is maintained through the data structure used by a blockchain, combined with a consensus algorithm. At the core of this data structure are the transactions. The exact structure of a transaction differs per implementation, but it is essentially an instruction for a state change on the blockchain (often a transfer of ownership of some asset). Each participant will have a public and private key (or multiple pairs). They can use their private key to sign a transaction and other participants can then use the corresponding public key to verify it, this enables a participant to prove that the transaction was signed by them. Most blockchains associate ownership of some piece of data with an address. This address is derived from a public key in some way[1]. By signing a transaction with the private key belonging to an address a participant proves ownership of that address (and the associated private key). These signatures serve to authenticate the user taking the action and since they are part of the blockchain's state they also provide non-repudiation of transactions.
A group of these transactions is collected into a block and new blocks are added onto the chain. Every block in the chain contains the hash of the previous block. If an older block is modified the hash of that block changes. The block after that block held the hash of the original version of the now modified block and as such is no longer a valid successor of that block. This effect cascades throughout the chain invalidating all blocks afterwards. In order to modify a block earlier in the chain all blocks afterwards would have to be recreated with the proper block hashes and added to the chain.

The process of adding a new block is handled through a consensus algorithm. The most common one at the time of writing this thesis is Proof-of-Work (PoW) combined with the longest chain rule. For Proof-of-Work participants have to win a computational lottery[2], to gain the right to add one new block to the chain[3]. Consensus is then achieved by selecting the chain with the highest amount of cumulative work invested[4]. Proof-of-Work on its own is not a consensus algorithm, instead it is more accurately described as a sybil resistant[5] leader election algorithm or alternatively a

[1]Often by hashing the public key and adding some additional (checksum) bits.

[2]In the case of bitcoin this entails adding a nonce to a block such that the resulting block hash has a certain number of leading '0' bits. The exact number of '0' bits depends on the total computational power in the network.

[3]The block for which the participant calculated the correct hash.

[4]Often referred to as the "longest" chain even if it does not necessarily have to be the longest chain in terms of block height, difficulty adjustments every 'x' amount of blocks (roughly every 2 weeks for Bitcoin) can theoretically lead to a longer chain with less cumulative work.

[5]In the case of a sybil attack, someone creates a large amount of identities (or nodes in the case of a

rate limiting algorithm, it is PoW together with the longest chain rule that constitutes a full consensus algorithm, which is often referred to as Nakamoto consensus. PoW could be utilised with other consensus algorithms as well, for example Ethereum combines PoW with GHOST which extends the calculation of the canonical chain to include the work invested in "uncles" (forks up to 7 levels deep). In practice using PoW with some consensus rule based on the invested amount of work goes hand in hand.
This means that adding a block requires investing computational power into the network. This activity is called mining blocks (and the participants actively involved in this process are called miners). This discourages malicious behaviour as mining a new block takes a considerable amount of resources. If a block is invalid other honest nodes will simply ignore it and continue working on the valid chain and any energy invested in the wrong chain will be wasted. Miners are rewarded with a transaction fee and in some cases new tokens that are issued (mined) by the network. These networks are generally considered safe for double spending if no miner controls 51% of the total computation power[6].

What this allows us to do is to maintain a shared ledger of data without having a single party that verifies and updates the ledger. Reverting a transaction that has been added to the chain is difficult. It would require either a compensating transaction if the rules of the blockchain system allow that or it would require rewriting part of the chain. Rewriting (part of) a blockchain is hard because it requires achieving consensus on a (partially) new chain which is longer than the old one. In the case of Bitcoin that would mean calculating valid PoWs for all the new blocks added to the chain.

The initial concept was to utilise this technology to create a decentralised payment system, enabling people to make digital payments without the need for a bank. The implementation of this concept is Bitcoin. It is important to note that although a blockchain can be used to implement a payment system in a decentralised setting, it does not inherently do this. What it does is make a group of nodes maintain a consistent view of a long list of blocks. This then allows these nodes to have the same overview of the current state which in turn allows nodes to make decisions based on that single consistent state. What is then done with that state and what is and is

blockchain) to attack a system.

[6] A paper by Eyal and Gün Sirer [29] suggests that it would be vulnerable after 25% instead.

not allowed differs per implementation. In the case of Bitcoin it is used to transfer digital "coins" between participants. These coins are associated with an address on the chain and the owner of the private key associated with that address can transfer coins to other addresses. Every transaction will include a set of input coins and output coins. The input coins have to be output coins of previous transactions that have not been spent before. A transaction destroys a set of input coins and creates a new set of output coins. New Bitcoins are added into the system by rewarding the miner of a new block with a small amount of Bitcoins. These rules have been defined as part of the implementation of Bitcoin. It is possible to create a version of the Bitcoin software where outputs can be used twice as input though. It is also possible to have a version where transactions can only be signed by a single (or small group of) signers instead of the owner of an address. This can be done even if the blockchain is completely public and anyone can act as miner or validator.

Forks The chain of blocks is not a straight line, it is possible for multiple blocks to exist at a certain height in the chain. This is called a fork in the chain and can occur for three main reasons:

- A miner can mine blocks with invalid block headers (for example without a valid PoW) or containing invalid transactions. Other (honest) miners should discard these and not continue mining on these blocks. If a miner has more than 50% of the mining power they should be able to stay ahead of the "honest" miners forming a chain with more work as a result.

- It is possible for two (or even more) miners to mine a new valid block at (roughly) the same time. This will cause a fork as two valid versions of the ledger will exist. Nodes will always consider the longest version of the chain to be the valid one so in the situation of such a fork the nodes would have to wait until more blocks are mined and one of the forks grows longer than the other one[7]. Any mining power used on the other fork is effectively wasted as the mining rewards exist only on that fork and not on the longer fork which is now considered the "real" one.

[7] In the case of Bitcoin, nodes will continue to mine on the first (valid) block they receive, so different nodes would continue to mine on a different fork of the chain but the chance that a new block would again be mined on both forks at (roughly) the same time is very small.

- Another reason why a fork can occur is because of software updates. If a new version of the blockchain software is not compatible with the old one blocks produced by one version may not be accepted by the other version[8]. Because of this there can be two versions of the blockchain after such a software update (a chain split), with both versions diverging from each other over time.‘These software forks can be further divided into soft-forks and hard-forks. In the case of soft-forks the ruleset of the blockchain is altered so that blocks produced by the new version will be valid for nodes running the old version, but not vice-versa. For a hard-fork blocks produced by the old version will be valid for nodes running the new version, but not vice-versa. These forks do not necessarily have to lead to a chain split[9]. If a chain split does occur it may resolve itself in some cases as more nodes upgrade and the new version becomes the "canonical" version, in other cases barely any nodes upgrade and the new version is effectively discontinued. When the chain split does not resolve itself over time two new blockchains will exist with a shared history up to some point.

3.1 Smart contracts

Where the blockchain is essentially a database storing state with a default set of rules (the core protocol) as to how this state can be changed, many blockchain implementations have provided some way for other developers to extend the default functionality. These are called smart contracts and can be compared to the application code in traditional applications. Application code will check business logic and update data in the database. Smart contracts are similar but executed locally on individual nodes instead of on a single server. This allows for more applications than just the issuance and transfer of assets. Generally speaking nodes in the network can freely "deploy" new smart contracts onto the network. Any logic that can be added to a blockchain using a smart contract could also be added as part of the core underlying logic of the blockchain software itself. But that would require a software update and nodes would need to update their version of the blockchain software. When smart

[8]For example the signature format may have changed which means that the old and new version of the software will consider transactions signed by the other version invalid.

[9]For example: if there is more mining power for the new fork in the case of a soft-fork, the longest chain will conform with the new rules and will be considered the "canonical" chain for both versions.

contracts are "deployed" the smart contract code and internal state are added to the shared state of the blockchain with their own associated address. Participants can then "call" that smart contract, potentially with parameters if the smart contract specifies those. Calls to a smart contract have to be signed by the caller and are added to the chain as part of a block in the same way as a normal transaction. The node mining the block will execute the contract logic and the resulting state of the contract will become part of the blockchain state. Other nodes receiving the block will execute the smart contract as well to check its validity.

Smart contract languages are often "Turing complete", meaning they can solve most general computational problems and this should allow for almost any logic to be programmed as a smart contract[10]. A common use case for smart contracts is for participants to issue their own tokens[11] onto a blockchain.

It is important to note that these smart contracts are just code, with all the risks attached to code. A bug in a smart contract can potentially have unintended consequences and smart contract languages are generally not any "safer" than an average high-level programming language. If smart contracts were to be used in place of normal contracts careful auditing and testing would be required. Not just to ensure that there are no bugs in the code, but also to make sure that the code properly encodes the intended behaviour of the smart contract. Correcting these bugs is significantly more complex than in a traditional centralised application, due to the immutability and decentralised nature of a blockchain. Immutability does not necessarily prevent reversal of a transaction, traditional ledgers use compensating transactions and a blockchain can do the same, if it is allowed by the rules of the contract. An update to a smart contract would entail deploying a new version of it. As long as the interface of the smart contract stays the same there are ways to update a smart contract with minimal impact[12]. If the interface of the contract changes it would require all users to switch over to the new address however.

[10]The contract has to be deterministic however. If that is not the case, state transitions on a contract would have different results for different nodes. Decisions based on randomness and time are risky and can potentially lead to a divergence in the blockchain state between different nodes.

[11]Token is a generic term referring to some fungible or non-fungible asset with its ownership kept on a blockchain. Some of these tokens have similarities to securities and are used to raise funds. Others have some utility and can be exchanged for a service.

[12]For example by having a data and library contract, with the data contract calling the library contract and having some option for a contract owner to update the address of the library contract. This would give a backdoor to the developer of the contract to update the logic at any time however.

An example of a case where security issues caused a major hack is the DAO (Decentralised Autonomous Organisation), which was a decentralised venture capital fund[13] for blockchain related projects. Someone exploited a weakness in the code[14] to "steal" a large amount of Ether. This was "fixed" through a software update that caused miners to mine a block transferring the stolen Ether to a smart contract that could be used by investors to safely retrieve their Ether[15].

3.2 Permissionless vs. Permissioned & Public vs. Private

The original concept presented by Nakamoto [1] is of a public permissionless blockchain. Everyone can start a node and can mine new blocks. Transferring Bitcoins only requires a signature by the private key of the address, with no further approval by other parties. This provides the highest amount of decentralisation.

These permissionless systems are not without their flaws however. In theory there is no single party or group of parties in which participants put their trust. In practice however large mining pools hold a significant amount of the total mining power in a blockchain. In the case of Bitcoin there are 4 or 5 mining pools accounting for more than 50% of the hash rate at the time of writing (June 2019) [30] [31] [32], with roughly 20 miners being responsible for practically all blocks that are produced. These blockchains also require a significant amount of participants in order to ensure that the 51% is not within easy reach.

3.2.1 Scalability

Scalability is a major issue: the interval between new blocks and the size of those blocks is often restricted. This is important because the barrier to entry in terms of computing power has to be low enough for "regular" participants to keep up with the

[13] A pool of money gathered by different investors to be invested in various start-up projects.

[14] The internal state of the contract was updated after the ether was refunded to an investor. The refund was handled by calling an address supplied by the investor which could be a smart contract as well. That smart contract could call back to the DAO smart contract before the DAO internal state was updated, thus getting their refund multiple times and reducing the amount of ether in the DAO.

[15] Not all miners and participants agreed with this update and it led to a chain split and the creation of Ethereum Classic.

network. This requirement limits the potential throughput of public permissionless blockchains. Bitcoin for example produces a block every 10 minutes which can be up to 1MB in size[16]. In addition to this the inherent nature of the blockchain as a chain of blocks means that the size of the chain grows over time. The size of the bitcoin chain at the time of writing (June 2019) is roughly 225GB [33]. Furthermore there has to be some incentive for miners to do their job. Bitcoin currently handles this by rewarding miners with new bitcoins and transaction fees. The issuance of new bitcoins is going to stop at some point however and the transaction fees are driven by request and demand as miners can freely pick any transactions they want for a block. This incentivises them to pick the transactions with the highest fees. During periods with a high amount of transactions this can lead to high fees. For example the Bitcoin fees around the start of 2018 were over $30 [34]. In addition to this the amount of electricity consumed by PoW systems is very high due to the need for miners to be actively computing PoW hashes 24/7 [35] [36] to create new blocks and earn block rewards.

Some improvements to these issues have been proposed over the last years though most of these are not used at a large scale yet:

- Proof-of-stake (PoS): Proof-of-Stake is a different solution to choosing block proposers that is sybil resistant and currently the most often proposed alternative to Proof-of-Work. Some blockchains like NXT [37], Peercoin [38] and EOS [39] already implement it. For Proof-of-Stake the miner (or validator, which is more commonly used to refer to nodes taking part in the PoS consensus process) of a new block is not selected by having them guess a random number, but by a semi-random algorithm selecting the new validator based on its stake. Stake is based on the amount owned by a validator of the (native) token of a blockchain. These tokens may have to be locked to take part in the consensus algorithm. In some cases (like for Peercoin) it is also based on the "age" of the tokens held (the amount of time the tokens have been owned without being spent). Similar to PoW, PoS by itself is not a full consensus algorithm. It provides a different way to select a block proposer based on stake, but it would still need some further definition of consensus. This can be similar to PoW where

[16] An update in 2017 implementing SegWit (Segregated Witness) allows for larger blocks. The "main" block will still be 1MB but the witness data will be stored separately and including that in the block leads to larger blocks.

honest nodes extend the longest chain and the longest chain is the canonical one. It is also possible to use different consensus algorithms along with it, for example a classical algorithm such as PBFT [40][17]. These algorithms require far less energy and time to execute.

- Sharding: Sharding is a possible solution to the scaling problem that intends to "split" the single large chain into multiple small chains. Currently every node has to process and store every transaction[18]. With sharding accounts would be split into different shards[19]. Each of these shards would be its own chain with its own set of (periodically rotated) validators. This would allow the shards to execute different transactions in parallel while still contributing to a single "master" mainchain. The Ethereum blockchain is currently developing sharding [41].

- Sidechains: Sidechains aim to offload some of the work from the main chain similar to sharding. It is a "layer-2" solution instead of a "layer-1" solution (like PoS), i.e. it is not part of the core protocol of the blockchain but builds on top of it, generally using smart contracts. In this case participants will be able to "lock" some assets on the mainchain in a smart contract which would then be issued to that participant on a sidechain. This chain would have its own consensus algorithm and would function similarly to the mainchain. An example of a project working on this is plasma [42], which provides a set of specifications for these sidechains for Ethereum.

- State/payment channels: State channels are somewhat similar to sidechains in that they intend to move some of the work off the mainchain. Similarly to sidechains some assets on the mainchain would be locked in a smart contract

[17] PBFT does not scale well to large amounts of nodes though so it would likely not work well for a fully public PoS based blockchain. It could be used alongside delegated proof-of-stake (DPoS) where stakeholders vote on a limited set of validators that are responsible for proposing and validating new blocks. In addition to this PBFT is not Sybil resistant (participants could create a large amount of nodes to influence the consensus process. PBFT requires that participants identities are known and access of new nodes to the network has to be controlled.

[18] The usage of Merkle trees allows for periodic pruning of the state removing all transaction data except for the Merkle root hash and still being able to verify that a transaction is present in the hash. Alternatively nodes can opt to not store transaction data at all and only storing block headers which include the root hash. A full validation of the current state by a new node would require downloading the full chain though.

[19] This could be based on account address or asset type traded.

and these funds would be available in the state channel. However the state channel is not a blockchain, but instead a bilateral relationship between two parties. Initially these parties will have a balance based on the initial assets provided to the smart contract on the mainchain. The total balance of the two parties can never exceed what was originally provided to the smart contract on the mainchain. The two parties can only redistribute the total balance among them. When going back onto the mainchain one party can present the most recent distribution of balances (signed by both parties) and the other party has some time to dispute this. After this the smart contract keeping the funds will distribute them according to the provided balances. In addition to the simple two-party transactions it is possible to transact with another party as well if some path of intermediaries exist. For example if party A and B have a state channel and B and C have a state channel, A and C can have a transaction through B. This does require B to have sufficient assets in the channels though as the total number of assets in each channel has to stay the same. For state channels only two transactions are necessary: one to create it and one to close it and any number of transactions can be executed in the channel at far better performance than on-chain. Some concerns exist that this could lead to a hub-and-spoke type of topology though as it is cheapest to open as few channels as possible (less transaction fees on-chain) while still being able to reach a large amount of other parties. In addition to this any parties along the path have to have sufficient assets, the longer the path, the larger the chance that one party has insufficient assets. Some examples of this solution are Raiden network [43] and Lightning network [44].

3.2.2 Privacy

Another challenge is privacy, by default the full chain including the full current and historic state is visible to all participants. Transactions will happen between addresses giving some degree of anonymity (or more accurately pseudonimity). But when you conduct a transaction with someone of whom you know the identity, you then have a full overview of the transactions of that person/company (at least the ones executed with that address).

3.2.3 Permissioned & Private chains

Not all blockchains are public permissionless chains. Instead many projects have been private or permissioned or both. In the case of a permissioned blockchain not all nodes are equal; not all nodes are able to participate in the consensus process or create new transactions. In the case of a private chain not everyone may freely become a part of the network. Some party (or parties) will be controlling access to the network. These blockchains are often used by individual corporations or consortia of corporations.

Though the exact implementations here vary greatly, these will often have a relatively small and controlled number of nodes and a greater level of trust between them. The participants will also often be bound by (traditional) contractual agreements.

The advantage of these types of blockchains is that they are far more efficient. There is no need for Proof-of-Work, instead traditional BFT algorithms (like PBFT [40]) can serve as a consensus algorithm. Using these in a public permissionless blockchain is impractical as it opens up the possibility of Sybil attacks[20] and many classical BFT algorithms don't scale well too the huge number of nodes that a public permissionless blockchain can have. These blockchains can also enforce higher minimum computation requirements on their participants allowing for far higher throughput than public permissionless blockchains.

The technical implementations here also vary greatly, not all of these systems will use a chain of blocks (instead only the current state may be maintained) and in some cases not all participants will be aware of all transactions going on in the system. Some of these systems should probably not be categorised as a blockchain, but simply as some other form of distributed ledger. However the definition of what exactly constitutes a blockchain is still somewhat vague.

It is important to note that any direct advantages of using a blockchain with restricted membership will be limited to the participants with nodes in the network. If for example a group of banks operate a private network only the banks will be able to have any direct benefit from it. For clients of the bank it will not make a difference unless the blockchain solution reduces costs or increases efficiency and these gains trickle down to their clients.

[20] An attack where an attacker can create a large amount of notes to influence the vote.

Chapter 4

Issues with the current situation

4.1 Reconciliation

A report in 2014 from the Aite Group [45], predicts spending on reconciliation technology to be $1.27 billion in 2017. The need for reconciliation is driven by the different uninteroperable and unsynchronised (traditional) ledgers and databases kept by the various intermediaries. Ensuring that the ledgers of all parties involved stay up to date during the post-trade process and any inconsistencies are resolved takes a significant amount of time and money.

4.2 Intermediation

Part of the reason why the costs of reconciliation are so high is because of the large amount of intermediaries between the two counter-parties.

In the most extreme cases the parties involved in post-trade, in addition to the two counter-parties ('A' and 'B') and not including any pre-trade intermediaries like brokers, are (see subsection 2.3.2 for an overview of their roles):

- An issuer CSD
- An investor CSD (with CSD link to issuer CSD)
- Two global custodians
- Two local custodians
- A registrar

- A CCP
- Two clearing members

This does not include any other parties that provide general services to the parties involved, like the SWIFT Foundation which facilitates the network for post-trade messaging between parties. In addition the cash leg of a trade is often settled in central or commercial bank money which then also includes a central or commercial bank into the process.

Not all parties mentioned above are always involved in the clearing and settlement of a trade. Either counter-party (or their custodian) may be a clearing member of the CCP, removing the need for a separate clearing member. The CSD will often take up the task of a registrar (or the securities may be bearer securities). The custodian of a party may not employ a local custodian but can be a direct participant of a CSD. In general though there are a lot of intermediaries involved. This drives up prices and reduces efficiency of the overall process. These costs do not just include reconciliation, but also the costs of the various intermediaries in the chain repeating activities like corporate actions. Which have to travel down and then up the chain again.

In addition to the costs the large amount of intermediaries between the investor and the original issuer of the security can make it harder for investors to exercise their rights, which is especially relevant for shares. This is noted as one of the considerations of the second EU shareholder directive (consideration 4) [46].

4.3 Settlement time

At the time of writing, most 'spot' trades are settled at T+2 (2 days after the trade was executed). Derivatives have a more complex lifecycle where both the derivative contract and the underlying asset have to be settled and depending on the type of the derivative contract this may include multiple individual settlement cycles over the lifecycle of a derivative.

Longer settlement times expose counter-parties to risk as the value of the asset can change over time and the counter-party can default in the interval between trading and settlement. The T+2 settlement time for trades on a trading venue that was mandated

in the CSDR is already an improvement over settlement times in the past, but the closer we can get to (near) real-time settlement the more the associated risks will be reduced.

Paragraph 3.15 of the PFMIs [13] notes that further reduction of the settlement time is primarily difficult because of the changes required to existing processes and systems. They further note additional difficulties where cross-border transfers are involved due to timezone and holiday differences.

4.4 Failed trades

Trades can fail if one counter-party cannot settle its obligations. This is undesirable for multiple reasons: a party will be left with assets they intended to trade and they will not have the assets they wanted to aqcuire. This is especially inconvenient if settlement times are longer as the time between trade and the trade failing will be longer. If the party needed the assets to settle its own obligations it also opens the risk of a cascading effect as the inability to settle ripples out. Depending on how tangled up a market is this may have national or international effects.

4.4.1 Causes

There are several causes for failed trades:

- The settlement instructions don't match: if the settlement instructions supplied by both counter-parties don't match the trade cannot be settled, in most cases one party will have made some mistake in entering the instructions. Generally speaking this should be resolved before settlement, but if it has not been resolved before then the trade will fail.

- Missing cash: If the buying party has insufficient cash it cannot settle its obligations. This does not immediately mean the trade fails. In many cases the buyer will be able to lend the required cash. It is also possible for the trade to be partially settled, with a possible future settlement when the cash is available.

- Missing securities: This is similar to cash but on the sell side. Lending securities is also possible, but will often be harder as securities tend to be less readily available than cash.

The inclusion of a CCP in the process will reduce the risk of failed trades for the counter-parties. That risk will be transferred to the CCP however. In theory it is also possible for a CCP to be unable to settle its obligations or even go bankrupt. In practice only three CCPs have gone bankrupt so far [47] and CCPs are required to ensure they properly reduce risks, for example with margins and haircuts, maintaining a default fund and ensuring that their assets have a high liquidity.

Chapter 5

Role blockchain

This chapter will provide an analysis of the challenges and potential advantages and disadvantages of using a blockchain for post-trade settlement activities. It will be based on the explanations of the post-trade processes (subsection 2.3.2) and blockchain technology (chapter 3). This will be done by looking at various regulatory and technical challenges that have to be dealt with for clearing and settlement. Each section will look at one of these topics and how it impacts a blockchain implementation for post-trade processes.

5.1 Anti-money laundering and counter terrorist financing regulation

AML regulation aims to make it more difficult to use money for illegal purposes. The two main tasks for financial institutions are:

- Identifying the final beneficiary to an account or transaction and the intended purpose for it.
- Monitoring and reporting transactions for any unexpected or high volume transactions.

The rules above apply to parties in financial instrument trades as well. This is especially relevant because these will often have a high value (large amounts of money are transferred). As such it is important to see how this affects clearing and settling trades in financial instruments on a blockchain.

Currently public permissionless blockchains like Ethereum and Bitcoin allow anyone to enter and transact in the system and addresses are pseudonymous. This means that these networks could be used to avoid traditional monitoring [48]. The most recent European AML directive (EU AML directive 5 [15]) addresses this by adding cryptocurrency exchanges and custodians to the list of applicable entities for the directive. This will be effective as long as those exchanges form the main gatekeeper between the cryptocurrency and traditional banking world. If cryptocurrencies start to be more widely and directly used for transactions, it will be much harder to regulate as there is no longer a limited group of entities (like banks or exchanges) that can be regulated.

An obvious solution would be to not use a public blockchain, but use a private one. In this case participants could be identified by a central party (or set of parties) before they are allowed to participate and afterwards be assigned a PKI certificate associated with their address on the blockchain, enabling them to communicate on the network. This allows for proper identification beforehand and continuous monitoring afterwards as the identities of the participants are known.
A similar approach could be taken on a public chain though. From a privacy perspective it is undesirable to have participants share their identities and associated documents (e.g. passports) on chain. That would entail sharing that personal data publicly with all other participants and it would mean that addresses would no longer be pseudonyms, but would include direct identifying information. It is also possible however for trusted parties to issue a certificate stating that someone (a public key associated with an address) is allowed to hold and transfer (certain classes of) financial instruments and make use of clearing and settlement facilities provided on-chain. This would allow for controlled access to financial instruments clearing and settlement without requiring a participant to share large amounts of private information on a public blockchain. In addition it would allow these certificate issuing parties to monitor (and report) any suspicious transactions made on the blockchain by running a node. In extreme cases they can even revoke the certificate and block access to transfers if required[1]. In practice this allows these certificate issuing parties to control all access to this particular set of smart contracts (assuming that it is implemented using smart contracts and not as part of the core protocol). Vitalik Buterin argues that

[1]This would require the revocation to be published on-chain however, either by the issuing party itself or some other party serving as oracle.

even in these cases there is value in using a public blockchain [49]. He notes that the open design of a public blockchain can instill trust in its users due to the public verifiability of what is going on and it can prevent censorship since a smart contract may not allow anyone (not even the original developers) to take certain actions. It is important to note that this highly depends on how a smart contract is written. Many contracts (for example the Ethereum Name Service [50]) employ an "Owned" or "Ownable" interface which specifies an owner (by default set to the address deploying the contract). An owner may have special permissions that are not available to normal users of the contract. In the case of the ENS this owner can reassign names at will. This is often combined with the proxy contract pattern[2]. Proxy contracts are a way to upgrade smart contract logic without publishing a completely new contract which would require users to change the address they are calling. A proxy contract sits in between the user and the real contract containing the logic to be executed. It stores the address to the logic contract which can be overwritten to direct calls to a new contract.

The usage of a such a solution (ownership and/or upgrade-ability) does not remove the core immutability of a blockchain: deploying a new version of a contract will still have to be done with a digital signature and will be part of the history of the blockchain and the old version of the contract will still be part of the blockchain state. It does open up the possibility for the owner to change the functionality of a contract. For example an escrow contract may be programmed to allow a withdrawal of a deposit after 100 blocks have been added. In that time the logic may be modified to allow a withdrawal by the owner of the contract at all times. These risks are especially relevant if a proxy contract solution is used. The user of a contract may not be aware of a change in logic of the contract without continuous monitoring of the proxy and the logic that it points to. The usage of ownership in smart contracts also makes the owner a single point of failure with a breach of security creating risks for all users of the service the contract provides. Such issues may be (partially) mitigated by requiring multiple signatures for ownership related tasks (like upgrading a contract). Ideally updates to a smart contract are handled by creating a new contract and directing users to it via some public announcement. This allows users the freedom to migrate if they desire to do so. This can provide challenges however in regards to the retention of

[2]For descriptions see for example: [51] or [52].

existing state and transactions (the transactions will stay a part of the blockchain, but will be connected to a different contract). In addition it provides an inconvenience for users (and developers) of a contract if a gradual migration is chosen as some users may still be using the old smart contract.

Buterin also notes the possible network effects of being on a public blockchain. Applications developed on a public chain can easily interface with other applications on the same chain to add functionality.

5.2 Clearing: novation and netting

Currently the main parties involved in the clearing process are the CCP and its clearing members (and their clients). The two main tasks of a CCP are multilateral netting and serving as a central counter-party to reduce risks. In addition to this the CCP can offer additional privacy to counter-parties where trades are conducted on trading venues, by stepping in as central counter-party at the moment the trade is conducted.

The primary advantages of a CCP are:

- Reducing counter-party/credit risk by taking on the role of a central counter-party; guaranteeing delivery even in the case of a defaulting counter-party
- Improving efficiency by reducing the amount of necessary settlements through multilateral netting
- Optimising collateral efficiency by reducing exposures between counter-parties through multilateral netting

5.2.1 Cash securities

For traditional cash securities the need for a CCP (and clearing in general) could theoretically be removed by switching to real time gross settlement of these transactions. If this were to be the case counter-party risk could essentially be eliminated. It removes the need for posting collateral at a CCP and if settled on a gross basis no netting would be necessary either.
A blockchain could potentially facilitate this. This is however unrelated to the usage of a blockchain. Proper integration between CSDs and trading venues could give

similar results. Assuming that an executed trade or a set of matching settlement instructions (for OTC trades of cash securities) could be automatically handled at a CSD level, the CSD could directly settle the trade. This would require that sufficient cash and securities are available in the associated accounts at the moment of trade execution.

5.2.2 Derivatives

For derivatives the situation is a bit more complex. The transfer of a derivatives contract itself could be theoretically be handled in real-time. The settlement(s) that follow afterwards based on the underlying asset are more complex. These will often follow months or even years after the contract was created and there may be multiple individual payments/transfers over the lifecycle of a derivative. For example in the case of a Credit Default Swap (CDS), party A will pay a periodic payment (say monthly) to party B and party B will make a single payment if the underlying asset of the CDS defaults. This would mean that if party B defaulted after a few months, party A's payments and its potential insurance against the default of the underlying asset would be lost. This is something a blockchain cannot inherently prevent. A blockchain can prevent participants from spending assets that they do not currently own, but it cannot inherently guarantee that some amount of a particular asset is present at a particular date and time. It is possible to give these guarantees by reserving certain assets when a contract is created. This would be very inefficient though as large amounts of capital would be locked up in derivatives contracts.

Non-CCP cleared derivatives

Not all derivatives are subject to the clearing obligation. For derivatives without a clearing obligation it is still required to exchange collateral. This can be done through smart contracts which can lock up collateral and release it, either through automated rules or the influence of some empowered third party. Blockchains could improve the risk management of counter-parties due to the transparency of data on-chain giving a detailed overview of the assets and available liquidity of counter-parties. As discussed in section 5.9 however, the level of transparency that allows parties insight in all the assets and transactions of a party is undesirable.

CCP cleared derivatives

The bilateral exchange of collateral can help alleviate some of the risk, but it provides weaker guarantees than the usage of a CCP.

A CCP could hook into an existing blockchain and accept and make transfers using it for e.g. margin payments and the settlements it is involved in. The CCP would continue to operate as normal, keeping the need for a CCP and clearing members as intermediaries. It would be more interesting if a CCP could operate through a series of smart contracts without any single party backing it while providing similar guarantees regarding risk. In theory this could be achieved through a smart contract that required the posting of initial (and variation) margin and contribution to a default fund. There are several issues with this however:

- Collateral has to be regularly "marked-to-market"[3], this would entail using one or more "oracles" (i.e. exchanges in this particular case) to provide this information. Unless trading itself was executed on-chain (on the same chain as used for clearing) this will add a reliance on external centralised entities.

- Multiple participants joining in a single CCP share a certain amount of risk with each other. This makes it unlikely that parties will be willing to join in such a construction with fully anonymous parties and no external guarantees backing those parties. This will require a system for onboarding new participants that allows for identification of the new party and determine if its complies with its rules (non-discriminatory rules, as required by EMIR). The participants will have to define a clear governance structure with rules on who is responsible for checking and onboarding new participants. Who is allowed to evict participants if necessary. How margins are calculated. Who will be responsible for further maintenance and development of the smart contracts if required by new regulation. Many of these rules could be encoded in the smart contract(s). For example rules on eviction of a participant in the case of repeated failure to meet its obligations could be encoded in the smart contract logic.

- There is a current proposal by the European Commission [53] to have a formal set of recovery procedures for failing CCPs given their importance for the

[3]Marking-to-market means determining the current market value of an asset.

stability of the financial system. This can be done if these CCPs are known and authorised by ESMA. In a situation where people can freely create these constructions it will be harder for ESMA to back this however, removing this safety-net. As such it will not be possible to freely create these smart contracts. ESMA would have to approve individual applications for such a setup, including its rules on membership and handling of margins. Depending on its setup one party may still effectively be a CCP even if the execution of the system is handled through smart contracts. If a single party is given the responsibility to onboard new members and if it is responsible for the maintenance of the contracts (e.g. through special ownership permissions), such a party will still hold a large amount of control and effectively function as a CCP.

- If more than one of these smart contracts exist (potentially on different blockchains) with different participants and a trade has participants of different smart contracts, some degree of interoperability is necessary. Otherwise parties would need an intermediary that is part of the other smart contract that can act on their behalf for this trade.

- According to EMIR a CCP is defined as a 'legal person'. This would mean that in situations where a group of participants would want to run such a construction on a blockchain through smart contracts, they would need to setup a legal entity together that can be authorised as CCP.

In addition to reducing counterparty risk, CCPs also provide utility through multilateral netting. This is especially relevant on public blockchains due to their scalability issues. Some of the current solutions to these issues (specifically sidechains and state channels) are somewhat similar to deferred net settlement, by moving settlement off-chain and only "fully" settling on-chain every now and then. Multilateral netting can also reduce liquidity requirements however, as counterparties will only need to have sufficient liquidity to settle their obligations at end-of-day. With state channels and sidechains the required funds for individual transactions need to be available throughout the livespan of the state channel/sidechain. Multilateral netting could also be implemented on-chain through smart contracts, aggregating transactions in a contract throughout the day. Some external party would still have to be responsible for triggering the actual settlement of these obligations at some point though.

5.3 Settlement and registration

5.3.1 Securities

The settlement of trades in transferable securities is currently primarily handled by CSDs, using "securities settlement systems". A blockchain used for the registration and transfers of securities traded on a trading venue would fit the description of a securities settlement system and would need to be operated by a CSD. The usage of a blockchain would only make sense if a CSD could share that responsibility with other running nodes. As mentioned in section 2.3.3 CSDs are allowed to outsource their core activities, but this requires separate authorisation. Two exceptions to this are mentioned:

- In article 30(5) in cases where the outsourcing is done to a public entity. The CSDR frequently asked questions [54] mentions T2S as an example of this type of outsourcing. This means that unless the blockchain based settlement system was under the control of some public entity (government or local government) this exception would not apply.

- In article 31 in cases where the exception is provided through applicable national law. This is unlikely to apply for this particular case.

If participants of the CSD were to hold nodes in the system which are part of the consensus algorithm, the CSD would have to request authorisation. Given the mention of "service provider" it is likely that a CSD operating a blockchain would have to request authorisation for individual miners/validators. At the very least separate authorisation under article 19 would have to be requested for the general usage of blockchain as a securities settlement system.

The register of an issued security[4] and the accounts in a securities settlement system holding these securities are currently not considered the same thing. The CSDR mandates that the accounts in a securities settlement system are reconciled with the entries in the register on a daily basis. In the absence of technical errors a blockchain should be very resilient to these inconsistencies. Nevertheless existing hacks (like the DAO [55] and parity multisig wallet [56]) have shown that this is not

[4] If the security is a non-bearer security.

always the case. Given the requirements in the CSDR, the operator of a blockchain securities settlement system would still need to perform this reconciliation and would need to be able to correct any inconsistencies if necessary.

5.3.2 Derivatives

The settlement of derivatives differs per derivative. In some cases cash settlement is chosen and settlement will only entail transfers of cash. In other cases physical delivery is chosen which will depend on the nature of the underlying asset. If the underlying asset is a security this will entail both cash and security movements (involving a CSD), if it is a commodity it may entail actual physical delivery of e.g. oil or gold. Though securities will be fully dematerialised and ownership could potentially be transferred using a book entry on a blockchain, the same is not true for physical commodities. There have been suggestions to "tokenize" these physical assets, but that will only ever be a representation. The physical asset would still have to be transferred in some way, preferably with a minimal amount of risk for the receiving counter-party.

5.3.3 Forks

As discussed in section 3, blockchains can fork. In subsection 5.3.5 we will discuss the complications in regards to settlement finality. In addition to this there is another complication in regards to hard-forks due to software updates. A software update where some group of node operators does not update to the newest version can lead to a hard-fork (only if there are incompatibilities). Afterwards there are essentially two separate blockchains that share part of the history of the chain up to a certain block. For cryptocurrencies this effectively leads to the creation of two new cryptocurrencies. If these cryptocurrencies purely live on the blockchain and are not tied to some off-chain organisation or asset this is not a huge problem though it can have a big impact on the community. For financial instruments it is more complex. Owners of securities will suddenly hold two versions of the security that can be traded individually on both forks (effectively double spending). One of these would have to be recognised as the "real" one. One option could be to have the issuer decide. This means that

owners (or parties acting as a custodian on behalf of the owners) of a security may be forced to hold their assets on the fork that they are personally not in agreement with. It is also important that an announcement regarding the canonical fork for a security is made promptly. Until the time where it becomes clear which fork is the "real" one, it would be necessary to settle a trade on both forks to reduce risks for counterparties. The choice of fork also has to be made carefully as a larger fork could potentially attack a smaller one. Another choice could be to have a regulated entity like a CSD decide which fork will be canonical. This would be the clear choice if a CSD operated a securties settlement system through a set of smart contracts on a public chain. In practice this would mean that said party would have a large control over the overall development of the blockchain and would be able to "force" software updates on participants. The ability for miners (and users) to "refuse" an update is what prevents the developers of a blockchain from holding control over it. If miners could not do this it would mean that updates such as the rollback of the DAO hack could be enforced by a single party[5].

This control over software updates is especially relevant as such a system would have to comply with regulatory requirements, for example the measures to address settlement fails described in article 7 of the CSDR. Regulatory requirements can change over time and the blockchain would have to stay up to date with these requirements or the associated processes would have to be moved off-chain. These requirements include the need to remove a party from the settlement system after a certain number of failed trades. If this were to be done off-chain someone would have to be able to block access to the system for this party. If it were done on-chain such logic would have to be encoded in the core protocol or in smart contracts and it has to be possible to reliably adjust this logic over time (without the option for parties to "opt-out").

On a private blockchain this issue is less pressing. Generally speaking there will be contractual obligations between the limited set of parties involved, that can include rules on software updates and can settle disputes on forks.

[5]This forced choice would only be relevant for parties that are holding financial instruments on the forked chain. Other parties would still be free to choose which chain to adopt.

5.3.4 DvP

As mentioned in the principles for financial market infrastructures and CSDR: securities settlement systems need to support DvP settlement. Assuming that the assets for both legs of a trade (security and cash) are present on the same chain, achieving DvP is trivial and can be implemented as part of the underlying protocol or through smart contracts by having both parties sign the simultaneous transfer of assets.

Achieving the same in a situation with multiple chains (cash on one, securities on the other) is more complex. The Stella report [57] and project Ubin [58] implemented proof of concepts using hashed timelock contracts (HTLC). These do achieve the goal of having atomic swaps, but come with some notable disadvantages:

- They require parties to be online during the settlement process, as each parties has to actively claim their assets.
- They rely on time, requiring synchronised clocks to maintain consensus on the ledger, something which is hard to achieve especially on public ledgers.
- Liquidity is locked up for a certain period of time. Locking up liquidity is not considered to be beneficial to the financial markets and the need to lock up liquidity for at least several hours feels like a step backwards instead of forwards.

A further complication for achieving DvP comes from the probabilistic finality of settlement in primarily PoW systems. At any moment multiple valid forks can exist, the longest fork (fork with the most work) being the "canonical" one. In addition to the fact that multiple forks with the same length can exist, giving no clear picture on the real one, there is also the risk that a longer fork is overtaken by a shorter one. In theory these forks can be very deep, potentially undoing a large amount of transactions. In situations where cash and securities are on the same chain this does not necessarily have to prevent DvP, as the transfer could be designed as a single atomic transaction. This means that the new fork would have to either include or not include the transaction without having the opportunity to undo only one leg. In cross chain situations this is harder however as on one chain a fork could undo a transaction, while the other chain would still include its transfer. This could be handled by locking securities/cash for some time as suggested by the Stella Report and project Ubin, but

comes with the disadvantages mentioned above. In addition to this it is theoretically possible for an attacker to do a deep rewrite of the blockchain which could still undo part of a DvP transaction even if the assets on both chains were locked for some time.

5.3.5 Settlement finality

Settlement finality is a legally defined moment. In the EU it is up to the operators of various settlement systems (including payment systems and securities settlement systems) to define the moment where transfer orders have "entered the system" and are binding, as well as the moment where they are irrevocable by a participant or third party.
A blockchain based system can define these moments too (though it may be harder to define the operator of such a system). A very obvious choice in this regard for blockchain applications is the moment when the transfer order is included in a block. There is a problem with this approach though:

As mentioned in subsection 5.3.4 blocks included in a PoW chain can at any moment be overtaken by another chain, thereby undoing the transaction. To be safe a certain amount of blocks has to be mined afterwards to give a reasonable certainty that no other fork will overtake it. This depends on the total available hashing power and its distribution over participants and may have to be adjusted over time. This is especially relevant for securities as their value is not directly tied to the network itself. The value of a cryptocurrency like Bitcoin will be affected by public trust in the network and an attack will affect it. The value of securities however is tied to the company that issued them and the value of derivatives is often tied to the value of the underlying asset. This makes it hard to clearly define a reliable moment of settlement finality.

This issue does not apply to blockchains using a classical consensus algorithm like PBFT.

5.3.6 Failed trades

Failed trades occur when at settlement time a counterparty is unable to settle its obligations. It is important to note that settlement finality and DvP do not prevent failed trades. Failed trades prevent a trade from being settled before even getting to the

point of DvP and settlement finality. The only way to fully prevent any failed trades is to reserve the assets that counterparties owe each other when the trade is executed. While this may be achievable for trades in some types of financial instruments by using reservations as discussed in section 5.2 (with or without blockchain), this is impractical for many other types: most notably derivatives that often settle over months or years. In these cases neither a blockchain nor a traditional centralised system can fully guarantee the availability of the required assets at the time of settlement.

5.4 Custodians: Custody & Asset servicing

In the context of settlement, custodians are already not a regulatory requirement. The usage of a CSD for settlement of securities is defined in the CSDR, but custodians are not defined as a requirement. In theory end-investors could hold their securities directly at a CSD. In practice this is not the case however as only custodian banks are able to become participants of a CSD. CSDs in some European countries (most notably various Nordic countries) already mandate segregated accounts on an end-investor level, these accounts are not managed by the end-investors themselves though, but still by custodians [10]. A system based on blockchain technology does not inherently change this however. The operator of a blockchain securities settlement platform could opt to let end-investors manage their own accounts (addresses), however a choice could also be made to maintain the current holding structure and restrict participation in the system to custodians.

Custodians are especially relevant in situations where investors hold their securities spread out over various CSDs in various countries. In these cases it can be more convenient for an end-investor to hold their securities at a single global custodian rather than a plethora of CSDs.

A single unified ledger for the capital markets could remove that complexity and make it easier for individuals to hold their own assets. This only holds if a single global platform emerges though. Given the differences in legislation between different areas around the world however, it is more likely that individual solutions will emerge for different markets and countries. In that case an end-investor could still be forced to have various different accounts on different chains and may wish

to outsource the task of managing those accounts to a third party. At this point the custodian is reintroduced into the system and depending on the number of chains and their technical interoperability the custodians may wish to further outsource their responsibilities. Recreating a chain of custodians.

5.5 Reconciliation

The consensus protocol of a blockchain will provide participants with a single consistent and auditable view on the data on the chain. This can help address the issue of reconciliation where different participants in the clearing and settlement process may have a different view on the assets they own. Similar processes may be executed on different systems (or on paper without automated digital systems in some cases) by different parties leading to discrepancies in their data. By moving these processes and their associated data to the blockchain all participants will have the same view (and a common truth) of the data. This does not remove the need for manual (or automated) checking of this data. Issues in the blockchain software or smart contracts may still lead to mistakes. It will make those mistakes easier to rectify however as each participant will be looking at the same copy of the data.

These advantages do not solely come from the usage of a blockchain however. Adopting a blockchain based solution for certain processes implies adopting a common set of standards and harmonising the approach to those processes and their associated data. This adoption of common standards and processes is more important in reducing the cost and complexity of reconciliation than the blockchain itself. The blockchain adds a layer of consensus over that, reducing the ability of individual participants to deny certain actions were taken or certain results were calculated as these will be part of the (immutable) chain and signed by the participants where necessary. Furthermore the usage of a blockchain ensures that all participants will be looking at the same data and the same set of transactions leading to that data. If only a messaging standard was used with individual applications processing those messages, differences in the applications could still lead to discrepancies. It would also be possible to add a traditional application to the messaging standard which will be responsible for processing messages. This will also provide a more unified view on the data, similar to a blockchain. One advantage that a blockchain provides,

compared to a messaging standard + traditional application solution, are smart contracts. As business processes change or new processes are added there is a risk of implementations diverging again, reintroducing the need for reconciliation. Smart contracts allow participants to add on to the logic of the chain, introducing such new (or changed) logic as new smart contracts. These smart contracts will be available to all participants ensuring shared logic and data for the new processes.

Any advantages a blockchain provides in terms of reconciliation only apply to the direct participants of a blockchain. Any other parties using traditional systems or a different blockchain system will not benefit from it and will still require traditional approaches to reconciliation. Furthermore any processes that are handled off-chain by blockchain participants will also not benefit from the consistency guarantees of a blockchain and will have to be reconciled in some other way.

5.6 Cash

In addition to the general difficulties with cash potentially being on a different chain than securities (see: subsection 5.3.4), there are some additional challenges.

Most cryptocurrencies are currently very volatile [59] [60] [61], making them a poor means of exchange for securities trades, especially given the high values of many of these trades and the lengthy delay before settlement in the case of derivatives. The simplest way to solve this issue is by having a trusted organisation issue a tokenised version of a traditional government issued currency on-chain, fully collateralised by that particular currency. Examples of this already exist, the most notable being Tether [62]. In addition to this some of these issued currencies are regulated like Paxos [63]. According to article 40 of the CSDR there should be a strong preference to use central bank money instead of commercial bank money, so it would be preferable to have a central bank itself handle these issuances[6]. At this point the ECB has no plans to issue such a currency [65].

There are some other initiatives to create stablecoins, these can be broadly divided in two categories:

[6]Tokenised government issued currencies may hold the reserves in central bank accounts, however according to Dirk Bullmann of the ECB this would still not be considered central bank money if it was not issued by the central bank itself [64].

- Algorithmic stablecoins, an example being Basis (no longer in operation) [66]. These stablecoins rely on automatically adjusting the volume of coins in circulation depending on supply and demand. If the price drops below an acceptable limit bonds will be sold of at a discount removing coins from the market. If the price gets too high new coins will be created and bondholders can exchange their bonds for these new coins.

- Crypto-collateralised coins, an example being the DAI [67]. These coins are collateralised using other cryptocurrencies instead of government issued currencies. In order to manage the volatility of cryptocurrencies they are "over-collateralised". This means that to buy €100 worth of DAI, €150 (or €200 or €300 depending on the parameteres of the system) worth of some other cryptocurrency would have to be provided as collateral.

Neither of these stablecoins has a lot of academic research or analysis done on their long term stability and performance under pressure however. As such they are for now unsuited for the cash leg of settlements.

With no reliable on chain currency at the time of writing this thesis, a blockchain based securities settlement system would have to integrate with an existing payment system (preferably ran by a central bank, like Target2 in the EU) in order to handle the cash leg of the securities transaction.

5.7 Corporate actions

Corporate actions could be handled using smart contracts. They could automatically disperse dividends or coupons to relevant investors or conduct votes if necessary. This is assuming that there is a disintermediated structure though. If accounts on chain are still managed by intermediaries (and not all parties in the chain of intermediaries are part of the same blockchain), any such corporate actions would still have to travel up and down the chain. The ability for the blockchain to provide true value here is largely linked to the ability to disintermediate and reduce the gap between investor and issuer. If custodians are still managing investor accounts, it would still be up to the custodians to process this further down the chain.

5.8 Integrity and availability

CCPs and CSDs are considered critical financial infrastructures. Attacks on the availability or integrity of their systems could have a destabilising effect on the larger capital markets. In this regard a blockchain provides clear advantages. Classical consensus algorithms will generally guarantee availability with up to 33% consensus participants with byzantine failures. For an attack on the integrity of the ledger 67% would be necessary. These algorithms require the identity of the participants to be known in advance though to prevent sybil attacks. PoW or PoS based systems will generally be safe as long as no single party controls more than 50% of the mining power/stake. Assuming that these nodes are under the control of different entities an attack on a blockchain is more difficult than on a traditional centralised system. This does assume a certain amount of decentralisation in the implementation of the blockchain. If a single party has a lot of special permissions that party will still be a potential weak spot of the system.
While a blockchain can provide better integrity and availability than a traditional centralised system, it weakens confidentiality of information stored on the chain. In addition to the fact that all participants will have insight in the data stored on-chain, it also makes it easier for an attacker to get access to the data. To gain insight in the settlements of a CSD operating a traditional system, an attacker would have to gain access to the CSD's securities settlement system. In a blockchain system the attacker could gain access to the system of any of its participants and gain (read) access to the data on the blockchain.

5.9 Trading privacy/anonymity

Trading of securities and derivatives is a competitive area and individual investors will not want to have their transactions publicly visible. In the event that retail investors are involved this would even be in conflict with the GDPR [68]. Currently transaction information is limited to the various intermediaries involved: custodians, clearing members and potentially a CCP and CSD if a segregated account structure is used. In some situations the counterparty may also be aware. When trades are conducted in a trading venue the CCP will generally step in immediately however, providing

anonymity to both counterparties. This may also be the case in OTC trades if the trades are intermediated by broker-dealers. A blockchain by default only provides pseudonimity and provides full insight for participants to see all transactions going on in the system.

5.10 Regulators

Assuming that various custodians hold nodes in a blockchain system it can provide a powerful audit log for regulators. Even if the CSD has the ability to take certain extraordinary measures these will be part of the blockchain history[7]. For this to be the case it has to be the blockchain itself which is designated as the "securities settlement system" for the purposes of the CSDR. The blockchain has to be leading (and not another system ran by the blockchain operator and connected to the blockchain) when it comes to the administration of securities accounts and the transfers of securities between accounts.

It would also possible for regulators to hold a node (or multiple nodes) in the blockchain as a participant. This would give them more direct insight in the activities of the custodians than they have with the current system of reporting. In the current system of reporting it is up to the regulated entities to submit reports to the regulator as required by regulation. A node (or multiple nodes) in the blockchain would give the regulator direct (and near realtime) insight with less opportunity for fraud in reports of the regulated entities. It is likely however, that multiple blockchain systems will be created for post-trade settlement. Holding and administrating nodes in all of those would require significantly more effort from regulators than the current system, where regulated entities make their reports to the regulator in a format specified by the regulator. This would require regulators to run multiple nodes, possibly with differences in setup, configuration and operation if there isn't a sufficient amount of standardisation in the ecosystem.

[7] Assuming that the core logic of the blockchain is solid and relies on digital signatures for all changes/actions.

5.11 Summary

The challenges of regulatory comliance (notably anti-money laundering requirements and the CSDR) make it difficult to gain true value out of operating on a public chain as a certain degree of central governance and control remains necessary. Though these challenges do not necessarily prevent operating on a public blockchain it removes a signficant amount of value of the blockchain while posing challenges in terms of privacy, scalability and flexibility in terms of deployment of new updates. Most problematic for this solution however is the potential for hard-forks on public chains which cannot be fully prevented and will cause instability and uncertainity which is undesireable for the settlement of securities. Private permissioned chains do not suffer from the issues mentioned above, but they are also far less decentralised.

A single party could be authorised as a CSD/CCP and maintain responsibility and (a certain amount) of control over the blockchain. The only potential regulatory challenge here is that the presence of other miners/validators on the chain should be considered outsourcing and would require separate authorisation. In practice a CSD or CCP would still need to hold a significant amount of control as the responsible party for the process. The system would also have to connect to existing external systems for example for cash settlement. With no real solution for decentralised stable cryptocurrencies such a system would have to rely on an external system or on a participant issuing a token backed by central or commerical bank money on the chain.

Many advantages of the blockchain for post-trade clearing and settlement (instant settlement and removal of intermediaries between issuer and investor) can be achieved with or without a blockchain as they are not issues that a blockchain specifically aims to solve.

Achieving real decentralisation and censorship resistance of securities settlement on a blockchain will not be possible to achieve under the current legislation. The added transparency and accountability (non-repudiation) of the blockchain still remain though. However these issues do not exclusively require a blockchain. RFC6962 [69] proposes a solution based on digital signatures and merkle trees to create more transparency and accountability for the certificate issuance process. Similar ideas could be employed in the financial markets to improve transparency and accountability while allowing financial infrastructures to retain the discretionary control required by regulation, without the scalability challenges and inflexibility of a blockchain.

After this the main values of using a blockchain are byzantine fault tolerance and the single consistent view of data and processes on a blockchain. The need to compromise multiple nodes to succesfully attack the system adds resilience which is important in the financial markets. A single party could operate a byzantine fault tolerant database, however the distribution of nodes over different separate parties will make an attack more difficult.

The usage of smart contracts and a consensus algorithm enable a consistent and unified approach to certain data and processes. This can reduce the complexity of reconciliation, but the usefulness of this scales with the number of participants and the amount of shared processes on the blockchain.

Chapter 6

Case study

6.1 Current implementation & future vision

This case study was conducted on a company (hereafter referred to as 'the company') using a blockchain for the purpose of settling equity securities of SMEs (hereafter referred to as 'the system'). The goal is to improve the post-trade settlement infrastructure for SMEs that have their equity traded on trading venues. They have had a successful pilot with full launch planned later in 2019. Since they intend to settle transactions of transferable securities they will operate as a CSD.

Deployment of the system will be done in phases. In the first phase only the CSD itself will control all nodes and smart contracts, as well as the private keys of the participants. The system is build from the start in the spirit of decentralisation, with the blockchain at its core and the settlement logic and data stored on-chain. This is done in preparation for future phases which will further decentralise the system. Later on in the lifecycle of the system participants will be able to deploy smart contracts and control their own nodes and take part in the consensus process. The order in which this will happen will depend on the maturity of the technology and ecosystem and there is no specific order planned. The system is not a public blockchain (and there are currently no plans to transition to a public permissionless system). Participants will be given access by the company. End-investors will not be direct participants of the blockchain, instead custodians will be the direct participants of the system/blockchain.

The longer term vision for the system is to see if regulation can be created to have a more "lightweight" permit as a blockchain operator rather than a full CSD. This would allow the company to run the system in a more decentralised manner,

with a network of custodians operating nodes and contributing smart contracts to the system. In this case the company would operate as a service provider developing functionality in the form of smart contracts and being responsible for the general operation of the system, rather than being fully responsible for all settlement activities like a CSD. To create a network of custodians rather than a centralised CSD a more decentralised governance structure is also important. Further development of the system would have to be handled in a more decentralised manner. Some of this could be handled fully on-chain through the implementation of voting smart contracts which would impact the parameters of other smart contracts [1]. This would allow these parameters to be changed in a fully automated non-discretionary manner. For other more radical changes to the smart contracts or the core protocol itself on-chain voting could still be used, but the actual development and deployment of updates cannot be fully automated as it will require manual (human) labour. For this traditional contractual agreements would have to be made regarding the proposal and voting on changes/features.

The system is not solely a blockchain. The blockchain itself is only used to transfer securities between participants and maintain positions and cash balances of participants. Other data and processes are kept off-chain. The blockchain is surrounded by a layer of microservices. These are used to store privacy sensitive data (data of direct and indirect participants). On-chain participants are only identified by their address and the mapping between addresses and "real" identities is kept off-chain. These microservices use normal relational databases to store their data. In addition these services handle interfacing with external systems. They are responsible for receiving and sending FIX and SWIFT messages and they provide data to a web interface. In the first phase where the participants do not have their own nodes yet, the web interface and the FIX and SWIFT connections will the interfaces to the system that are used by the participants.

The system directly interfaces with a trading venue instead of having the normal CCP and clearing members in between. The relatively low value of these trades (since they focus on the SME market) means that a CCP is not necessary. This cuts out several of the middlemen normally involved in the process. To ensure that the amount of failed trades is limited and to provide instant settlement the system makes use of

[1] Since the system is a private blockchain the complexity of how to prevent participants from voting more than once is not an issue here.

reservations. When an order is accepted into the system a reservation is made and the securities/cash are blocked during the reservation. These reserved assets cannot be used for further trades. When an order is cancelled or executed the reservation will also be dereserved and the real position/cash balance will be updated accordingly.

As required by the CSDR the system offers omnibus and segregated accounts to its participants. The cash leg of the settlement process is handled using commercial bank money. The company holds the power of attorney over the cash accounts at the commercial bank. The balances at the commercial bank are reflected on the blockchain. The blockchain itself holds technical cash accounts that reflect the cash accounts at the commercial bank. This enables DvP on the blockchain itself, as a transfer of cash on-chain will always be followed by a transfer of cash on the accounts of the commercial bank.

Finality of transfers and transfer orders is also achieved on-chain. This finality is achieved when blocks are added to the chain.

6.1.1 Technology

The current implementation is based on Ethereum, specifically the parity client. There are plans to switch to Pantheon in the near future and there is a further implementation in development build on Corda. The current consensus algorithm used is Aura, the planned consensus algorithm used with Pantheon is IBFT. The actual logic of the settlement and the reservations and the related position/cash balances are encoded in smart contracts. Currently privacy of data is achieved by limiting access to custodians and by keeping privacy sensitive data off-chain in the microservices. To ensure the ability to continue updating the system software updates will be mandatory for participants.

6.2 Discussion

In the initial version of the system all nodes will be controlled by the company itself and other participants will interface with the system through a web interface or FIX and SWIFT messages. There is no decentralisation with this solution and from the perspective of the participants using the system it is normal traditional system.
This does not mean the usage of the blockchain has no added value. The usage of a

byzantine fault tolerant algorithm provides byzantine fault tolerance and will make the system more resilient to malicious and non-malicious faults. The fact that a single party controls all nodes lessens this a bit, a security breach or other fault is more likely to affect all nodes. In addition the usage of a blockchain in this manner may provide better transparency and accountability. It will not provide this out-of-the-box though. Since the company controls all private keys it can theoretically (the company is heavily regulated and audited) rewrite the blockchain (or partially rewrite it) with little effort, since no expensive hash computation is necessary with Aura or IBFT. One option to improve on this could be to periodically publish the current block hash in a public place (like a public blockchain), this provides a checkpoint at which point rewriting will no longer be possible. If the blockchain is later shared with another party they can easily verify these "checkpoints" and the overall integrity of the chain itself. This still does not provide strong accountability guarantees though. Stronger guarantees could be provided by having participants sign requests to the system and have the system return signed responses. Incorporating these into the chain can add stronger accountability guarantees though the system still won't be decentralised.

At some point after the initial release of the system participants will be able to hold their own nodes, deploy smart contracts and participate in the consensus algorithm of the system. This turns it into a more "traditional" private blockchain. As discussed in section 5.3 however, the company will have to maintain responsibility for the settlement activities performed on the system as required by the CSDR. This means that they will have to be able to revert transactions in extraordinary cases and have to be in control over who can participate on the system. This does not require them to be able to remove or change blocks on the chain, but they do need to be able to perform compensating transactions in certain cases. The more special permissions the company has as a CSD, the more they will operate as a traditional centralised entity.

As mentioned in section section 5.11 the use of a blockchain will add transparency and accountability to the direct members of the blockchain. However as mentioned in that same section, these properties can also be achieved without a blockchain, by using Merkle trees and digital signatures. As such the primary advantages of a blockchain remain: the additional security provided by the byzantine fault tolerance of the consensus algorithm and the shared consistent view of data and processes enabled by the consensus algorithm and smart contracts.

The usage of smart contracts is the most noteworthy of these advantages. Multiple participants using the same smart contract on a blockchain implicitly agree upon a shared standard for data storage and processing. Furthermore the usage of smart contracts adds another a further layer to this by guaranteeing that all users will have a shared implementation of that standard. The advantage derived from this will depend on the amount of participants the company can gather (the network effect). In addition to the consistent view of data and processes smart contracts also provide strong accountability and transparency guarantees in a decentralised network. The exact functionality of the contract is visible to all members (at least to those with sufficient technical knowledge to understand them), with no opportunity for participants to tamper with it "behind the scenes"[2]. Any calls to a contract's functionality will have to be signed by the caller, providing non-repudiation. Even if certain participants have special permissions due to regulatory requirements they will still have to play by the rules of the network and any actions taken will be part of the shared immutable state of the blockchain.

The smart contracts can also pose a risk if other nodes can freely deploy them into the system. The initial set of smart contracts, deployed by the company, forms the core of the securities settlement system. As a blockchain system the throughput of transactions is ultimately limited due to the need for all nodes to retain a consistent overview of the system state. In the initial setup all of that throughput will be dedicated to handling orders and executions for the securities settlement system. If other participants can freely deploy (and call) smart contracts, they can take up some of that throughput. Nodes could be configured to prefer transactions relating to the core settlement smart contracts, but this will in turn affect the processing delay (and thus usability) of the other contracts. Moreover it is hard to enforce such a rule. Individual nodes can choose to prioritise other transactions and blame it on the unreliability of the network, claiming they never received certain transactions.

These issues are further augmented due to the solution the company has chosen to prevent failed trades. A reservation is made in the securities settlement system when the order is first created. Depending on how exactly the communication between the trading venue and securities settlement system is implemented it may cause further

[2]As mentioned in section 3.1 it is possible to use proxy contracts to update contract logic "behind the scenes" this issue can theoretically be solved with good monitoring tools however that check and notify a participant when certain changes are made to a smart contract.

problems. If the trading venue waits for confirmation that a particular order has been reserved, it may cause delays in between the submission of an order by a trader and its processing by the trading venue. For instruments with a lower liquidity this may be acceptable, but for instruments with a high liquidity it will not be acceptable. If the processing of the reservation and the submission to the trading venue are instead handled in parallel, it creates the risk that an order will be (partially) executed before the reservation was processed. This reintroduces the risk of failed trades.

If more lightweight regulation is passed that allows the company to operate as a "blockchain operator" instead of a CSD, it could lead to a larger degree of decentralisation. This decentralisation is still limited to the custodians which will no longer have to depend on a CSD. For clients of a custodian not much changes in terms of decentralisation, they are still dependent on their custodian and whatever system the custodian uses to administer their accounts. For the end-investors there will still be several intermediaries in between them and the issuer of the securities.
This decentralisation implies a greater control by custodians though which means that the new permit for a "blockchain operator" would either have to be accompanied by a permit for its participants or the permit for the blockchain operator would have to impose strict rules on the admittance of participants to the network. This assumes that the blockchain operator maintains sole responsibility for onboarding new participants to the blockchain.
Even if this further decentralisation happens, it will still be limited to the securities transfers. A transfer of securities in the system is a real direct transfer of ownership. As soon as the transfer is done, those securities are available for further transfers. For the cash side this is not the case. The company holds the power of attorney over accounts at a commercial bank. A transfer of cash in the smart contracts will eventually lead to a real transfer in the accounts of the commercial bank, but there may be some time delay in between that and the participants will rely on the company to handle this.

There remains the possibility of human error in the development of the core blockchain logic or the smart contracts. Where such errors affect the proper functioning of the settlement process a clear plan has to be created on how this is handled and participants will have to be forced (through contractual obligations) to promptly update their software to fix these issues if they arise.

Privacy of trades is handled by restricting access to custodians. Custodians holding nodes will be able to see all settlements in the system, including those on accounts of other custodians. Some of these accounts will be omnibus accounts. This limits the information that can be gained from the settlements as they can be for any of the custodians clients. Even if the accounts are segregated by beneficial owner it is still only the custodians that have insight in it. The custodians themselves will already be accounts for various clients and have insight in their trading behaviour. In addition to this the addresses on-chain are also pseudonyms and no (directly) identifying information is stored on-chain.

When the system will first be released, CCPs will have no role in its settlements. In the future this may become relevant if other types of instruments are settled or if liquidity becomes an issue for the participants. When it comes to the settlement process itself, the CCP is simply another participant and could be onboarded as such. In the simplest form they could simply have accounts (and own a node) in the system and take part in the DvP settlements. They could then transfer securities and cash on the chain and would handle all other concerns off-chain in their own systems. That would remove the current automation the system provides however. Executions would no longer be executed immediately (and automatically) after being received from the trading venue and the CCP is reintroduced as an intermediary.
Further integration of the CCP into the system could alleviate some of these disadvantages. If the CCP would have its own smart contracts for managing margin and collateral, it could integrate nicely with the settlement smart contracts and it would be easy to use on-chain securities and cash for the purpose of margin/collateral. This would be limited to the cash and securities already on-chain though. The CCP could also maintain an overview of other assets it holds as margin on the chain, but any transfers would have to be handled off-chain using whatever system is required for that asset (like another payment or securities settlement system). Furthermore as mentioned before the addition of these new smart contracts introduces new transactions that will be competing for the throughput of the system.

Chapter 7

Related work

Several papers have already been written about the usage of blockchain in this specific field. Though several of these have academic origins there are also papers and reports written by (employees of) various financial institutions like the ECB, Bank of England and Federal Reserve System.

Though out of scope of this thesis some research has also been done on the potential of blockchain to affect the pre-trade processes. Malinova and Park (2017) [70] focus primarily on the pre-trade aspects of market transparency and how the blockchain could facilitate more transparency to reduce the costs of OTC markets.

Mainelli and Milne (2016) [71] interviewed several experts from the financial markets and blockchain fields, to validate several hypotheses they had. From their discussions the results were that some sort of permissioned blockchain would probably be best and that widespread cooperation would be necessary to arrive at a practical solution.

Papers were also written by Pinna & Ruttenberg (2016) [72] as well as Mills, Wang, Malone, Ravi, Marquardt, Badev, Brezinski, Fahy, Liao, Kargenian, Ellithorpe, Ng & Baird (2016) [73] of the European Central Bank and the Federal Reserve respectively. The paper by the federal reserve is a more high level analysis of whether or not the blockchain could play a role in the financial markets without going into details what that could look like in practice. Their conclusion is that while the exact impact of the blockchain on the financial markets is unknown, it has the potential to reduce the operational and financial frictions in the financial markets and to potentially change the overall structure of the financial markets.

The paper by the ECB presents several possible applications of the blockchain

where it replaces various processes/parties in the current system.

They analyse the impact on 3 layers of the post-trade process: settlement, custody and clearing.

In the case of settlement they raise 3 main issues/challenges: they identify the need for a trusted independent party to supervise the ledger to insure that the overall integrity of the ledger stays intact (the amount of shares in circulation should match what was originally issued). Furthermore the cash part of the transaction raises a potential issue. Assuming that the cash is not paid in some digital currency like Bitcoin it means that a link "outside" the ledger remains. Not mentioned in this paper is that even if a cryptocurrency would be used it would still create the challenge of having cross ledger transactions which is discussed in the Stella Report [57]. In addition to this the concept of settlement finality is important. Transactions may be able to be recalled and some DLTs are integrated in other systems. Furthermore in the case of e.g. bitcoin a transaction is only truly final after several more blocks have been added afterwards. They also briefly touch on cyber security, noting the fact that multiple actors will have to be comprised for a successful attack on the ledger. They also note that if many of the actors on the ledger are less "cyber-aware" it could overall increase the risk of attacks. They note however that it could drastically reduce the costs of reconciliation which is currently necessary is different parties may have different ledgers that do not match.

Regarding the custody layer they see the potential to completely cut out the "chain-of-custodians" that generally exist between an end-investor and his or her securities at a CSD. A distributed ledger could enable end-investors to hold their securities directly and could also enable automatic corporate actions via smart contracts. They do identify the need for a "gatekeeper" to control and limit access to the ledger. This will also be necessary to comply with KYC and AML regulations.

Regarding the clearing layer they identify the potential of real-time (T+0) transactions and the potential to remove the need for clearing houses and CCPs. This could reduce costs and also reduce the amount of "failed" trades. Important for real-time settlement would be integration between the trading venues and DLT as the DLT would need to be involved before the trade is sent to the exchange whereas in the current system it would only be involved afterwards. They note however that the DLT implies a certain level of transparency that will also be necessary to validate

transactions. Traders often like to keep their strategies secret however, something that does not mix well with DLT.
In addition to this analysis the paper presents 3 possible scenarios where DLT could be used in various parts of the post-trade process.

In their first scenario, individual parties and groups of parties use the technology internally to improve their internal processes. This will have an overall small impact as it would leave the current infrastructure and the need for intermediaries. In scenario 2 they sketch a situation where some core market players like a CSD pickup the technology and allow others to access it. This would potentially allow for easy settlement and transparency as supervising authorities could directly access the ledger. In scenario 3 they describe a scenario where issuing parties or a government implements a solution where investors and issuing institutions interact directly. Removing all parties except for the investors and issuers. The main issue here relates to regulation. KYC and AML regulation requires vetting of participants in the financial markets. In addition CSD regulation currently does not account for the possibility of the CSD not being a legal entity, but a DLT. In addition to this the earlier mentioned problem of privacy remains as transaction and potentially identities would be public to all participants.

Benos, Evangelos and Garratt, Rod and Gurrola-Perez, Pedro (2017) [74] of the Bank of England wrote a working paper on the economics of DLT in the financial markets. Their main conclusions are that coordination is likely required for success, that there is a large risk that the first successful initiatives will be able to mostly control this new market. Thus creating a chance that the old intermediaries will be replaced with new network providers. Finally they suggest that the race to deploy a working DLT solution for the financial markets may lead to a less resilient system vulnerable to cyber attacks.

The European Securities and Markets Authority (ESMA) also wrote a report on this topic [75]. They analysed the potential technological and regulatory advantages/disadvantages and challenges of the technology. Most of these are mentioned in the other papers, they primarily relate to privacy, existing legislation, efficiency and transparency. They verified their conclusions by interviewing various respondents about their claims.

Micheler, Eva and von der Heyde, Luke (2016) [76] focus their analysis on

the custody/holding part of the post-trade process. They note that in the current infrastructure there often is a big gap between issuer and investor. This gap is filled by a "chain of custodians". These custodian banks hold the securities on behalf of their end-investors. They can efficiently settle transactions if both counter-parties in trade are a client of the custodian and will otherwise simply move up a step in the chain. This has made it harder for investors to exercise their rights. They believe that DLT could help in removing these intermediaries. An important thing that they note however is that even with DLT intermediaries still pop up. There are exchanges and hosted wallets where you are not in control of your own private key and transactions are often settled off the chain. Though this offers advantages in terms of performance and efficiency one can wonder if this was the original intent of Nakamoto.

Chapter 8

Conclusion

In this thesis we started with an overview of the current post-trade infrastructure. The current post-trade infrastructure consists of various intermediaries performing activities related to clearing and settlement of securities and derivatives trades. These intermediaries operate in a heavily regulated environment (in Europe). With various regulations and directives providing requirements for the intermediaries involved in the process. The need for all these intermediaries can also negatively affect the efficiency of the financial markets however as they will have to communicate and reconcile their data and processes.

The blockchain seems like it can have some added value here, potentially removing intermediaries and improving the efficiency and speed of the post-trade processes. The blockchain is a distributed append-only datastructure that can provide decentralisation, censorship resistance, transparency and accountability to existing processes. It does this by relying on digital signatures, merkle trees and consensus algorithms. Many of these blockchain platforms allow for participants to add their own logic onto this distributed datastructure in the form of smart contracts.

In practice achieving the decentralisation and censorship resistance properties of a blockchain for post-trade is not feasible. Regulatory requirements require a certain amount of central governance. The ability to block participants from using the system or to block or revert transactions in certain cases. Transparency and accountability can be provided by other means as well (by utilising some underlying technologies of a blockchain like digital signatures and merkle trees). Many oft-cited advantages of the blockchain like T+0 settlement and removal of the many intermediaries in the holding chain do not rely on the blockchain at all and can be achieved with traditional

centralised solutions as well. The primary advantages of a blockchain for post-trade processes are the added security if multiple nodes owned by different entities take part in the consensus algorithm and the consistent view of data and processes it provides.

Chapter 9

Abbreviations

AML: Anti money laundering
CCP: Central counter party
CSD: Central securities depository
CSDR: Central securities depositories regulation
DLT: Distributed ledger technology
ECB: European Central Bank
EMIR: European market infrastructure regulation
ESMA: European Securities and Markets Authority
FIX: Financial Information eXchange
IBFT: Istanbul Byzantine Fault Tolerance
KYC: Know your client
MiFID: Markets in financial instruments directive
MiFIR: Markets in financial instruments regulation
OTC: Over-the-counter
PBFT: Practical Byzantine Fault Tolerance
PFMI: Principles for financial market infrastructures
SME: Small and medium-sized enterprise
SWIFT: Society for Worldwide Interbank Financial Telecommunication
T+x: Settlement occurs 'x' days after trade execution

Bibliography

[1] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: (2008). URL: https://bitcoin.org/bitcoin.pdf.

[2] "Wall Street rethinks blockchain projects as euphoria meets reality". In: *Reuters* (Mar. 27, 2018). URL: https://www.reuters.com/article/us-banks-fintech-blockchain/wall-street-rethinks-blockchain-projects-as-euphoria-meets-reality-idUSKBN1H32G

[3] *The Capital Markets Industry: The Times They Are A-Changin'*. URL: https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2015/March/The_Capital_Markets_Industry.pdf.

[4] *SECURITIES ACT OF 1933*. URL: http://legcounsel.house.gov/Comps/Securities%20Act%20Of%201933.pdf.

[5] *SECURITIES EXCHANGE ACT OF 1934*. URL: http://legcounsel.house.gov/Comps/Securities%20Exchange%20Act%20Of%201934.pdf.

[6] *Securities and Exchange Commission v. W. J. Howey Co., 328 U.S. 293 (1946)*. URL: https://supreme.justia.com/cases/federal/us/328/293/.

[7] *Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN.

[8] *The registration of securities holders*. URL: https://ecsda.eu/wp-content/uploads/2016_07_19_ECSDA_Registration_Report.pdf.

[9] Christian Chamorro-Courtland. "Counterparty substitution in central counterparty (CCP) systems". In: *26.3 Banking & Finance Law Review* (2010), pp. 517–538.

[10] *Account segregation practices at European CSDs*. URL: https://ecsda.eu/wp-content/uploads/2015_10_13_ECSDA_Segregation_Report.pdf.

[11] *European Infrastructure - Aite Group*. URL: https://www.aitegroup.com/report/sibos-2013-one-thousand-and-one-reflections.

[12] *T2S Special Series | Issue No 3 | January 2014 | Corporate actions in T2S*. URL: https://www.banque-france.fr/sites/default/files/media/2016/11/08/t2s_specialseries_issue3-janvier2014.pdf.

[13] *Principles for financial market infrastructures*. URL: https://www.bis.org/cpmi/publ/d101a.pdf.

[14] *DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN.

[15] *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=en.

[16] *REGULATION (EU) No 909/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories*. URL: https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014R0909-20160701&from=EN.

[17] *Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0600&from=en.

[18] *Public Register for the Trading Obligation for derivatives under MiFIR (visited 30-06-2019)*. URL: https://www.esma.europa.eu/sites/default/files/library/public_register_for_the_trading_obligation.pdf.

[19] *Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=en.

[20] *CLEARING OBLIGATION AND RISK MITIGATION TECHNIQUES UNDER EMIR (visited on 30-06-2019)*. URL: https://www.esma.europa.eu/regulation/post-trading/otc-derivatives-and-clearing-obligation.

[21] *Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31998L0026&from=EN.

[22] *Fix trading*. URL: https://www.fixtrading.org/standards/.

[23] *Swift standards*. URL: https://www.swift.com/standards.

[24] *ISO 6166:2013*. URL: https://www.iso.org/standard/44811.html.

[25] *LEI*. URL: https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei.

[26] *Business identifier code (BIC)*. URL: https://www.iso.org/obp/ui/#iso:std:iso:9362:ed-4:v1:en.

[27] *ISO2002: Universal financial industry message scheme*. URL: https://www.iso20022.org/.

[28] *ISO 17442:2012: Financial services – Legal Entity Identifier (LEI)*. URL: https://www.iso.org/standard/59771.html.

[29] Ittay Eyal and Emin Gün Sirer. "Majority is not enough: Bitcoin mining is vulnerable". In: *Communications of the ACM* 61.7 (2018), pp. 95–102.

[30] *Hashrate Distribution (visited on 30-06-19)*. URL: https://www.blockchain.com/en/pools.

[31] *Pool Stats (visited on 30-06-19)*. URL: https://btc.com/stats/pool.

[32] *Pool distribution (visited on 30-06-19)*. URL: https://www.blocktrail.com/BTC/pools.

[33] *Blockchain size - visited on 13-02-2019*. URL: https://www.blockchain.com/charts/blocks-size?.

[34] *Bitcoin Transaction Fees*. URL: https://bitcoinfees.info/.

[35] Alex de Vries. "Bitcoin's Growing Energy Problem". In: *Joule* 2.5 (2018), pp. 801–805.

[36] *Bitcoin energy consumption index - Digiconomist*. URL: https://digiconomist.net/bitcoin-energy-consumption.

[37] *Whitepaper:Nxt*. URL: http://nxtwiki.org/wiki/Whitepaper:Nxt.

[38] *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. URL: https://peercoin.net/whitepapers/peercoin-paper.pdf.

[39] *EOS*. URL: https://eos.io/.

[40] Miguel Castro, Barbara Liskov, et al. "Practical Byzantine fault tolerance". In: *OSDI*. Vol. 99. 1999, pp. 173–186.

[41] *Sharding introduction R&D compendium*. URL: https://github.com/ethereum/wiki/wiki/Sharding-introduction-R&D-compendium.

[42] *Plasma: Scalable Autonomous Smart Contracts*. URL: https://plasma.io/.

[43] *Raiden network*. URL: https://raiden.network/.

[44] *Lightning network*. URL: https://lightning.network/.

[45] *Reconciliation Technology Solutions in 2014: Recs Get Ready to Rumble ...* URL: https://www.aitegroup.com/report/reconciliation-technology-solutions-2014-recs-get-ready-rumble-%E2%80%A6.

[46] *Shareholder Rights Directive II*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0828.

[47] *Post Trade explained*. URL: https://www.afme.eu/globalassets/downloads/publications/afme-post-trade-explained.pdf.

[48] *Cryptocurrency anti-money laundering report*. URL: https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf.

[49] *On Public and Private Blockchains*. URL: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

[50] *Ethereum Name Service*. URL: https://ens.domains/.

[51] *Proxy Patterns*. URL: https://blog.zeppelinos.org/proxy-patterns/.

[52] *Proxy Delegate*. URL: https://fravoll.github.io/solidity-patterns/proxy_delegate.html.

[53] *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a framework for the recovery and resolution of central counterparties*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0856.

[54] *CSDR: Frequently asked questions*. URL: https://ec.europa.eu/info/file/42490/download_en?token=dNRVBCWc.

[55] *The DAO (organisation)*. URL: https://en.wikipedia.org/wiki/The_DAO_(organization).

[56] *The Multi-sig Hack: A Postmortem*. URL: https://www.parity.io/the-multi-sig-hack-a-postmortem/.

[57] *Securities settlement systems: delivery-versus-payment in a distributed ledger environment – Stella project report phase 2*. URL: https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf.

[58] *Delivery versus Payment on Distributed Ledger Technologies - Project Ubin*. URL: http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20DvP%20on%20Distributed%20Ledger%20Technologies.pdf.

[59] *Bitcoin price - coinmarketcap.com*. URL: https://coinmarketcap.com/currencies/bitcoin/.

[60] *Cryptocurrency prices - blockchain.com*. URL: https://www.blockchain.com/prices.

[61] *Bitcoin price - coindesk.com*. URL: https://www.coindesk.com/price/bitcoin.

[62] *Tether*. URL: https://tether.to/.

[63] *Paxos Standard (PAX)*. URL: https://www.paxos.com/pax/.

[64] *Blockchain in the cash and securities settlement space: Utopia or reality?* URL: https://www.youtube.com/watch?v=C-9Zo5FQPeo&feature=youtu.be.

[65] *ECB has no plan to issue digital currency: Draghi*. Sept. 14, 2018. URL: https://www.reuters.com/article/us-ecb-bitcoin/ecb-has-no-plan-to-issue-digital-currency-draghi-idUSKCN1LU1JM.

[66] *Basis*. URL: https://www.basis.io/.

[67] *MakerDAO*. URL: https://makerdao.com/en/.

[68] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

[69] *RFC6962 - Certificate Transparency*. URL: https://tools.ietf.org/html/rfc6962.

[70] Katya Malinova and Andreas Park. "Market Design with Blockchain Technology". In: (2017). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2785626.

[71] Michael Mainelli and Alistair Milne. "The impact and potential of blockchain on the securities transaction lifecycle". In: (2016). URL: https://swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL-1.pdf.

[72] Andrea Pinna and Wiebe Ruttenberg. "Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution?" In: (2016). URL: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

[73] David C Mills et al. "Distributed ledger technology in payments, clearing, and settlement". In: (2016). URL: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

[74] Evangelos Benos, Rod Garratt, and Pedro Gurrola-Perez. "The economics of distributed ledger technology for securities settlement". In: (2017). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3023779.

[75] *Report: The Distributed Ledger Technology Applied to Securities Markets*. URL: https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf.

[76] Eva Micheler and Luke von der Heyde. "Holding, clearing and settling securities through blockchain technology creating an efficient system by empowering

asset owners". In: (2016). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786972.