DEGREE PROJECT IN MATHEMATICS,
SECOND CYCLE, 30 CREDITS
STOCKHOLM, SWEDEN 2017

Counterparty Credit Risk on the Blockchain

ISAK STARLANDER

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF ENGINEERING SCIENCES

Counterparty Credit Risk on the Blockchain

ISAK STARLANDER

Degree Projects in Financial Mathematics (30 ECTS credits)
Degree Programme in Industrial Engineering and Management
KTH Royal Institute of Technology year 2017
Supervisor at Safello: Frank Schuil
Supervisor at KTH: Boualem Djehiche
Examiner at KTH: Boualem Djehiche

TRITA-MAT-E 2017:69
ISRN-KTH/MAT/E--17/69--SE

Royal Institute of Technology
School of Engineering Sciences
KTH SCI
SE-100 44 Stockholm, Sweden
URL: www.kth.se/sci

Abstract

Counterparty credit risk is present in trades of financial obligations. This master thesis investigates the up and coming technology blockchain and how it could be used to mitigate counterparty credit risk. The study intends to cover essentials of the mathematical model expected loss, along with an introduction to the blockchain technology. After modelling a simple smart contract and using historical financial data, it was evident that there is a possible opportunity to reduce counterparty credit risk with the use of blockchain. From the market study of this thesis, it is obvious that the current financial market needs more education about blockchain technology.

Keywords: Counterparty Credit Risk, Expected Loss, Blockchain, Smart Contracts

Sammanfattning

Motpartsrisk på blockkedjan

Motpartsrisk är närvarande i finansiella obligationer. Den här uppsatsen undersöker den lovande teknologin blockkedjan och hur den kan användas för att reducera motpartsrisk. Studien har för avsikt att täcka det essentiella i den matematiska modellen för förväntad förlust, samt en introduktion om blockkedjeteknologi. Efter att ha modellerat ett enkelt smart kontrakt, där historiska finansiella data använts, var det tydligt att det kan finnas en möjlighet att reducera motpartsrisk med hjälp av blockkedjan. Från marknadsundersökningen gjord i studien var det uppenbart att den nuvarande finansiella marknaden är i stort behov av mer utbildning om blockkedjan.

Nyckelord: Motpartsrisk, Förväntad Förlust, Blockkedjan, Smarta Kontrakt

Acknowledgements

I would like to thank Boualem Djehiche at KTH for supervising me in my work and for giving valuable feedback. I also want to thank my supervisor at Safello, Frank Schuil, who not only inspired me with his ideas, but also showed a lot of generosity with his knowledge and network in the field of blockchain. Last but not least, I am grateful for the support given by my family and friends troughout the process of this thesis.

Stockholm, October 2017

Isak Starlander

List of Figures

List of Tables

Contents

Chapter 1

Introduction

Trading financial derivatives is always a risky business. One risk is that a counterparty cannot pay what is obligated. This is known as counterparty credit risk. In financial risk analysis, this is modelled mathematically as

$$EL = PD \cdot EAD \cdot LGD$$

which is known as the expected loss (EL). The three factors PD, EAD and LGD are determined to evaluate the expected loss.

Meanwhile, there is a new technology known as blockchain which has gotten more and more traction in recent years, due to its many positive features. Amongst others, the possibility to run self-executing programs on the decentralised platform. A feature which could be beneficial for more frequent evaluations of the expected loss, thus potentially reducing the risk.

The purpose of this master thesis is to investigate the financial problem of counterparty credit risk and to suggest how blockchain could be used in order to minimise and make more precise evaluations of expected loss.

This master thesis is split into six different chapters. In this chapter there is an introduction to the chosen thesis subject, i.e. development of blockchain and regulations of counterparty credit risk. Furthermore Chapter 1 specifies delimitations and practical implementation of the master thesis.

Thereafter, in Chapter 2-3 the concepts of counterparty credit risk and blockchain technology will be presented in depth. Specifically how to mitigate risk in Section 2.1, and the three corner stones of counterparty credit risk, exposure at default, probability of default and loss given default are presented in Section 2.2-2.4 respectively. Whereas the sections of Chapter

3 are all about the background, technology, smart contracts and also initial coin offerings, which is a new way of fund raising crypto projects.

Chapter 4 is split into approaches for counterparty credit risk on the blockchain in Section 4.1, simulations of certain approaches in Section 4.2, and lastly the suggested method to find out where the current market stands in Section 4.3.

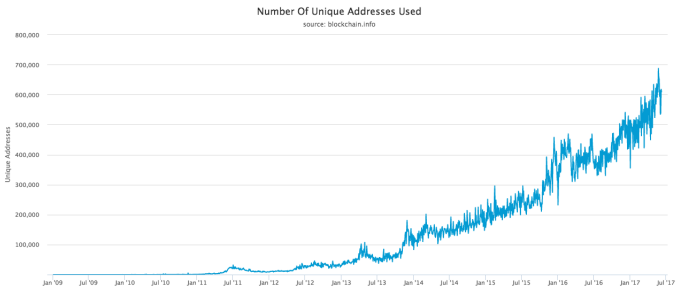
Moreover, Chapter 5 presents the results of both the literature study of blockchain technology and counterparty credit risk, as well as the interview study. In Section 5.3 a discussion regarding the results and the methodology is held. Finally, in Chapter 6 a conclusion of this master thesis is summarised.

The underlying technology for this thesis, Blockchain, has so far mainly been a subcultural knowledge which has spread by buzz marketing. Meaning an informed user talks with his/her peers about the product and they join the network. The product or service takes longer to become mainstream this way, however it establishes a solid foundation on the market instead. If the word of mouth marketing is successful, this may lead to an exponential increase of the service. Cryptocurrencies such as Bitcoin, Ethereum and many others have had their distribution this way and it can be seen from Figure 1.1 & 1.2 that the market has finally gotten up to speed with the technology. Furthermore, the increase of users in the network advocates the potential for future global usage.

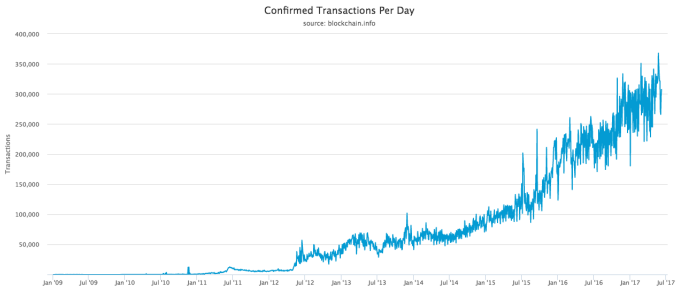
Continuous analysis of the two major underlying blockchains is available on the web. Information regarding the Bitcoin blockchain [1] and Ethereum blockchain [2] respectively provide the following plots that show user and value development for the underlying technology.

International finance and banking regulations have been agreed upon, lead by the Basel Committee on Banking Supervision. Since the first regulation in 1998, two updates have followed in 2006 and 2013 respectively. The series of banking regulations are know as the Basel Accords (or Basel I, II and III) and aim to act as a regulation for banking practices on an international level.

The Basel II was enforced because of the need to ensure liquidity of banks by expanding rules of a minimal capital requirement. This was first established under Basel I, that the financial institutions need to set aside capital for potential losses from investment and lending. By enforcing this internationally the Basel II attempted to prevent any nation to develop an



(a) Unique user addresses



(b) Daily confirmed transactions

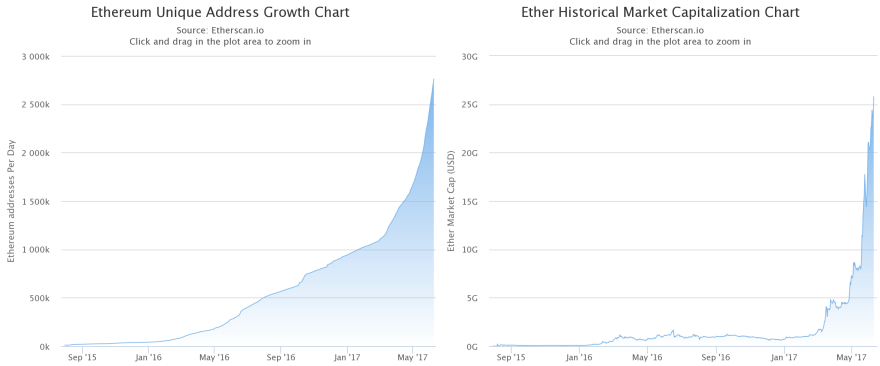
Figure 1.1: Bitcoin blockchain development

unfair system with competitive advantage. The main difference between the primary and secondary Basel regulation is that the latter incorporates credit risk of assets held by financial institutions to determine regulatory capital ratios.

The Basel III was implemented largely in response to the credit crisis of 2007-2008. The third Basel accord is intended to strengthen the bank capital requirements by increasing the bank liquidity and decrease bank leverage. Professionals within the banking industry can prove their understanding of the Basel III regulations by achieving a certification.

This master thesis will be delimited to a presentation of the underlying blockchain technology, in order to explain the concept thoroughly for the recently introduced readers. Moreover, it is delimited to counterparty credit risk and specifically to the related area of expected loss. These concepts will be combined in simulations and examples of approaches. Lastly, the report will summarise comments from the current financial market, concerning risks and development related to blockchain.

The practical implementation of this thesis is limited to further research



(a) Unique user addresses (b) Market Capitalization

Figure 1.2: Ethereum blockchain development

on applications of blockchain technology as well as guidelines on how to approach the current financial market. Highest wishes are that it will function as a springboard for other interested on writing their master thesis on this subject, by presenting the underlying technology thoroughly.

Chapter 2

Counterparty Credit Risk

Derivatives in finance are instruments that derive their value from the performance of certain assets, interest or FX rates, or indexes. Common ones are debt obligations, swaps, futures, options and forwards. These may all be traded on their own or in various combinations.

When parties have agreed to trade these derivatives, certain risks are present. Either party of the agreement may lose money. Counterparty credit risk (CCR) is the risk that an obligor will default, i.e. that a counterparty will not pay as obligated on the financial contract. Counterparty risk is a two way risk and should be considered by both parties when evaluating a contract.

Through implementation of the Basel II framework, banks can evaluate the so called expected loss (EL). EL is part of the capital that banks need to hold, in order to be protected against financial risks when doing business. The other part is the unexpected loss (UL), which intuitively is less predictable and more difficult to evaluate. The EL is thus the loss that can be estimated and it is described as the product of three different parameters, as in Eq. (2.1). These three are probability of default (PD), the exposure at default (EAD), and also the loss given default (LGD). PD is the probability for a counterparty to default, given a certain trade. The EAD is the estimated amount deviating from the deal, expected at the default of the obligor. The LGD on the other hand is the percentage of the exposure that the bank (a party) may lose if the obligor (counterparty) defaults.

$$EL = PD \cdot EAD \cdot LGD \tag{2.1}$$

The following chapter will cover some of the mathematics and related sub-

jects around the estimation of these exposures. In Section 2.1 we will cover some methods used to mitigate risks in obligations with counterparty risk.

The following Section 2.2 will introduce the standardised approach for estimating counterparty credit risk (SA-CCR), which covers the evaluation of the EAD.

In Sections 2.3 & 2.4 we will move on to the mathematics behind the PD and LGD respectively. And thus cover the full set of parameters to consider in estimation of the EL.

2.1 Mitigation of CCR

2.1.1 Selection of Counterparty

The simplest and most obvious way to mitigate the counterparty credit risk is to make contracts with institutions or vehicles that have a very small probability of defaulting [3]. Although, before the financial crisis of 2008 many still believed in the concept of being "too big to fail", which today is known to be a somewhat modified truth.

Another method is to use so called central counterparty clearing houses (CCPs), i.e. organisations that help facilitate trading done in the market, in order to reduce the financial risks. CCPs work as an intermediary which uses collateral and netting agreements in financial contracts of large scale as mechanisms for reducing CCR. Hence, it is possible to extensively lower the CCR by making the derivative trades in exchanges, instead of in the OTC market [4].

2.1.2 Collateral

Collateral is referred to an amount posted by at least one of the parties of the agreement which is to act as a security, i.e. in order to mitigate CCR. The agreement can be set up in many different ways. However, cash is the most common way, whereas real estate and stocks are other examples of what can be used as collateral.

In relation to collateral agreements are margin agreements that further mitigate the CCR of a contract. A margin agreement involves counterparties posting collateral over time as a result of the changes in a volatile market. The agreement includes a variation margin which depends on the value of the contract and is paid at a predetermined margin period which typically is on a

daily basis, weekly or monthly. In some cases the agreement also includes an initial margin, where the less credit worthy counterparty posts the collateral upfront. The posting itself can be subject to a predetermined minimum transfer amount (MTA) which prevent unecessarily small transactions, and a threshold (TH) above which level a party has to start post collateral.

2.1.3 Netting Agreements

The essence of netting agreements is to offset different exposures with each other, such that a positive exposure can cancel a negative one with the same specific counterparty. This is commonly used at banks that have a range of contracts that are sold and bought with their different counterparties, and thus reduce the total exposure to this counterparty. However, for this to be the case, a netting agreement (NA) has to be declared between the parties which then can be enforced in the event of a bankruptcy or any other default by one of the counterparties. The NA can be established to cover all contracts between the parties, or otherwise some specific types of contracts. A netting set is known as the subset of contracts that are subject to a NA, in case of default. Thus implying that the same counterparty may own a number of netting sets. Through netting agreements the total exposure can be expressed as:

$$Exposure = \sum_{i \notin \{NA\}} \max\left(V_i, 0\right) + \sum_{k} \max\Big(\sum_{i \in \{NA_k\}} V_i, 0 \Big) \tag{2.2}$$

where then NA_k is the kth netting agreement and V_i is the value of contract i and of course, if $i \notin \{NA\}$ these are the contracts that are not covered by a netting agreement.

2.2 Standardised Approach for Counterparty Credit Risk

The standardised approach for counterparty credit risk (SA-CCR) is since the first of January 2017 the new universal approach towards evaluating counterparty credit risk. It replaced an older method known as the current exposure method (CEM). CEM was replaced mainly due to its inability to adequately capture the risk. In particular, it neither differentiated between margined and unmargined transactions, nor captured the levels of volatility

observed. Furthermore, CEM was not built to evaluate EAD which became a requirement as Basel III was introduced. [5, 6]

Under the regulation of SA-CCR, EAD is defined as the sum of the replacement cost (RC) and an add-on typically known as the potential future exposure (PFE) or rather

$$EAD_{SA-CCR} = \alpha \cdot (RC + PFE) \tag{2.3}$$

where $\alpha = 1.4$ is a multiplier set by the Basel Comittee for the Internal Model Method. The multiplier may vary from somewhere between 1.1 for global dealer portfolios, and 2.5 for new users of derivatives. It is decided that institutions use the specified factor of 1.4, but they are also given the possibility to estimate an α specific to the bank's portfolio. [6, 7]

2.2.1 Replacement Cost

In a written contract where there is no collateral agreement, then the RC is defined as the mark-to-market (MtM) value of the derivative, meaning the current value compared to the initial value of the derivative. In the presence of any kind of collateral agreement the situation for evaulating the replacement cost is quickly getting more complex which is illustrated by Figure 2.1. A clear distinction between the two cases of a collateralised agreement and a non-collateralised agreement can be seen.

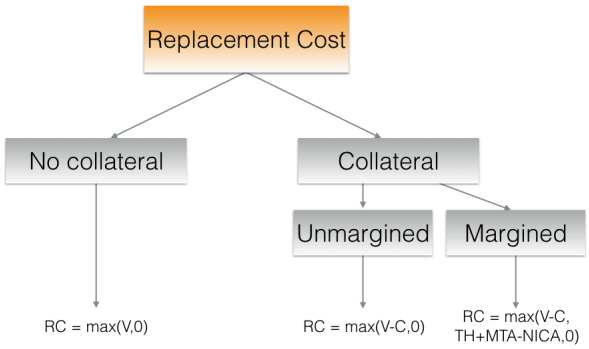


Figure 2.1: Differentiation between replacement cost under posting of collateral and not.

Under the SA-CCR the collateral agreements are distinguished between margined and unmargined transactions, where the latter case is a simpler form of collateral agreement where the RC basically is the MTM value V

reduced by the collateral, C, posted to the bank. Important to notice is that the RC is always floored by zero, ie. you cannot be accountable for over-collateralisation and thus get a negative RC.

In a margined agreement however, the RC takes a value which is the maximum of $V - C$ and the largest exposure that would not trigger a call for collateral. This largest exposure is known as the sum of a threshold (TH) value and the minimum transfer amount (MTA), reduced by the net independent collateral amount (NICA). In other words, $TH + MTA$ represents the level over which a collateral transaction will take place. Whereas NICA represents the collateral posted by the counterparty that may be kept in case of a default. Thus $TH + MTA - NICA$ corresponds to the largest exposure which would not trigger a variation margin call (being a requirement of charge, to cover the observed changes in replacement cost of a derivative instrument).

2.2.2 Potential Future Exposure

The future uncertainty of a contract's value is covered by the add-on known as the potential future exposure (PFE). It is the factor which is supposed to cover volatility in the exposure of a contract and is for a netting set defined as:

$$PFE = multiplier \cdot AddOn_{aggregate}, \quad AddOn_{aggregate} = \sum_j AddOn_j \quad (2.4)$$

where the *multiplier* is present to account for over-collateralisation and in that way reduce the minimum capital requirement for the contract. The aggregated add-on, $AddOn_{aggregate}$, is a function of the different asset classes, j, that are present in the contract. Each of these asset classes are dependent on their hedging sets within each class when calculating them and thus we denote the add-on for each asset class by $AddOn_j$.

A framework for calculating the PFE of the future MtM value is necessary, particularly for banks due to their large portfolios, in order to compare with credit limits, or to price and hedge the CCR. The framework implemented is universal in order to calculate the entire exposure distribution at any future date.

Another framework than the add-on framework is usage of Monte Carlo simulation. Scenario generation and instrument valuation are essential for this framework. The scenario generation evaluates potential market scenarios

for a fixed number of simulation dates, and the instrument valuation is made for each trade in a counterparty portfolio. The outcome of this procedure is a set of realisations for the counterparty exposure at each simulation date, where each realisation is related to a certain market scenario.

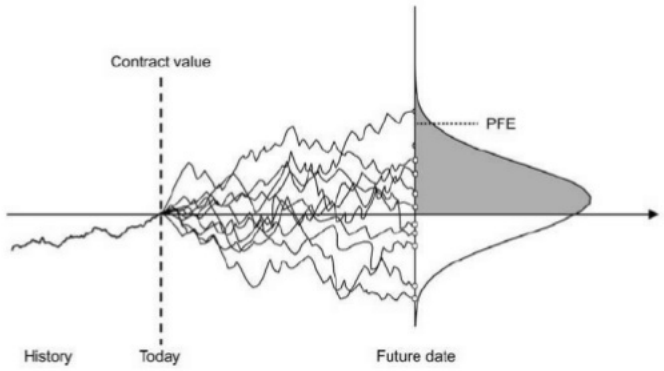


Figure 2.2: A typical Monte Carlo simulation of PFE

Due to the computational intensity of this method, the simulation dates are commonly restricted to daily or weekly intervals up to a month, monthly up to a year, and yearly up to five years, etc. Similarly for the market scenarios, which generally are restricted to a few thousand.

In order to generate the scenarios one needs to take into account certain price factors such as FX rates, interest rates, equity prices, and commodity prices to name a few. One method to generate the price factors is known as the path-dependent simulation (PDS), which describes a potential trajectory for a market scenario up to maturity. The scenarios are commonly stochastic differential equations (SDE) that describe Markovian processes. E.g. for modelling FX rates and stock indices the common geometric Brownian motion is given by $dX(t) = \mu(t)X(t)dt + \sigma(t)X(t)dw_t$. From this SDE one could then specify the PDS as

$$X(t_k) = X(t_{k-1}) \exp\left([\bar{\mu}_{k-1,k} - \frac{1}{2}\bar{\sigma}^2_{k-1,k}](t_k - t_{k-1}) + \bar{\sigma}^2_{k-1,k}\sqrt{t_k - t_{k-1}}Z\right)$$

where Z is a standard normal variable and

$$\bar{\mu}_{j,k} = \frac{1}{t_k - t_j} \int_{t_j}^{t_k} \mu(s)ds, \qquad \bar{\sigma}^2_{j,k} = \frac{1}{t_k - t_j} \int_{t_j}^{t_k} \sigma^2(s)ds$$

with $\mu(t)$ being the time-dependent drift and $\sigma(t)$ the time-dependent volatility.

The potential future exposure is then obtained by computing a high-level (typically 95%) percentile of the different scenarios at each simulation date. This corresponds to the future MtM value and can be used to compare with e.g. credit limits of the counterparty.

2.3 Probability of Default

The probability for an obligor to default in the coming year is known as probability of default (PD). There are two philosophies on how to describe the behaviour of PD and these are known as point-in-time (PIT) and through-the-cycle (TTC). There are no fixed definitions on PIT and TTC, but some minor consensus on how to describe them. Generally speaking, PIT PD is described as a rating system that follows the business cycle and changes over time. Whereas TTC PD instead is more or less unaffected by the economical conditions. There is also a wide range of mixtures between these two philosophies which take both into consideration.

2.3.1 Estimating the PD

Different methods to determine PD are to study historical data and make regression analysis on different parameters, and another method is to evaluate observations of asset prices. As the two philosophies generally have relations to economic conditions or not, when talking about risk factors the two approaches regard different factors. The risk of macroeconomic variables, or the idiosyncratic risk, meaning the obligor specific risks.

We know that PD is the expected defaults, but by considering the actual defaults one may instead find the default frequency (DF) defined as

$$DF = \frac{\textit{Defaulted obligors}}{\textit{Total number of obligors}} \tag{2.5}$$

Another way of assessing the philosophies PID and TTC is their relation to

the DF in the following manner

$$Portfolio\ DF = \sum_y \sum_r \frac{N_y^r DF_y^r}{N_y}$$

$$Portfolio\ PD = \sum_y \sum_r \frac{N_y^r PD^r}{N_y}$$

where y is the year, r is the rating and N is the total number of obligors.

By using this measurement it is possible to compare the estimate with the real defaults that have occurred. If the PD follows the DF perfectly it is said to be a PIT approach, if it instead compares to the mean of the DF it is a TTC approach.

2.4 Loss Given Default

In the case of a default, the percentage of the EAD that is expected to be lost is known as the loss given default (LGD). It is defined as the percentage that is not expected to be recovered in the event an obligor defaults, or more specifically:

$$LGD = 1 - RR \tag{2.6}$$

where RR is the recovery rate, i.e. the share of an asset that is recovered.

In accordance with Basel Regulation (BIS, 2006, §460) the estimates of LGD must include workout costs from collecting the exposure, such as lawyers and similarly. Moreover the estimates are dependent on the type of exposure that is at hand. Thus implying that the LGD theoretically can be larger than one. However, as this is not a common case, it is assumed that $LGD \leq 1$ and estimates are therefore capped at one.

2.4.1 Estimating the LGD

There are several ways of estimating the LGD of a counterparty. Some suggestions of these are ratings, meaning that each counterparty should have a rating in order to be mapped onto an agreed default probability. Another, by using credit spreads which become an important aspect for hedging counterparty risk. Also, estimation of the counterparties recovery rates is important as it has an immediate relation to the LGD. The estimates can be dependent on characteristics of the counterparties and also the seniority of a claim should be made, i.e. the order in which the claim should be repaid.

Apart from these approaches there are two approaches stated in the Basel Regulation known as the foundation and advanced approach. Under the sooner all senior claims on corporates and banks not secured by collateral are assigned a 45% LGD. All subordinate claims on corporates and banks are assigned a 75% LGD. The latter approach states that subject to certain minimal conditions, a supervisor may permit banks to use their own internal estimates of LGD for exposures.

Chapter 3

Blockchain Technology

Blockchain is the missing piece of the internet, which finally has started to get some traction. It is the underlying technology which enables users to make transfer of value over the internet, without doubting who owns the assets. It is a futuristic technology with the potential to make a complete change in a variety of industries. Maybe the industries and organisations of the future are all managed in a decentralised and autonomous manner, and maybe sharing of information is publicly available with the major benefit of knowing exactly when and where information is transferred. Tomorrow's technology gives back the ownership to the individuals and is here to stay.

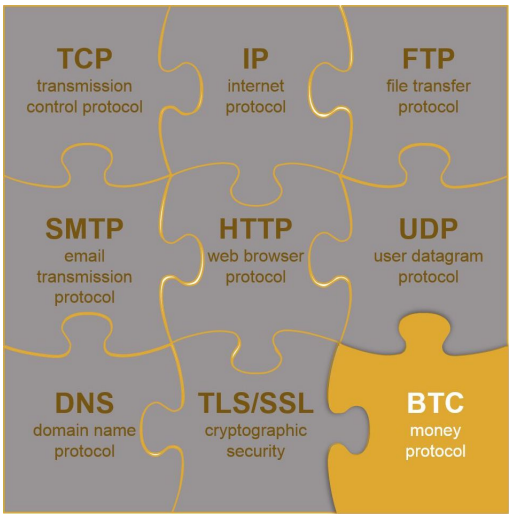


Figure 3.1: Blockchain as the missing puzzle piece of the internet.

3.1 Background of Blockchain

Blockchain technology was first introduced in 2009, when the today well known cryptocurrency Bitcoin was launched. It is a result from the precursor, the Cypherpunk movement, who wanted less control by the government and more freedom to the people. The first report on the technology was posted in 2008, under the pseudonym(s) Satoshi Nakamoto. This particular white paper focused mainly on describing the idea of Bitcoin and the underlying technology which is today known as blockchain. Curiously the author(s) of the white paper, as well as the founder(s) of Bitcoin, are still up to this date unknown.

The idea of the blockchain is to have an open, transparent, distributed, online ledger in which anyone with internet access can participate. The unique solution that the blockchain technology provides, contrary to previous digital currencies, is a solution to the double-spend problem. The double-spend problem is the possibility for a user of a digital currency to spend the same coin several times.

Some key features of blockchain are: a higher level of decentralisation; identity management and security through cryptography; usage of the peer-to-peer (P2P) network for consensus ruling. Furthermore, the fact that the technology is kept open source is highly favourable from a development perspective. Decentralisation was and still is the fundamental idea, as it was seen as unfavorable to have a middle-hand in transactions of value.

3.1.1 Areas of Application

The number of possible implementations of the blockchain technology is vast. Amongst others, personal identity numbers and decentralised voting could become realised within a foreseeable future.[8] The former has already started to develop by request of the UN [9, 10].

Some applications of the blockchain technology that are already available on the market are of course Bitcoin wallets, to replace or function side by side fiat currency; Steem, which is a decentralised social media platform where valuable contributions are rewarded; Storj, Sia and MaidSAFE all provide decentralised cloud storage with their own niche; Golem is a decentralised supercomputer which provides computing power to anyone; BitShares offers financial services such as exchanges and banking; Augur is a decentralised

platform for forecasting on prediction markets; GameCredits is a payment gateway for the gaming industry; and Basic Attention Token which is a decentralised currency for digital advertising. All of these usecases emphasise the fact that the industry for blockchain technology is booming.

3.1.2 How is Decentralisation Achieved?

Decentralisation is a vague concept as it is difficult to tell how decentralised something is. When it comes to blockchain technology there are several aspects to consider. First, who has the power on the blockchain? Secondly, what can be decentralised? Then last, where is decentralisation a good idea?

The power over a blockchain is commonly divisible. For instance there is the core developer team who write the "rulebook" which most users follow by using their code. However, miners have power as well as they write the history which is only consistent with the miners' consensus rules. Moreover, the investors have power as they determine whether the blockchain currency has any value and in case of a hard fork they decide which fork will win. Merchants and their customers also have power, as they are the ones generating the primary demand and thus drive the long-term price. Without payment services transactions could not be handled in the first place, so merchants and investors would simply have to follow them, meaning they have power. The truth is however that all of these are required for the ecosystem to fully function. Thus decentralisation is in one sense achieved by distributing the power between all the market participants.

Several categories can be made of that which is possible to decentralise. The simplest covers things that are purely digital such as digital storage, random number generation and lotteries, etc. A second category are things that can be digitally represented, such as real world currency, stocks and other assets. Complex contracts such as for crowd funding, and other financial derivatives is another example. However, financial derivatives not on the blockchain might require a data feed, which obviously could be decentralised as well. Markets and auctions could be decentralised, as well as autonomous agents working with contracts, data feeds, voting etc. [11]

Mainly decentralisation in a blockchain manner refers to technological alternatives to institutions such as e.g. legal-, social-, or financial institutions. Where one can make agreements outside the current legal system, where disputes can be solved by a third trusted party instead of today's court. Have

decentralised payments and financial derivatives, without the bank handling the transactions and agreements. Or even tax payments handled by a decentralised social system.

3.2 Technology Behind Blockchain

A blockchain is built and kept secure by using cryptography, it is a chronological chain which book keeps transactions of value. The ledger is maintained by so called miners. The blockchain ledger is linked by hash pointers. An illustration of this complex idea can be seen in Figure 3.2.

It is somewhat relevant to comprehend parts of the underlying technology in order to fully understand blockchain and its power. At a first glance the technology may seem too complex to understand. Nevertheless, with some basic knowledge of underlying concepts, it all becomes more tangible.

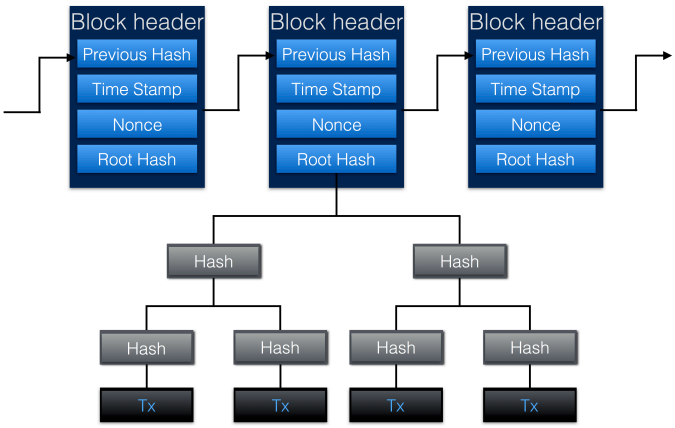


Figure 3.2: Visualisation of the blockchain setup with blocks and the Merkle tree of transaction data.

The block consists of two major parts, the block header which is important for the mining and the transaction data. The block header contains hash for the current block, as well as a pointer to the previous block. Along with this, the block header contains a time stamp for the book keeping and some puzzle information being the nonce. The Root Hash is a pointer to the transaction data, which holds a so called Merkle tree which keeps track of the different transactions that have been made in this block.

3.2.1 Cryptographic Hash Functions

A cryptographic hash function is a mathematical function which has three essential attributes.

1. Can take any string as an input and produces a fixed size output, often 256 bites.

2. It needs to be efficiently computable.

3. It needs to be collision free. I.e. nobody can find any x and y s.t. $x \neq y$ while $H(x) = H(y)$. The collisions may exist, but it should be computationally impossible to find them.

Hashes are both practical and useful as message digests since they commonly are smaller than the whole file containing the message, but still are comparable.

Cryptography is used for identity management, where a mathematical process known as the Elliptic Curve Digital Signature (ECDSA) is used to separate a signature from a verification, by using properties of an elliptic equation of the form:

$$y^2 = x^3 + ax + b$$

The signature is represented by a securely stored private key, i.e. the key which states ownership and enables users to "speak for themselves". The verification is represented with a public key, i.e. a key known to everyone that can be used to distribute transactions and thus find the matching private key in the network.

Another area of application of cryptographic hash functions is for the hash pointer, which is pointing to a source of some stored information. With these pointers one can build data structures (or blocks) that become tamper-evident, meaning that if some information is changed in a block, this becomes evident as the hash no longer will match with the pointer. A binary tree of hash pointers is known as a Merkle tree and is commonly used to store the transactions in a block. Its main advantages are the ability to hold many items, but only needs to remember the root hash and also to make it quicker for controls as one only needs to evaluate $O(\log n)$ items instead of $O(n)$.

Moreover hash functions are used for the so called hash puzzles, or nonces, which are key driving factors of the blockchain distributed ledger. These hash

puzzles are part of every block and it is a competition to find the correct match by making computational guesses for the corresponding nonce.

3.2.2 Peer-to-peer Network and Consensus

Blockchain technology is built to be used as a peer-to-peer (P2P) network with participants as nodes and with a random topology which makes it easy to join and leave the network.

Transactions that are broadcasted to the network are propagated from node to node and each node adds the transaction to their own history of transactions. Nodes propagate a transaction if it is valid with the current blockchain, if it has not been seen before (to avoid infinite loops of propagation), and if it does not conflict with any other transaction that is already propagated (such as to avoid double spends). These are all "sanity checks" that all honest nodes would follow, however there are no rules that a node has to follow, simply some guidelines.

Because of the possibility of transactions or blocks to conflict each other, the default behaviour is to accept the first heard of. As the chain of transactions become longer the true blockchain emerges as a result of the consensus of the network, meaning the largest chain rules the blockchain.

Example - Disagreement and reaching consensus

Alice, Bob and David are all nodes in the P2P-network they constitute. Alice has made a transaction to Bob, but has tried to double-spend by also sending the same amount of value to herself and then validating that transaction in her protocol instead. Bob has received the money from Alice and naturally validates that transaction. Now Alice has a block with the transaction from her to herself, whereas Bob has a block with the transaction from Alice to himself. In this simplified case David, who is an honest friend of Alice, learns that she has done this malicious double-spend. David acts in favor of Bob and agrees with his blockchain, rather than with Alice's. So consensus rules out the double-spend and the longest chain is now that of Bob and David, so Alice simply has to follow that blockchain anyway.

> In a larger scale it all boils down to where the most hash power lies and which blocks reaches the nodes first and which blocks that are validated first. In this sense consensus provides security, provided that a majority of the hash power on the network is not malicious.

Propagation of a block is nearly identical to that of a transaction. It has to meet the hash target, have all valid transactions, and also the block should build upon the current longest chain. As for the transaction propagation, these guidelines are simply "sanity checks" that honest nodes can follow. Each node is however free to choose for itself.

3.2.3 Mining and Incentives

So far we have covered propagation of information to the network. But, why would nodes choose to participate in the network by spending electricity, i.e. money, on propagating other peoples' transactions? If it was not for the built in incentives in the blockchain, this might not have been the case. However, as it is designed, each transaction contains a minor amount of value which can be collected if the transactions are added to the blockchain. Moreover, by finding a new block and adding it to the blockchain you are rewarded with a block reward of some larger amount of the currency which the blockhain provides.

As these rewards have been comparatively big, combined with the increasing rate of cryptocurrencies' value, it is only natural that people have tried to find out ways of getting more rewards. As the propagation of information and computation of the so called hash puzzles is closely related to the computational power of a node, you can increase your rate of finding blocks by increasing your computational power. For some blockchains this has lead to a few nodes that have a majority of the computational power of the network and are the ones that drive the propagation mechanism of the technology. These nodes are called miners and the block rewards these nodes want to obtain are commonly known as mining rewards.

By understanding this need of incentive for the miners to maintain the blockchain, you can also understand that whatever you want to use the blockchain for, it is necessary to have some underlying driving force. Workers

for the network want to obtain something of value in exchange for providing their services of propagating information.

3.2.4 Forking the Blockchain

Due to the consensus property of blockchain, the network can agree to make changes to the blockchain. There are two different categories of changes that can be made. Either the network decides to make changes to system, or software, which is possible to run parallel to the previous blockchain. This is known as a soft fork. Or alternatively, the network decides to make larger changes, such as to the operational codes, by changing integrated block size limits, or by fixing major bugs. This would be known as a hard fork.

A soft fork is generally created by adding some metadata to the transactions, or "colour" as it is sometimes called. This allows part of the network to read some extra underlying meaning of a transaction, such as e.g. ownership of a financial derivative. The rest of the network can still propagate the transaction, but might not be able to understand the extra meaning of it. The advantage of this is that you can build new services, that uses the large blockchain market capitalisation for security, but has new features.

A hard fork is more rarely made, as these affect the whole network in a much larger sense. There are currently many hard forked blockchains from the original Bitcoin blockchain, in these forks changes to mining rate, bug fixes, better cryptography, or other operational codes have been added to alter the usage of the blockchain. The second largest blockchain is at the moment the Ethereum blockchain, which itself has hard forked four times shown in the following example.

Example - Hard forking the Ethereum blockchain

Table 3.1: Hard forking the Ethereum blockchain

Date	Fork Name	Motivation
14/03/16	Homestead	Change the difficulty adjustment algorithm for finding a block. Increase the internal price for running a transaction or contract on the blockchain.
20/07/16	The DAO	After a hacker attack, stealing away a major amount of ether, this hard fork reversed those transactions and restored the stolen amount.
18/10/16	Tangerine Whistle	Increased the price of certain operations to prevent a denial of service (DoS) attack on the blockchain due to a computable difficult operation. This aimed at reducing pending transactions.
22/11/16	Spurious Dragon	Further tuned operations prices to prevent future DoS attacks, it limited the contract code size, and introduced protection against a certain "attack".

3.2.5 Technological Risks

Blockchain technology and especially cryptocurrencies on it are not completely risk free. Due to the nature of the blockchain, it is highly dependent on computational power, which means that if the majority of the computing power is malicious, there could be risks of hacker attacks. One such attack is known as the 51% attack, where a majority of the computational power may

choose to build upon a malicious block, rather than the honest block, in order to spend money and then make it unvalid. This event is highly unlikely on the larger blockchains as the computational power is well distributed, whereas it is more likely on minor ones.

Other technological risks might be the underlying cryptography. Although this is not an issue at the moment, in the future there may be ways to decrypt easier than today and by then newer and better cryptographic hash functions must be developed to stay ahead of the risks. Moreover, the use of private and public key pairs is a risk for the user in case they would lose their private key, as that is their access to the blockchain. This risk may however be mitigated by introducing split keys, such that you have a key split into several parts, where you only need a certain number of them to validate your identity.

3.3 Smart Contracts

A brief history of the internet begins with the connection of two nodes at the University of California, Los Angeles (UCLA) in late 1969. Early European adopters origined in Norway and Sweden during 1973. In 1982 the Internet Protocol Suite (TCP/IP) was standardised and permitted worldwide interconnected networks. In 1990 the WorldWideWeb (www), the HyperText Transfer Protocol (HTTP) and the HyperText Markup Language (HTML) were all introduced by a man named Tim Berners-Lee, and by then one can surely say that an Internet 1.0 had been formed. Many years later, in 2008 the first concept of Blockchain was introduced and thus enabled an Internet 2.0 with the possibility of transacting value in a secure way over the internet. Only seven years later the Ethereum Blockchain takes a new leap to Internet 2.5 with the addition of smart contracts to the blockchain.

The idea of a smart contract was however introduced much earlier than this by computer scientist Nick Szabo in 1994, who emphasised the goal of bringing practices of contract law and related business practice to e-commerce protocols between strangers.

Within the recent hype of Blockchain however, the terms *smart contract* are used more specifically for the general purpose of computations that take place on the distributed ledger. With this interpretation a smart contract is not necessarily related to the classical concept of a contract, but rather

to any kind of computer program. A clarifying example is that of a vending machine. Ordinarily you would go to say a lawyer, pay them, and wait for them to give you your document. With a smart contract you would instead deposit an amount of cryptocurrency, and the blockchain provides your bought service (or product).

The founder of the Ethereum Blockchain, the 22-year-old programmer Vitalik Buterin, explained in a recent Blockchain Summit that in a smart contract approach, an asset or currency is transferred into a program "and the program runs this code and at some point it automatically validates a condition and it automatically determines wheter the asset should go to one person or back to the other person, or whether it should be immediately refunded to the person who sent it or some combination thereof." Meanwhile the decentralised ledger stores and replicates the document which provides a certain security and immutability. These smart contracts are a vital coponent in the next-generation blockchain platforms (thereof the Internet 2.5) and are also reasons for the present comparative decline in the Bitcoin blockchain.

A smart contract can be broken down into two distinct components

- Smart Contract Code - The code which is stored, verified and executed on the blockchain.
- Smart Legal Contracts - The use of the smart contract code that can be used as a complement, or substitute, for legal contracts.

How the smart contract would work in a practical sense on a distributed ledger follows this process.

1. **Coding (What goes into a Smart Contract)**
   As a smart contract work like any other computer program it is important that they carry out the exact intention of the contractual parties. This is then achieved by using proper logic when writing the smart contract. As the code behaves in certain predefined ways and lacks the nuances of the human language, it has now automated the “if this happens, do that” part of traditional contracts.
2. **Distributed Ledgers (How the smart contract is sent out)**
   When the coded contract is encrypted, it can be sent to the distributed network of nodes. If it is sent on a permissionless blockchain it is sent in the similar way as a normal transaction would have been made. This can also be done in a permissioned or hybrid ledger.

3. **Execution (How it is processed)**
   Once computers in the network receive the code, they come to an individual agreement on the result of the code execution. The network then updates the distributed ledger by recording the execution and then monitors for compliance with the terms of the contract.

3.4 Initial Coin Offerings

Appcoin sales, commonly known as initial coin offerings (ICOs), are a new form of crowdfunding. Contrary to ordinary crowdfunds, ICOs bypass the rigorous and regulated capital-raising process required by venture capitalists or banks. However, the use of ICOs are so far limited to the release of a new cryptocurrency venture.

In an ICO campaign, some percentage of the cryptocurrency is sold to early backers of the project in exchange for other more established cryptocurrencies such as Bitcoin or Ethereum, or sometimes fiat currency. As a result the company obtains capital to fund the product development and the audience members get their share of the crypto tokens. These ICOs have proven to be very efficient in order to kickstart crypto projects, and given a solid team and a product satisfying demand the ICOs are also very successful.

Table 3.2: Successful initial coin offerings

Altcoin	**Funding in $**	**Idea**
MobileGo	50,000,000	MobileGo is the first crypto mobile gaming platform and store for in-game purchases.
Brave	35,000,000	Brave is a fast, open source, privacy-focused browser that blocks malvertisements, trackers, and contains a ledger system that anonymously captures user attention to accurately reward publishers.
Storj	29,200,000	Storjs goal is to disrupt the traditional cloud storage industry's centralized storage model.
Ethereum	18,000,000	The Ethereum ICO was one of the first of its kind. It put this concept of an initial coin offering on the map.
Waves	16,000,000	Waves is a blockchain-based colored coins platform, which will allow for future decentralised value transfers all over the world.
Iconomi	10,500,000	The company aims to provide a connection to the distributed economy by allowing anyone to create their own Digital Asset Arrays (portfolio).
Golem Project	8,600,000	Golem is a decentralized global market for computing power, which attracted its funding in mere minutes.

There are certainly some similarities between ICOs and more traditional initial public offerings (IPOs). However, one can point out some key distinguishing features. A company's shares, released during an IPO, always denote a share of ownership of the company, which is not necessarily the case for an ICO, where the crypto tokens instead are units of currency. Another crucial difference is that IPOs are heavily regulated by governments. This

requires a partaking company to complete large amounts of paperwork before releasing its shares. In order to launch an ICO there are few requirements, meaning that any project can launch an ICO at any time with little preparation and any person can contribute their money, no matter what country they are from.

Profits are not a guarantee when investing in ICOs. Campaigns may fail, and in that case some contributions may be refunded to the senders. Also, even if it does succeed, there is no guarantee the price of the tokens will go up, or that the project will deliver their product. This is a risk all participants must be aware of before they decide to contribute to an ICO campaign.

When looking for today's trends in cryptocurrency, a look at current ICOs is a good place to start. ICOs have come to enable every individual or company to easily release freely tradable tokens in order to raise funds. It could be used to completely change the landscape for financial systems of shares, securities and so on. It decentralises not just money, but also stock creation and trade. Important to keep in mind is though that it is not the ICO which is the great enabler of business models and innovation. The blockchain is. So one would still need to bolt a sound business to it.

Chapter 4

Methodology

4.1 Approaches for CCR on the Blockchain

At the time of writing there are no current CCR strategies on the market for blockchain technology. Hence, this chapter will aim at enlightening certain ideas and approaches towards this topic.

From Chapter 2 we learnt about the foundations of CCR. There we noticed two different concepts, EL which is the expected loss (i.e. computable) and UL which is the unexpected loss. Furthermore, in Section 2.1 we found suggestions on how to best mitigate the CCR. Selection of counterparty was a strongly suggested method and from Eq. (2.1) we know that PD and LGD are those closest related to the counterparty. Whereas EAD is the more computationally dependent factor in the EL.

In the following two subsections several suggestions on how to approach the different factors of the EL are stated. An approach for the EAD is suggested in Section 4.1.1. Thereafter an approach for selecting better counterparties is investigated in Section 4.1.2.

4.1.1 EAD on the Blockchain

As we learned from Section 2.2, the EAD has two factors, the replacement cost and the potential future exposure that can be specified. The PFE is commonly calculated by Monte Carlo simulation as described in Section 2.2.2.

What can be done on the blockchain with the use of smart contracts is to have automatic and frequent updates of the PFE in order to keep track

of the exposure each counterparty is under. Furthermore, certain walk-away agreements could be introduced. By setting some threshold value on the PFE above which the traded derivative is cancelled, one could have a positive effect on the CCR for the counterparties and an easy way out, if the exposure is too large. Below follows two examples of how such smart contracts could be applicable for reduced CCR on two different OTC derivatives.

Example - An interest rate swap

Two parties want to make an agreement for a fixed for floating interest rate swap. I.e. one party wants to trade a fixed interest rate, and the other party wants to trade a floating interest rate, both on some principal value, in this case $1,000,000. They decide the fixed paying party pays the interest rate of 8%, whereas the floating paying party pays the interest rate of the London Interbank Offered Rate (LIBOR). The swap occurs every month until maturity.

For the sake of the example, we have a look at the historical LIBOR rates shown in Figure 4.1. Let us assume this agreement is made in the beginning of 1990 with maturity at the start of 1994. Furthermore, each counterparty are using Monte Carlo simulation for testing the PFE of their trade, and both counterparties have a credit limit of $1,000,000.

The parties sign this swap on a smart contract which has the following features: the contract is self-executing, meaning there is nothing but the program running the trade; the contract evaluates the PFE with Monte Carlo simulation every month of the active trade. Moreover, the contract has a built in walk away feature which terminates the contract if the PFE is higher than the credit limit three consecutive months in a row. The simulation procedure for this example is presented in Section 4.2.1. The results of the contract is presented in Table 5.1, and shows how the PFE differs each month and when the contract is terminated.

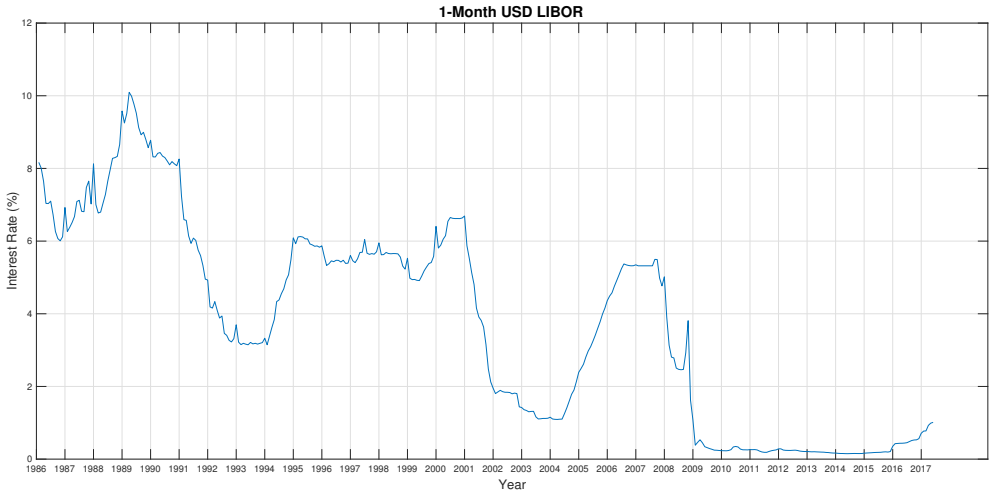


Figure 4.1: LIBOR interest rates from 1986 to 2017

Example - A call option on FX rate

In this example two parties sign a call option for an FX rate between USD and BTC (bitcoins). The option states that the investor may choose to buy 1000 BTC for $200 each, with maturity 10 months from the contract is signed. For simplicity the fees for entering the option are ignored. Both parties have a credit limit of $1,000,000.

For the sake of the example we have a look at the historical exchange rates of USD/BTC, seen in Figure 4.2, and assume the contract is signed in April 2013 and has maturity in February 2014. Similar to the previous example, both parties are using Monte Carlo simulation to calculate the PFE.

They enter the agreement on a smart contract designed as follows: the PFE for the future value of the option is evaluated weekly; and if the PFE exceeds the parties' credit limit three consecutive weeks, the contract is ended. Upon early termination of the contract, the buyer has the possibility to purchase the coins at that time instead. This way the seller does not risk to lose the PFE, and the buyer can still make a major profit. The simulation

for this example is presented in Section 4.2.2, and the outcome of the contract is presented in Table 5.2.

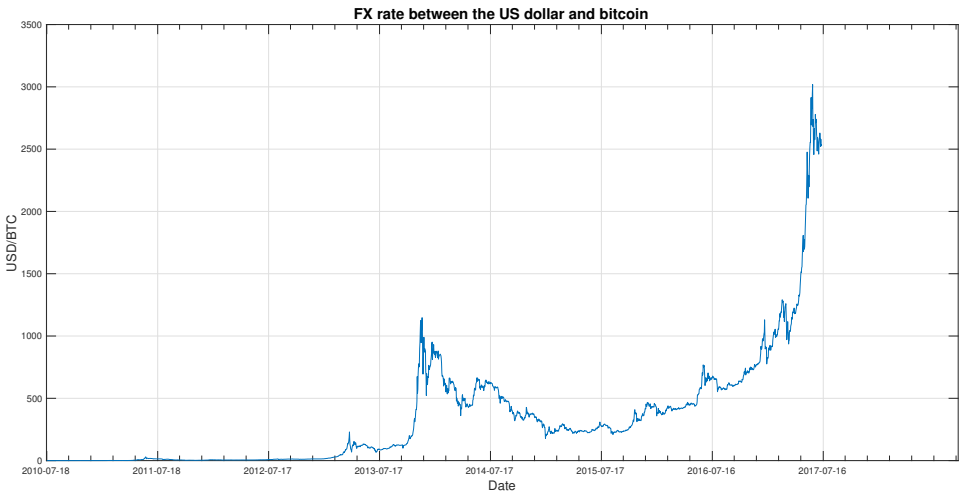


Figure 4.2: USD/BTC exchange rates since mid July 2010

Both of these examples are suggested in order to show how certain potential features of smart contracts can be used to reduce CCR. All interest rates and exchange rates are true historical rates, whereas times and amounts are chosen for the sake of the examples. The simulations for both examples are presented in Section 4.2.

4.1.2 PD and LGD on the Blockchain

In section 2.3 & 2.4 the concepts probability of default and loss given default were introduced. These parameters are both evaluated by investigating the counterparties, or by following the Basel regulatory guidelines. Both PD and LGD have thus shown potential to be individually bound to the counterparty.

It could be possible to introduce a factor to each party on the blockchain, related to their own PD and LGD. This factor could then be possible to re-evaluate after each trade has settled. Parameters that come into play for such a re-evaluation would be amount traded, length of contract, number of defaults, number of completed contracts, etc.

Reasonable would be that e.g. if the trade is successful without any defaults, then the parameters decrease slightly, whereas a default increases

the parameters. This way everyone would be able to know in advance how trustworthy their counterparty is, as their counterparty's PD and LGD is related to their previous trades and how succesful they were.

In Section 5.1, as a result of the suggested approach for PD and LGD on the blockchain, two examples are presented to show a relevant take on how to manage the factors PD and LGD. They could work as a foundation for developing autonomously evaluated parameters that could be implemented as a smart contract on a blockchain application.

4.2 Simulations

By using Matlab for computing and coding exemplified smart contracts, simulations for the approaches on PFE are performed. The results from the simulations are presented concisely in Section 5.1.

4.2.1 An Interest Rate Swap

The first simulation explains the interest rate swap example presented in Section 4.1.1. For this purpose one-month USD LIBOR rates from 1986 to 2017 were loaded and are shown in Figure 4.1. The smart contract for the example was constructed in a Matlab setting. The contract was carried out under certain simple programmed constraints. Namely, that the PFE should be recalculated every month of the active trade. Also, if the PFE is higher than the credit limit set to \$1,000,000 a counter is increased. If the PFE does not exceed the counter is set to zero. When (or if) the counter reaches three, then the contract is terminated.

The PFE is calculated with a simple Monte Carlo simulation, which has a probabilistic factor representing different market scenarios. The probabilistic factor is from a normal distribution, adjusted for the initial values of the true historical rates. The scenarios are simulated 100 times. The first round of calculating the PFE can be seen in Figure 4.3. One may notice the black trajectory, being the true LIBOR rate, during the same period. The simulation does not expect such a radical decline in the floating interest rate. This is purposeful as it is the subject for CCR in this example and points out the necessity of a re-evaluation of the PFE at future times.

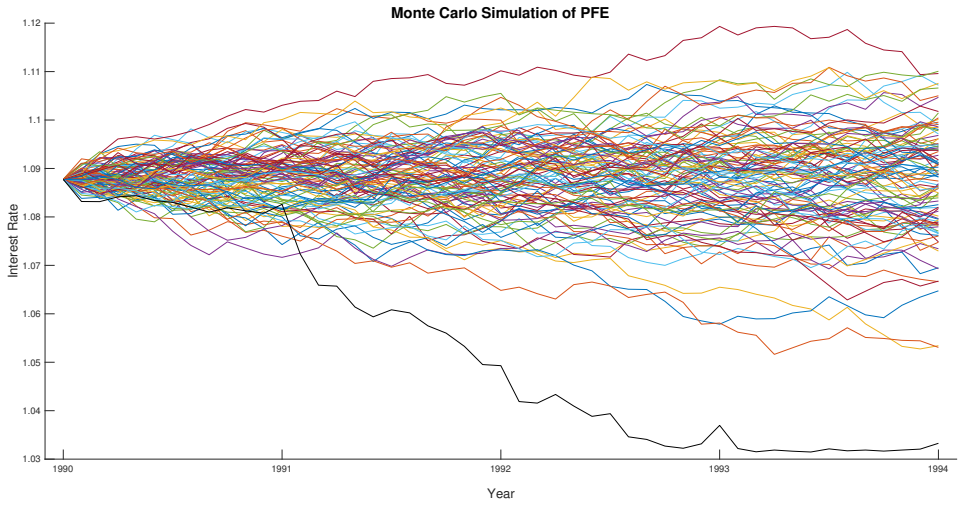


Figure 4.3: Initial Monte Carlo simulation of the PFE

For the values and dates of this example, the contract is active during 25 months approximately. At that point the PFE has exceeded the credit limit three months in a row, for the counterparty paying the fixed rate of 8%. Hence, the contract ends and no more interest swaps are executed after that point. With this simulation, an immediate use of smart contracts on the blockchain are presented for one kind of financial instrument.

4.2.2 A Call Option on FX Rate

This simulation follows from the example on an FX option from Section 4.1.1. In Figure 4.2 the historical USD/BTC exchange rates are available. Thus, by choosing to make the example span a period with a major increase, the CCR becomes more obvious. Therefore the contract is said to have been made in April 2013 and is supposed to end in February the following year.

Similarly to the previous example, Monte Carlo simulation is used for the PFE. The probabilistic factor is chosen to fit the initial true values, being the black trajectory in Figure 4.4. It can be seen that there is a certain probability for an increase, however it seems unlikely considering the number of cases from the simulation of 100 scenarios.

The smart contract conditions are similar to those of the fixed for floating trade. Particularly, if the PFE exceeds the credit limit for a counterparty three times in a row, the contract is terminated. As one may see in the Monte Carlo simulation of Figure 4.4, the first 28 weeks of the simulation

seem quite reasonable. However, thereafter an increase spike happens which is not much expected from this simulation and hence the exposure is much higher from then on. This is where a smart contract can become useful, as a repeated calculation of the PFE can be done automatically and thus reduce the CCR if something unexpected happens.

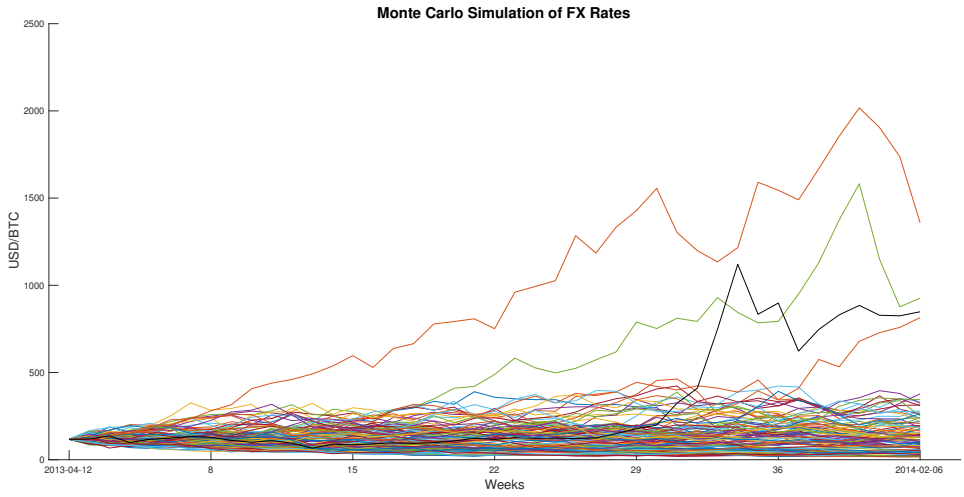


Figure 4.4: Monte Carlo simulation of the USD/BTC exchange rate

For the simulation of the values in Table 5.2, the contract is ended in week 35. At that point three consecutive weeks have passed where the PFE is above the credit limit of $1,000,000. The simulation of the PFE this last week is shown in Figure 4.5, which shows how valuable it can be to have a smart contract which frequently evaluates the PFE for an agreement.

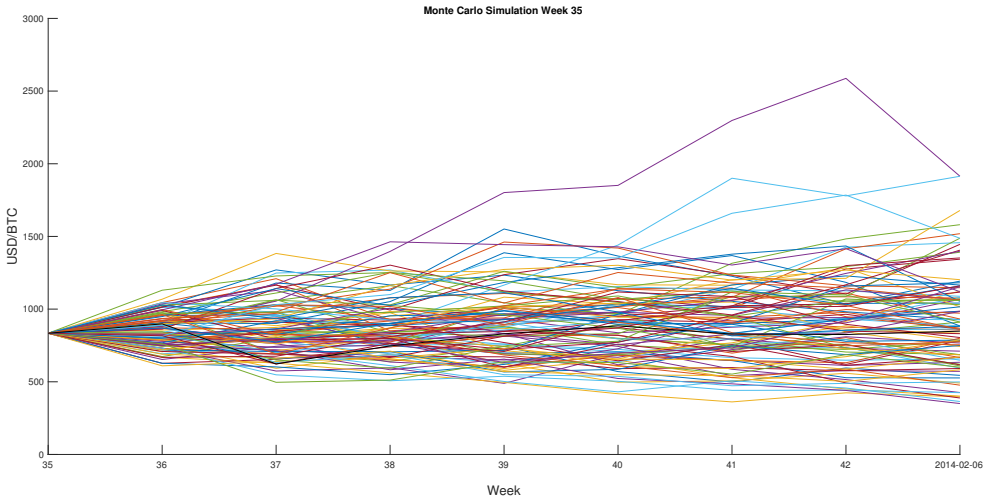


Figure 4.5: Final evaluation of the PFE for an FX call option

Obviously the seller could also have made a profit, if a put option was signed in the beginning of 2014 of Figure 4.2, with maturity in mid 2015, instead. Giving the owner of the bitcoins the right to sell them at some specified higher price.

4.3 Interviews

For the mapping of the current financial market and their stand point on blockchain technology, an interview study was carried out. The interview was supposed to target the market's interest and how it differed regarding the underlying technology and the cryptocurrencies used on it. In order to do so, a set of relevant questions where considered.

1. What is your current strategy in R&D on cryptocurrency?
2. What is your current strategy in R&D on blockchain technology?
3. Do you favour one over the other? If so, why?
4. What would need to happen for you to jump on the cryptocurrency market opportunity?
5. Is there a big demand from your customer base?
6. How do you work with businesses within the cryptocurrency market?

7. If you do not cooperate in any way, would you please mention why not?

8. What would it take for you to work with cryptocurrency businesses?

9. Finally, what are your current thoughts of ICO, the new way of financing and corporate structuring?

These questions were supposed to act as guidelines and support for mapping where the financial market, specifically the financial institutions, are in developing, or adjusting to, the decentralised technology.

Chapter 5

Results and Discussion

In this chapter results from following the methodology of Chapter 4 are presented. The results are split into two different sections: those stemming from the literature study of blockchain and counterparty credit risk, Section 5.1; and results of the interviews made on the current financial market, Section 5.2.

5.1 Literature study

From the thorough study of the literature on CCR and blockchain, approaches where presented in Section 4.1. These suggest a set of examples that have been developed as a result of the study.

Results - An interest rate swap

By using the smart contract suggested in Section 4.1.1, the LIBOR paying party make a profit of about $150,000. Meanwhile, the fixed rent paying party avoids losing more than $1,200,000 which would have been the case, if the agreement was not terminated half way through. The loss would then have been almost 10 times more than what is lost in the smart contract case. The following table summarises the outcome of the PFE each month of the traded derivative.

Table 5.1: A smart contract procedure for an interest rate swap

Month	**PFE** in $	**Strike**
0	207,000	
⋮	⋮	⋮
18	1,004,000	I
19	937,000	
⋮	⋮	⋮
22	1,010,000	I
23	1,020,000	II
24	1,100,000	III

Results - A call option on FX rate

The following table presents the outcome from the example of a call option on FX rate.

Table 5.2: A smart contract procedure for an option on an FX rate

Week	**PFE in $**	**Strike**
0	170,000	
⋮	⋮	⋮
33	1,200,000	I
34	1,740,000	II
35	1,330,000	III

The buyer would naturally buy the bitcoins when the contract ends, as the value at week 35 is $898, hence making a profit of $698,000. For the seller this does not make a big difference compared to what the loss at maturity would have been. This is however unknown at the time the contract is terminated. Compared to the calculated PFE, the seller has a smaller risk for this case.

Below are two examples developed as a result from the approach towards PD and LGD on the blockchain. The examples suggest how the parameters could be evaluated for agreements written on smart contracts, in a blockchain manner.

Example - Adjusting the PD parameter

Let us assume that two counterparties have agreed on a specific trade of an OTC-derivative. There have been no agreements for ending the contract in advance, so the trade will take place for as long as it is possible, up until maturity or a default.

Both parties have at the beginning of the contract some probability of default based on a regression analysis of trading parties in general and then compared with the actual counterparties in the trade. For instance their PD values are 0.5 each (i.e. 50% risk of default).

At some point, before maturity, one of the parties defaults due to the lack of economic resources. As a result this specific counterparty's PD value will increase slightly depending on the principal of the trade, how long the trade lasted etc. The other counterparty's PD value will remain the same as it cannot yet be evaluated, since there has been no settled deals so far. In summation, the defaulted party gets increased PD and the other's is unaffected.

The unaffected party enters a new trade with a safer counterparty, i.e. one which has a lower value on its PD, implying that it has effectively ended several trades without defaulting. The trade proceeds according to their written contract and by maturity there has been no default. Both parties get, as a result, a decreased value of their PD.

Example - Adjusting the LGD parameter

Similarly to the modification of the PD parameter, an update of the LGD parameter can be made. Let us say that both parties in the previous example start by having the Basel regulated LGD parameter 0.45 (i.e. 45% loss given default). Just as in the previous example one counterparty defaults. However, in this case the contract is ended, but the counterparty manages to pay back part of the obligation stated in the contract.

Let us say that the recovery rate of the default is 80%. As the counterparty manages to pay back a major fraction of the default, its LGD parameter may be decreased slightly (as $LGD = 1 - RR = 0.2$), thus stating that even though the counterparty might have defaulted, it shows a better probability of repaying a default than some other counterparties that have been subject to defaults.

On the contrary if the defaulting counterparty does not manage to repay as much of the default, the LGD may increase and thus make the counterparty a less attractive trading partner.

5.2 Interviews

By talking to influencers of the financial market, such as Stockholm Fintech, Handelsbanken, FCA UK, the European Central Bank and **...** a summary to the questionnaire, presented in Section 4.3, could be made. First and foremost, the general attitude towards the new technology of blockchain was positive and many more potential interviewees could not find time to answer due to question overload from the market. Hence, it is very thankful that answers were obtained from the previously mentioned interviewees.

Overall, there is more interest in carrying out R&D on blockchain technology rather than on cryptocurrencies, where some sources point out that regulatory frameworks are not yet in place for cryptocurrencies. Mostly different proof of concepts are carried out, in order to investigate potential use cases for the distributed ledger technology. Moreover research on provided

financial services are made to find potential areas for regulation in order to prevent, amongst other things, arbitrage opportunities.

The financial market concludes that cryptocurrencies and blockchain technology are not competitive. However, sources tell that more education and knowledge around the subject, as well as regulations that go hand in hand with the technology, are needed in order to fully engage in the market opportunity.

Although there is little immediate demand from the customer base of the interviewees, it is obvious that there is a market demand as all are head over heels to learn more and take part in the technology. As new innovative companies are seeking approval for their innovations, most demand currently lies within the regulatory framework.

Fund raising, regulatory advice, attempts to lower the barrier to entry are only a few of the methods the financial market uses to boost and work with new businesses in blockchain. Some sources have cosen to focus more on carrying out research of their own, rather than to cooperate with businesses that are already well informed regarding the technology.

When it came to ICOs, there was a lot of skepticism. Although there was a major inflation of ICOs during June 2017, it is believed that only a few of them will succeed. Moreover it is not denied that a regulatory framework for ICOs may be needed, depending on the structure of ICOs, as they have many similarities to initial public offerings (IPOs), or crowdfunds.

5.3 Discussion

In order to recapitulate, the purpose with this thesis was to investigate CCR and to suggest how to approach it on the blockchain. Furthermore, the thesis aimed to lay a foundation for future work on the subject of blockchain technology and the different applications of it.

The results found, when working with CCR on the blockchain, provide insight in how the decentralised technology functions, foundations of counterparty credit risk, as well as shows where applications of blockchain technology could be relevant. The thesis' results further show that certain conditions on a smart contract can have major beneficial effects on CCR. The results hope to enlighten the reader about how CCR could be affected, and suggest a few approaches to do so. From the literature study of CCR, in combination

with smart contracts, it was also shown that there are several parts of the CCR, alone or in combination with each other, that could be affected when making use of smart contracts on the blockchain. Approaches for EAD, PD and LGD are all suggested in the results, of which some where simulated to show that there actually is a potential benefit from using the decentralised technology.

Although the results capture the purpose of the thesis in a satisfactory manner, I wish that the problem could have been approached in a less mathematical way, with more focus on discussing blockchain's potential. The concept of blockchain technology is still comparatively young and therefore I believe the technology should be throughly studied before trying to find usages for it. As the technology lays a foundation for many potential applications, both mathematical and not, it could have been better to focus on presenting the technology on a deeper level in one thesis, before starting to investigate its potential applications. However, given the circumstances I hope the content of this thesis will have presented the concept satisfactory, in both a concise and also technological way. Furthermore I hope that future studies on the subject will find good use of Section 3.2 about blockchain technology, and find both inspiration and knowledge for their own work.

Here follows some suggestions on work that could be done from here on. Firstly, studying and mapping interesting areas of application for self-executing contracts. Which areas will be relevant for the future and why? Choose an application and learn to program a smart contract that could be applicable to the blockchain.

Regarding the interview and the mapping of the current market, it was surprising to see the positive attitude towards blockchain technology, mostly due to its competitive advantages that may affect the financial market tremendously. However, it is still a long way to go before a natural symbiosis between the current financial market and the new upcoming market is fully functioning. What needs to be done before this can happen is though rather clear. More education on the subject of blockchain is needed for the current market to understand the benefits blockchain bring, and this should be done as soon as possible. Furthermore, the legal systems concerning regulatory frameworks for digital currencies and different use cases, as well as for ICOs needs to get up to date with the technology. Otherwise the current exponential development of the technology will need to be halted, which in

my opinion would be unfortunate. The fact that market influencers have started with R&D is a good sign of market interest and still, most people do not know about the underlying technology, although many have heard of Bitcoin.

Chapter 6

Conclusion

To conclude this thesis, we may state that there is evidence for a growing market of blockchain technology and that there are yet many use cases to discover and implement. Furthermore, the technology is built upon market demand as well as solid technology which may yet be improved even more. This suggests that the technology will keep on growing and find new and innovative applications. Moreover, the report shows that there are reasons to further investigate the use of smart contracts for CCR, however a rigid proof of concept should be developed before it is possible to say how much the CCR can be affected by using blockchain technology. Finally, the current financial market and the legal systems are not yet up to date when it comes to education and regulation of blockchain technology.

Bibliography

[1] Bitcoin blockchain charts and statistics. `https://blockchain.info/charts`, June 2017.

[2] Ethereum blockchain charts and statistics. `https://etherscan.io/charts`, June 2017.

[3] Jon Gregory. *Counterparty Credit Risk, The new challenge for global financial markets*. Wiley Finance, 2010.

[4] Darrell Duffie and Haoxiang Zhu. Does a central clearing counterparty reduce counterparty risk? Master's thesis, Stanford University, 2011.

[5] Sara Jonsson and Beatrice Rönnlund. The new standarized approach for measuring counterparty credit risk. Master's thesis, The Royal Institute of Technology, 2014.

[6] Bank for International Settlements. The standardised approach for measuring counterparty credit risk exposures. Technical report, Bank for International Settlements, 2014.

[7] Bank for International Settlements. The application of basel ii to trading activities and the treatment of double default effects. Technical report, Bank for International Settlements, 2005.

[8] David Bauman, Pontus Lindblom, and Claudia Olsson. *Blockchain, Decentralized Trust*. Entreprenörsskapsforum, 2016.

[9] Power to the user: Accenture & microsoft are changing identity with ethereum. `http://www.coindesk.com/`, June 2017.

[10] Un leaders urge blockchain startups to collaborate on identity. `http://www.coindesk.com/`, June 2017.

[11] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.

TRITA -MAT-E 2017:69
ISRN -KTH/MAT/E--17/69--SE