NTNU

Norwegian University of
Science and Technology

Private Blockchain system for international currency exchange and hedging

Kristoffer Alvern Andersen

Master of Science in Communication Technology
Submission date: May 2018
Supervisor: Danilo Gligoroski, IIK

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

NTNU – Trondheim
Norwegian University of
Science and Technology

Private Blockchain system for international currency exchange and hedging

Kristoffer Alvern Andersen

Submission date:	May 2018
Responsible professor:	Danilo Gligoroski, ITEM
Supervisor:	Danilo Gligoroski, ITEM

Norwegian University of Science and Technology
Department of Telematics

Abstract

This master thesis designs a system that utilizes Blockchain technology in international currency exchange transactions, thereby act as a currency exchange interface among private parties and companies, to enable faster and cheaper financial transfers outside of the existing inter-bank system.

A proposed platform called Sonic Markets will issue a set of cryptocurrencies called Hedgecoins. These cryptocurrencies will fund the financial buffers needed to fulfill the transactions. Since Hedgecoin is reflecting an optimized diversified portfolio of various international currencies, it is a cryptocurrency with intrinsic value. Hedgecoin is thus a nonvolatile, liquid, digital currency asset that facilitates diversified saving for everyone, including citizens of severely inflated countries. The tech infrastructure is highly scalable and adaptable towards new technologies and cryptographic systems. The Blockchain is private and thus require no mining, nor extra transaction delay due to slow distributed consensus procedures. This thesis challenges the current strive for decentralization of cryptocurrencies in a time when the complete financial and technological foundation is centralized.

The thesis includes a simple proof of concept implementation of a private blockchain in Python, as well as an implementation of a portfolio optimization algorithm that utilize a genetic algorithm to find optimal portfolios efficiently.

Sammendrag

Denne masteroppgaven omhandler design av et system som utnytter Blokkjedeteknologi til internasjonal valutaveksling. Systemet vil derav fungere som et grensesnitt blant privatpersoner og selskaper, for å muliggjøre raskere og billigere finansielle transaksjoner utenfor inter-banksystemet.

Finansiell bufferkapasitet tilstrekkelig for å gjennomføre transaksjoner er finansiert gjennom et sett av kryptovaluta kalt Hedgecoins, på en plattform kalt Sonic Markets. Ettersom Hedgecoin speiler en optimalisert diversifisert portefølje av ulike internasjonale valutaer, har den reell verdi. Hedgecoin er derfor en ikke-volatil, likvid, digital valuta som tilbyr diversifisert lavrisikosparing for alle, inkludert borgere i land preget av høy inflasjon. Den teknologiske infrastrukturen er veldig skalerbar og tilpasningsdyktig til ny teknologi og kryptografiske systemer. Blokkjeden er privat og krever hverken gruvedrift eller ekstra transaksjonstid grunnet trege distribuerte konsensusprosedyrer. Denne avhandlingen utfordrer den nåværende streben etter desentralisert kryptovaluta, i en tid hvor hele det finansielle og teknologiske fundamentet, hvor kryptovalutaen er bygget på, er sentralisert.

Avhandlingen inkluderer også en grunnleggende *proof of concept* implementasjon av en privat blokkjede i Python, i tillegg til en implementasjon av en portefølje-optimeringsalgoritme som bruker en genetisk algoritme for å finne optimalt diversifiserte porteføljer på en effektiv måte.

Preface

This thesis is conducted at the Department of Information Security and Communication Technology at Norwegian University of Science and Technology (NTNU). The thesis is the final project for the MSc program in Communication Technology with specialization in Information Security.

The study was performed over 19 weeks, Spring 2018. The novelties described in this thesis are currently prepared in the form of a scientific paper that will be sent to an international Blockchain conference.

I would like to thank my responsible professor and supervisor, Danilo Gligoroski, and Chris Carr for guidance, good discussions and great advice throughout this period.

I would also like to thank my dear friend, Oliver Damsgaard Jensen for implementation assistance of the portfolio optimization algorithm, for many great late night dinners, and for dragging me through 5 seasons of Archer in the process.

Contents

List of Figures

List of Tables

Listings

Chapter 1 Introduction

Blockchain technology has received a lot of media attention the last few years, and quite a few cryptocurrencies have emerged since Satoshi Nakamoto published the *Bitcoin: A peer-to-peer electronic cash system* paper in 2008[Nak08]. The ideas were revolutionary, but not near scalable to fulfill their real purpose. The main bottleneck for these technologies are the tedious decentralized consensus algorithms. Not having a central decision maker introduce severe scalability limitations, complex networking communication and in many cases, non-sustainable waste of energy resources related to mining. The decentralization is supposed to give independence from governments and financial institutions, but it also restricts the technology from evolving, adapting and scaling. The decentralization ensures that the technology gets an expiration date when either the demand of the service itself gets too high, when the technology gets inefficient and outdated, or when the cryptographic schemes are compromised. Why do we so desperately need decentralized systems now? Also, at what price? This thesis will present a private Blockchain technology that solves the mentioned problems for international currency exchange, as well as other financial and socioeconomic issues.

1.1 Motivation

Nowadays, international currency exchange is slow and expensive. Every part of the value chain takes a small percentage for a seemingly effortless job, but we still have to use these services because we are short on suitable alternatives. The foreign exchange market is the most significant financial market today, but the actors are restricted to large banks and companies, all of whom are free to charge costly fees for their services.

With the right perspective, Blockchain technology can help reduce cost, enable faster transactions and help to secure the complete infrastructure of any financial transaction. By undressing Blockchain technology into its components, we can utilize the ideas that work great, and abandon the ones that are still immature. We can leverage the relevant features of Blockchain technology, and make new systems on top of the existing financial services that are faster, cheaper and more predictable. Together with existing technologies, we can build a system that is not as visionary as existing Blockchain solutions, but yet more realistic, scalable, adaptable, and most importantly, feasible and sustainable.

A more stable and non-volatile cryptocurrency system can prove to be valuable as an asset for hedging, but also help remove the widespread association between blockchain technology and speculation/gambling, caused by the Bitcoin hype at the end of 2017.

For the average citizen of a country affected by severe inflation, it is harder to save money when the purchasing power is decreasing fast. The idea of successfully saving enough money for education or creating a business seem more improbable for the general public, and will on a broad scale slow down the economy and decrease the overall wealth. Along with microloans, saving in an internationally diversified portfolio can alleviate the harm of inflation for some, which can result in more jobs and a more civilized and educated society.

1.2 Objective

The primary objective of this thesis is to design a Blockchain system and a cryptocurrency that

- facilitates international currency exchanges at low cost and high speed
- has low volatility, and real intrinsic value thus removes the speculation aspect of the cryptocurrency
- is scalable, adaptable and sustainable
- can be used for various financial purposes in a beneficial way for the world economy and further development of Blockchain technology

The second objective is to successfully implement a basic proof of concept of a private Blockchain, with corresponding key-management and user interface.

The third and final objective is to implement a portfolio optimization program using a genetic algorithm that finds the best currency portfolios, based on historical data.

1.3 Methodology

The thesis focus on designing a private blockchain for international currency exchange. Obstacles and limitations to the proposed solution are discussed underway, throughout the thesis. Several new beneficial services emerge, while trying to solve the primary problem of transferring money fast and cheap. The market potential and social impact of these services are also discussed and justified underway.

The methodology consists of 5 steps.

1. Get an overview of available competing services and cryptocurrencies
2. Acquire an in-depth understanding of primary concepts, strengths, and weaknesses, performance statistics, technological potential and limitations for similar purpose cryptocurrencies
3. In several iterations
   - Challenge choices made by existing technologies and concepts
   - Consider various adjustments and improvements
   - Reflect on consequences, impact, sustainability, scalability, and adaptability for these solutions
4. Proof of concept implementation of a private Blockchain with corresponding key-management and user interface, to get a better understanding of the underlying technical ideas and core concepts of the proposed idea.
5. Implementation of diversification optimization program to further emphasize the potential of the proposed financial services.

Apart from the design and overview of the proposed Blockchain solution, two areas are further investigated and implemented in code, one with a technical perspective, and one with a financial perspective. Firstly, a proof of concept of a private Blockchain is implemented with key management and user interface. Secondly, an optimization algorithm is implemented for the portfolios of the proposed *Sonic Markets, Hedgecoin*[1].

[1] Disclaimer: There was a cryptocurrency named Hedgecoin that was only active for three months back in 2015 https://coinmarketcap.com/currencies/hedgecoin/ . The design presented in this Master thesis is essentially completely different from that cryptocurrency.

1.4 Tools

The programming language Python is used in the two implementations. Essential libraries used during the implementation:

- **ECDSA** - For elliptic curve cryptography digital signatures and verification.
- **Tkinter** - For graphical user interface (GUI)
- **Numpy** - For multi-dimensional matrix calculations

All illustrations throughout this master thesis are made with *Draw.io*.

1.5 Thesis structure

This thesis will start out with a thorough background in Blockchain technology basics, with Bitcoin as an example. Then, a discussion on scalability related issues and an introduction to private Blockchain technology will follow, before a small overview over some of the available currency exchange services closes chapter 2. Chapter 3 introduces the proposed private Blockchain system, its purpose, and fundamental ideas, along with the Hedgecoin. Chapter 4 has a more technical perspective and explains the dynamics and infrastructure of the system. Chapter 5 takes a more financial point of view and introduces a few new extensions to the system that makes the service more useful and available for a wider audience. Chapter 6 summarize the proposed ideas and discusses the market potential for each of the presented services of Sonic Markets. Chapter 7 looks into portfolio optimization of the Hedgecoin, with supporting financial theory and optimization algorithm. Chapter 8 is a superficial walkthrough on the *proof of work* of the private Blockchain implementation done for this thesis. The final chapter with new content, chapter 10, is also a superficial walkthrough of the work done during the implementation of the proposed portfolio optimization from chapter 7. Closing the thesis is the final conclusion.

Chapter 2 Basic concepts and existing technology

2.1 Blockchain technology

Blockchain technology is first and foremost known as one of the revolutionary ideas from the famous "Bitcoin: A Peer-to-Peer Electronic Cash System" paper[Nak08], published under the pseudonym "Satoshi Nakamoto". At its core, Blockchain technology is merely a digital record of transactions, also known as a ledger. The integrity and validity of the ledger are maintained through cryptographic algorithms in the system. To ensure integrity, robustness, and availability, most implementations of Blockchain technology have a distributed infrastructure with no central authority.

2.1.1 Blockchain building blocks

Transaction

A transaction is a written statement of a change in assets or a shift of resources between two or more parties. Each transaction requires a sender and a receiver, and must be signed by the party transferring ownership of its resources. One simple example can be as follows: "Bob sends USD 5 to Alice" signed by Bob. The accumulation of all transactions in a network shows the status or resources of all entities, just like a balance sheet. A transaction can also contain extra information like a time-stamp, a message or perhaps a snippet of code. The possibilities are endless and way beyond what we are currently exploiting.

Block

Transactions are verified and bundled together in Blocks. A Block consist of a collection of transactions plus general information in the form of a header. The Block header contains identification and general information about size, time, integrity and number of transactions, to mention just some. The blocks are then serialized in a chain to maintain a timely order of the blocks. Each Block keeps information about the previously acknowledged block, in the form of a hash of the previous block. A hash is a one-way mathematical function that takes an input and outputs a fixed size string in a pre-defined space. For example, Secure Hashing Algorithm 256 bits (SHA256) transforms any input into a pseudo-random string of 256 bits. One small change in the previous block will result in a completely different hash, and thereby change all hashes of all later blocks. The property that even a single bit change will result in a chain reaction of altered hashes ensures the integrity of the data. So if the last hash is what we expect it to be, we know that no changes have been made to the data and that the integrity of the data is preserved. These blocks are thus implicitly chained in terms of integrity. Furthermore, each transaction is signed by the sender to provide authentication. The signature would yield invalid if any changes were made to the transaction.

Distributed ledgers

Blockchain technology inherently incorporates many valuable characteristics, such as enforcing accountability and integrity for transactions. The network as a whole is in most cases responsible for validating new transactions and maintaining the ledger. With Public-key cryptography, the users can both sign and validate the authenticity of transactions and thereby be confident that a transaction is made by the expected person. Public Key cryptography is a set of encryption algorithms that use a pair of cryptographic keys, one public and one private. These keys ensure integrity and authenticity of the data. A message sent from Alice to Bob will be encrypted with Bob's public key, and can only be decrypted with Bob's private key, only known by Bob.

2.2 Bitcoin

2.2.1 Background

Wei Dai was the first to introduce computational puzzles as a way to "create money" and achieve decentralized consensus with *b-money* in 1998[bmo]. Due to lack of details on how to implement the decentralized system, it was never a great success beyond the idea. In 2009, Satoshi Nakamoto implemented in practice the first ever decentralized currency, called Bitcoin. It has since become widely popular, mostly given media hype related to its originality and fast increase in market cap. The background and purpose of creating the Bitcoin system were based on solving the double-spending problem[1] without a central authority to resolve disputes. In the famous Bitcoin paper [Nak08], Satoshi Nakamoto stated that "The main benefits

[1] Double spending problem: Spending the same digital token twice. Example: Trade a cat for all of ones Bitcoins, obtain the cat before the transaction is on the Blockchain, send new transaction where the same amount of Bitcoin is sent to oneself, if the last transaction is put on the winning Blockchain first, the initial transaction will be invalid. In this case, one now has all of the Bitcoin and a cat

are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.", to accentuate his confidence in a fully decentralized solution.

2.2.2 Bitcoin Infrastructure overview

After its introduction in a white-paper in 2008[Nak08], Bitcoin has proven to be the leading cryptocurrency concerning the number of users, transactions and media hype. Bitcoin is supposed to be a globally transparent and border-less payment system, and it is the first generation of applied Blockchain technology. The system relies on a peer-to-peer infrastructure to accomplish decentralization and independence of any central authority.

The Bitcoin network consists of miners and regular users, all of which should possess the complete Blockchain. The miners verify the user transactions, and add them to the public and distributed Blockchain, also known as the ledger. This ledger is a long chain of data blocks where each block contains the information of several transactions. Figure 2.1 shows a simplistic illustration of the infrastructure. A network of Bitcoin miners must solve cryptographic puzzles to verify the transactions, called proof of work. With public key cryptography, Bitcoin establishes a simple but effective way to manage ownership of resources.

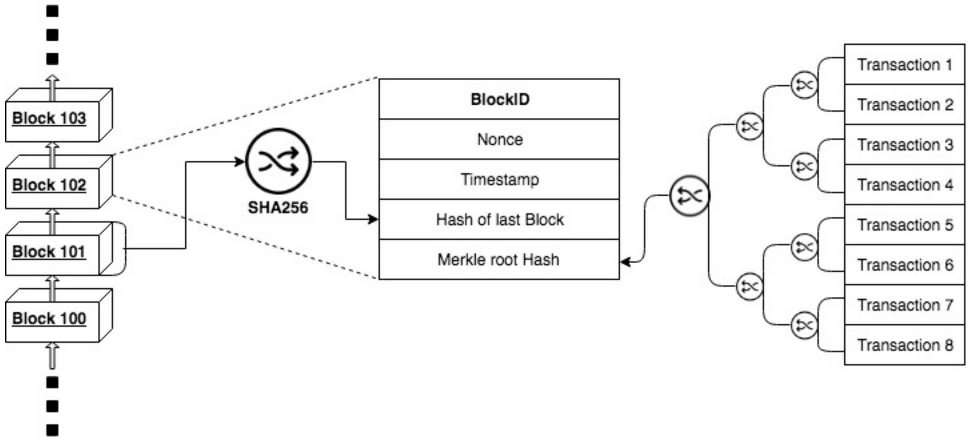


Figure 2.1: Blockchain infrastructure

Bitcoin Mining

The miners in the Bitcoin network have to agree on what is the correct Blockchain and reach consensus to solve the double spending problem. As a consensus algorithm, the network of Bitcoin miners competes in solving cryptographic puzzles first, called Proof of work (POW). The miners gather unverified transactions from the network, make sure none of the transactions violate the double spending problem and gather them in a block. The first transaction in a block is a reward sent to the miner for mining the block. This reward is a compensation for the power and electricity, but will also work as an incentive to stay honest, as the computer-power needed to hijack the network can be used to mine blocks instead. The data block is then hashed with SHA256[SHA][2]. If the resulting output of the hash satisfies the requirements set by the network, the puzzle is solved. If the requirement is not fulfilled, an increment is applied to the nonce [3], before retrying the hashing. The increment and hash are repeated until the puzzle is either solved or until another node solves the puzzle first. When a miner solves a puzzle, the solution is broadcast to the rest of the network. The rest of the nodes then verify that the transactions in the proposed solution are valid and that the block fulfills the puzzle requirements. The miners implicitly show their acceptance of the new block by using it as the previous block when continuing on the new puzzle for the next block of the Blockchain.

Mining inputs and outputs

The Bitcoin network adds a new block to the Blockchain approximately every 10 minutes, hence the difficulty of the puzzle depends on the computing power of the network. So when the computing power of the network increases, the difficulty of the proof of work must increase accordingly. The puzzle is to get an output hash with a given number of leading zeros. The number of zeroes depends on the difficulty needed to get the desired number of blocks per hour. SHA256 is a one-way function, which means that there is no known way to tell what input leads to a given output. Thus the only way of solving the puzzle is brute force [SHA]. The energy consumption of the Bitcoin mining network is extreme and still increasing. At this time of writing (6th of March 2018) the Bitcoin Network has an annual energy consumption of close to 54 TWh, which equals an estimated energy consumption equivalent to 5 000 000 US households or 1/400 out of the total global energy consumption [NRJ].

Proof-of-work solves two problems at the same time. Firstly, the race to complete these puzzles first gives incentives for the network to work on the latest valid block on

[2] SHA256: Secure Hash Algorithm 256 bit: Given a hash value of length n, it should require work equivalent to on average 2^{n-1} hash computations to find any message that hashes to that value [SHA]

[3] Nonce: Number supposed to be used once to ensure that replay attacks are not possible, and as a variable part of the transaction data for the proof of work

the longest chain. The network will naturally act truthful and thus leave a collective consensus on what is the valid chain. A miner implicitly expresses its consensus by working on a Blockchain. There may, however, be simultaneous chains competing to be the leading, but given the incentive to work on the longest and "most worked on" chain, a clear leader is often established within a few blocks. Secondly, there are no political barriers on who gets to join this consensus system. It is entirely open to joining for anyone with a CPU, and the weight of the vote corresponds to the computer power of that particular node/machine. An alternative approach that has been proposed is proof of stake, which instead of using CPU power as a proportioned weight of the consensus vote, use the proportion of total funds.

Independence assumptions

Bitcoin removes the need for a mediating party in transaction disputes, by making transactions non-reversible. However, the Bitcoin ledger is correct and trustworthy under the assumption that the majority of miners are legitimate and not cooperating. As a result, the system displays vulnerability towards an attack where the majority collectively pursues to accept a double spend transaction, known as the >50% attack [Majb]. To modify a past block, an attacker would have to redo the POW of the block and all blocks after and then catch up with and surpass the work of the honest nodes. The probability diminishes exponentially by each block. While this type of attack is probably impracticable, it highlights the large energy consumption needed to keep the system independent of a third party and valid at the same time.

Actions made to minimize necessary storage

To save space, the Blockchain does not store the transactions along with the blocks. We only need to make sure to preserve the integrity of the blocks and transactions. The transactions in a block are pairwise concatenated and hashed with SHA256[Nak08]. These output hashes are then repeatedly concatenated and hashed until there is only one hash, called the Merkle root hash. The Merkle root hash is the top node of a tree structure of hashes of the transactions, so if a single bit flips in any of the transactions, the Merkle root will completely change. The Merkle root thus serves as an integrity mechanism for the transactions. The Blockchain does not need to keep all the old transactions along with the blocks to prove the validity of the Merkle root hash. It only needs to keep two hashes at each level in the tree for each block. The process of removing the redundant transactions and hashes is called pruning, see figure 2.2. The number of hashes and transactions needed to be stored is thus only $\lceil 2log_2(T) \rceil$ instead of T. A pruned block with 1000 transactions would only need to store $\lceil 2log_2(1000) \rceil = 20$ hashes/transactions.

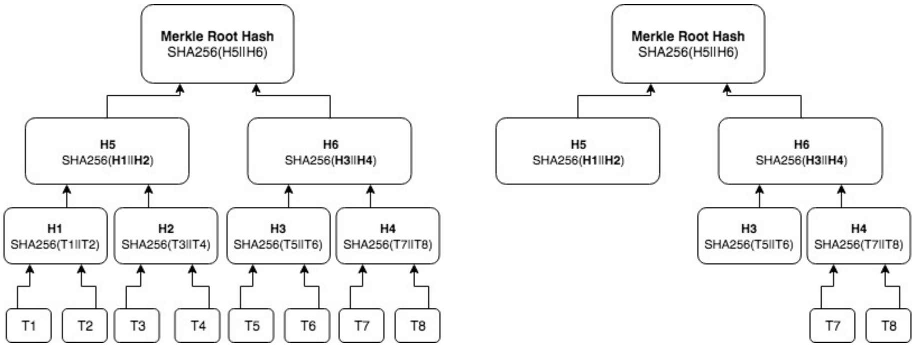


Figure 2.2: Merkle tree before and after pruning

Privacy

Bitcoin use Elliptic Curve Digital Signature Algorithm (ECDSA) to sign and verify transactions. ECDSA is a digital signing algorithm that uses Elliptic curves, a mathematical concept that enable smaller key sizes for the same level of security[DJ01]. The user has one signing key which is private, and one corresponding verification key which is public. When a user wants to make a transaction, he/she signs the transaction with the private signing key and broadcasts it to the network. Everyone can then use the user's public verification key to validate that the transaction is unaltered and made by the real user. Regarding privacy, the transactions are meant to be completely anonymous. Despite this, third-party cryptocurrency brokers like Coinbase[Coi] are investigated by the Internal Revenue Service (IRS), whom allegedly work on mapping the wallets to users to claim taxes from cryptocurrency speculators[pri].

2.3 Evolution of distributed ledger and Blockchain

Since the arrival of Bitcoin, many alternative cryptocurrencies and Blockchain solutions have emerged. The technologies have gone through significant evolutionary steps to pursue solutions that aim to effect more globalized connectivity in the years to come.

First generation of Blockchain technology

Bitcoin was the first digital currency to solve the double spending problem without the need for a trusted authority or central server. Later on, the concept of Blockchain was separated from its specific implementation in Bitcoin. The underlying technology had a more general application beyond digital currencies, especially its capacity to function as a distributed ledger, tracking and recording any exchange of ownership. The Bitcoin design has been an inspiration for other applications and has played an essential role as a relatively large scale proof of concept. Bitcoin is a rather poor payment network, due to its scalability limitations and slow processing speed, but it is a revolutionary breakthrough as an arbiter.

Second generation of Blockchain technology

Within just a few years, the second generation of Blockchain technologies emerged. Designed as a network on which developers could build applications, and was first made technically possible by the development of the Ethereum platform. Ethereum is an open source public Blockchain-based distributed computing platform, featuring smart contract[4] functionality. Ethereum facilitates the creation of any application as it offers an abstracted foundation layer in the form of a built-in Turing-Complete programming language[5]. Any user can write smart contracts and decentralized applications with customized specifications, formats, and rules for any purpose. Ethereum provides a decentralized virtual machine, which can execute computer programs using a global network of nodes. Vitalik Buterin introduced Ethereum in a white paper [B$^+$14] in 2013, with a goal of building distributed applications. The platform went live only two years later. Ethereum has attracted a large and dedicated community of supporters, developers, and enterprises. The contribution of Ethereum as a second generation Blockchain was to extend the capacity of the technology from primarily being a database supporting Bitcoin, to becoming more of a general platform for running decentralized applications and smart contracts. As of 2018, Ethereum is the largest and most popular platform on which to build distributed applications. Everything from social networks to financial applications

[4] Smart contracts: A computer protocol to digitally facilitate, verify, or enforce the negotiation or performance of a digital contract

[5] Turing completeness: A machine is said to be Turing-complete if it can simulate any Turing machine

exists on the Ethereum platform. The evolution of Blockchain technology is heading towards the development of a globally distributed cloud computing platform, on which any application can run at the scale and speed of today's major websites, with the assurance that it has the security, resilience, and trustworthiness of today's Blockchains.

Third generation of Blockchain technology

The current technologies are still facing grand scalability issues regarding throughput and processing speed, and solving these issues are at the heart of the third generation of Blockchain technologies. The high energy consumption in the mining process is not scalable for mass adoption. Ethereum requires every node to publicly store all smart contract on the Blockchain. This continuously growing chain of data slowly decreases the performance and speed of the platform. In response to these issues, numerous technologies have entered the stage with potential solutions.

Lightning Network

The Lightning Network is known as an off-chain approach to solving the scalability issues in Bitcoin[LN]. For small payments, the transaction fees are likely bigger than the value of the transaction. The lightning network solves this by setting up a payment channel between the two parties. A multi-signature[6] address is used when setting up the shared channel, along with a buffer of Bitcoin. The channel contains a balance sheet which is updated and signed every time they want to make a transaction, without involving the Blockchain. Both entities can close the channel at any time by merely broadcasting the last signed balance sheet to the Bitcoin network, which will result in a release of the funds accordingly. Instead of having one Bitcoin transaction for every small purchase, they can limit it to two, one to open the channel and one to close the channel. Only the latest signed balance sheet can be used to unlock the money. The system does not need to have a direct payment channel between all parties. Payments can go between intermediates if these channels are already established. So the lightning network tries to minimize the complexity of the network to minimize the number of channels and intermediates needed to make these transactions. The Lightning Network is not yet live at this point, but it is assumed to go live in 2018.

Altcoins - RIPPLE XRP and Stellar Lumen XLM

Alternative crypto-coins launched after Bitcoin's success are called Altcoins. Stellar Lumen XLM and Ripple XRP are two trending crypto-currencies with an ambition to be the future of banking. They both offer fast transactions at very low fees,

[6] Multisignature: Divided responsibility, cryptographic scheme where two or more signatures are needed to be valid

both across borders. These services will eventually be integrated into more banking systems and will serve as a monetary interface between banks, corporations, and people. Ripple started out first and focused on the inter-bank relationships as a primary focus, thereby large transactions between companies and banks[DS14]. The founder of Ripple left in 2014 and then went on to develop Stellar as a fork of Ripple[Ste]. Stellar is a fully decentralized, non-profit fork of Ripple, with a reviewed consensus algorithm [SCP]. Stellar is targeting micropayments primarily, and also offer its services free to use, not alike Ripple who charges banks for using the platform. Ripple is semi-decentralized as it is managed by a company and has a CEO. The market capital of Ripple is currently more significant than Stellar (March 14th, 2018).

2.4 Discussion

2.4.1 Scalability

A critical aspect is consensus on which transactions are valid and trustworthy and consensus on when these transactions are officially "on the Blockchain". Take Bitcoin as an example. A transaction can be valid and on the Blockchain, but the transaction is not official if it is not with high probability on the Blockchain with majority consensus. In the case of Bitcoin, the confirmation of transactions can take more than an hour to be reasonably sure, not the preferred speed of a financial transaction. The consensus in Bitcoin is to trust the majority of CPU power, and the majority needs time to settle on a choice. The consensus algorithm has an enormous impact on how fast, scalable and in general how sustainable a Blockchain technology will be. A Blockchain technology where every transaction must be broadcasted to the rest of the network requires in theory a communication link between every node in the network. Although these systems would broadcast at a best effort basis, the graph would resemble a complete graph K_n with $\frac{n(n-1)}{2}$ communication links[7]. This solution is neither feasible nor scalable. With the complexity of $\mathcal{O}(n^2)$ it is clear that with as few as 10 000 users, the network would have to maintain about 100 million links to keep everyone updated in real time. In practice, however, all nodes would not stay in contact with every other node, this reduces the number of necessary communication links, at the expense of information transparency and time to consensus.

The scalability in Blockchain technologies can be branched out into several categories, some of the most important are:

- Transactions/second
- Network bandwidth usage

[7] Any participant in the network act as a node, the communication links between these are edges

- Data Storage

The ideal Blockchain technology has the maximum throughput of transactions, with minimal network bandwidth usage, and require as little as possible storage. However, specific characteristics in these technologies counteract and affect one another. Network bandwidth can be a concern in solutions where all nodes are communicating and keep updating in real time. Also, the current public Blockchain consensus protocols inherently face one major scalability limitation. Due to the decentralized characteristic of the system, all nodes need to validate and process every single transaction. The throughput of transactions/second is thus limited by the transaction processing power of every single node in the network. The decentralized infrastructure also weakens as more nodes are added to the network, as the inter-node latency will increase logarithmically with each additional node. Moreover, each node will also have to keep track of the entire state of the system, including the whole Blockchain, which is not very sustainable in a scalability point of view.

Can decentralized public Blockchain technologies scale enough to replace current financial infrastructure solutions?

There is an apparent trade-off made between decentralization and transaction throughput. VISA is currently able to process at least 56 000 transactions per second according to Senior Vice President of network processing at VISA, Manny Trillo [vis]. With 6 Blocks per hour and an average of $1000 - 2500$ transactions per block, Bitcoin averages around 2-4 transactions a second[bct]. A Bitcoin block also has a max size of 1MB which restricts the upper limit transaction throughput to approximately seven transactions per second, pretty far from VISA´s 56 000.

Ethereum’s gas limit is restricting the block size in a similar fashion as Bitcoin’s 1 MB limit. The difference is that Ethereum’s gas limit is set dynamically by the miners while Bitcoin’s block size limit is hard-coded into the protocol. With the current 8 Million gas limit [gas] and the average gas used per transaction of 21K, the average number of transactions per block is a bit under 400. One block per 20 seconds yields 20 transactions per second at best, however, accounting for more complex transactions like smart contracts, a more realistic number is around ten transactions per second.

While a decentralized consensus mechanism, in theory, offers some critical benefits, such as a firm guarantee of security, fault tolerance, authenticity, and political neutrality, it comes at the cost of scalability. The number of transactions processed by a Blockchain can never exceed that of a single participating node in the network. The available technology today is not yet sufficient to replace the current full scale monetary centralized system with a distributed Blockchain system.

How decentralized are the decentralized systems in practice?

The scalability constraints mentioned above will also restrict the access of these Blockchain technologies to a limited number of users with sufficient storage and computational power. The required specifications needed to be a part of the network would exceed way beyond what is expected of a personal computer if these systems were actually to work as intended on a global scale. Bitcoin's resilience is dependent upon the distribution and independence of the validators. As of July 2017, six mining institutions represented the hashing computer power majority (nearly 60%) of the network[maja]. As a result, these companies could/can together hijack the ledger. Hence, the consensus is not achieved and secured through mining power alone when the entire security of the Bitcoin network rests with six companies.

Another scalability issue is the large energy consumption related to the proof of work done by some of the Blockchain technologies, like for example Bitcoin. As discussed in the section on Bitcoin, the hardness on the puzzles only depend on the computing power of the miners, so the collective system is actually a great example on tragedy of the commons[8]. For every new CPU added to the mining pool, the puzzle will have to be slightly harder to maintain the average block mining frequency to once every 10 minutes. The tremendous energy put into the Bitcoin system has one purpose, to maintain decentralization.

2.4.2 Decentralization

How important is decentralization?

As discussed in the sections above, today's public Blockchain technologies cannot scale to provide a global, high-speed payment system while sustaining independence and decentralization. However, why do we need the system to be decentralized? A common answer to this question will involve trust issues with third-parties and excessive overhead resources related to resolving transaction disputes. Blockchain systems solve the problem with overhead gracefully. As an example, Ethereum facilitates smart contracts for practically any purpose, no extra overhead needed. These Blockchain systems do however not need to be decentralized to enforce a clear and strict consensus algorithm that solves disputes.

[8] Tragedy of the commons: Term used in social science to describe a situation in a shared-resource system where individual users acting independently according to their own self-interest behave contrary to the common good of all users by depleting or spoiling that resource through their collective action

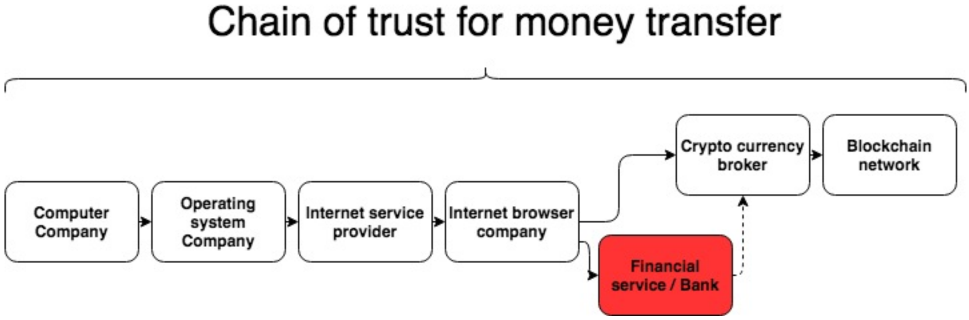


Figure 2.3: Chain of trust for cryptocurrency trading

To acquire cryptocurrencies today, we have to rely on and trust numerous third-parties. Every step of the path in obtaining and spending these digital currencies involve trusting third-parties. Figure 2.3 shows some of the entities in whom we trust to complete a financial transaction today. Any of these companies and many more can compromise the security related to the transaction. Nonetheless, we chose to trust the complete chain and assume that neither the computer company, the operating system provider, network provider, internet browser company or the cryptocurrency broker added any surveillance features to their systems. We trust that nobody added any spy-ware on our computer, and we assume that the government is not recording any key-strokes. Despite all this trust in third-parties along with our chain of trust, we still chose to put tremendous amounts of energy and money into a system that partly removes the need for one of the services provided by one particular third-party, in the case of Bitcoin, money transfer in the banking system. Although in most cases, the Bitcoin users have to bypass their bank services to obtain the cryptocurrency. The main point is, we put in enormous amounts of resources into making one part of the infrastructure autonomous regarding third-party trust, while the rest of the system is still dependent on big company third-parties. However, if we do choose to trust in a third-party to solve our needs, we can remove all scalability issues related to the decentralized solutions, and exploit the real powers of Blockchain technology.

2.4.3 Private and public Blockchain technology

We can make yet another distinction in the world of Blockchain, public Blockchain and private Blockchain.

Public Blockchain

is the well known distributed version found in technologies like Bitcoin and Ethereum. These technologies are public in the sense that no particular party is in full charge of the Blockchain. No particular party is entitled to change rules, laws, code or protocols. The modification of the Blockchain itself is set to the miners only, and a consensus algorithm approves any changes beforehand. The public is in charge of the consensus in transaction validation. The distributed infrastructure facilitate easy access to the Blockchain for anyone. Public Blockchains have slow transaction speeds because of the low "add to block" frequency, and due to loads of data processed by every node to reach consensus.

Private Blockchain

are Blockchains which are operated by an organization.[KS17] Private Blockchains are databases which are showcased as a distributed ledger. The transaction processes in private Blockchains are much faster and have a more simplistic network infrastructure compared to the public Blockchain equivalent. The consensus algorithm in private Blockchains is not driven by the majority of the network, but by the administrators/validators of the network. The validators are specific trusted nodes owned by the Blockchain company with the privilege to make blocks and add to the Blockchain. These nodes validate transactions in the same way as the miners in the public Blockchain network do. Figure 2.4 shows a simple overview of a private Blockchain process. Users send transactions to the validator, the validator then validates the transactions and make sure that the resources required to fulfill the transactions are sufficient. The validator can then sign the verified transactions and send them in a block to the administrator. The administrator then adds the block to the Blockchain. One important thing to notice is that the need for proof of work is not present, there is no ambiguity to what chain is the winning chain as there is only one chain. Hence, no unnecessary energy is wasted on cryptographic puzzles. The system depends on trusting the validator instead of trusting the majority of the system. The verification time of a transaction can be done extremely fast in this infrastructure, and it can also be scaled very nicely, an example of this will be presented in the next chapter.

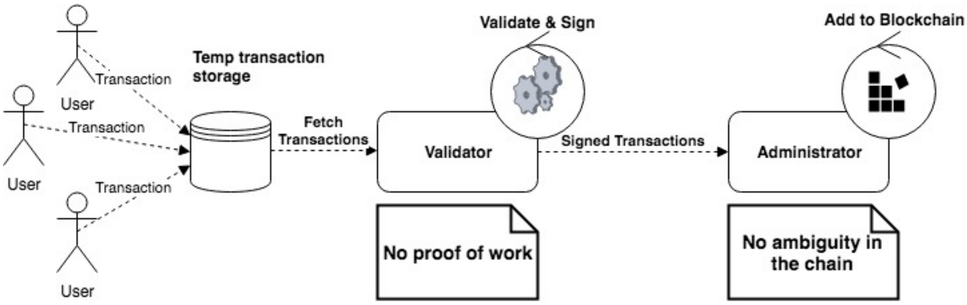


Figure 2.4: Simple overview of private Blockchain process

The creator of Ethereum, Vitalik Buterin, endorsea private Blockchains for use in institutions [But15] and also highlights the following advantages of private Blockchains over public Blockchains:

- Lower transaction cost
- Faster transaction speed
- More adaptable privacy regulation
- Technical scalability and software upgradability
- Not prone to >50% attack

Furthermore, private Blockchains also have advantages over the pure in-house database solution:

- Accountability for all transactions
- Cryptographical protection of data integrity
- Availability and transparency

Big corporations in many sectors are working on incorporating private Blockchain technologies into their systems. Bank of England is working on a proof of concept for a private Blockchain[Zha18]. The central bank will facilitate various financial transactions while maintaining privacy over a distributed network. Alibaba has made a private Blockchain to track product authenticity in the supply chain and reduce counterfeiting[Lan18]. The telecom[RS17] and energy[GD17] industries are also experimenting with private Blockchain technology. The transparency aspect of the private Blockchain can prove to be especially valuable for future solutions after the privacy regulations in regards to GDPR in May 2018[Tan16].

2.5 Available services for currency exchange

International currency exchanges are slow and costly processes if done through the regular bank system. The originating bank during an exchange might charge a fixed fee to initiate the process, any interbank can charge a fee for being a mediator, and the receiving bank can also charge a fee for receiving international exchanges. With potentially over four bank-days for the transaction to fulfill, the currency can fluctuate and thus introduce unwanted currency speculation risk on top of all fees and bad rates. Alternatively, paying directly with a foreign visa will result in an inevitable 2.0% currency markup [Ska]on top of visas own conversion rate. Using a convenient dedicated currency exchange bank like Forex[Bana] or Western Union [Banb] will be even more expensive, as their cut is about 5-10%.

The ideal way to exchange funds across currencies is to exchange with another party with the exact opposite motive. If such a trade were to happen, the two parties would physically meet up, agree upon the appropriate rate, and exchange funds without any fees or transaction costs. Without the proper channels to contact legitimate people to trade with, we are stuck with the traditional bank services. The exceptional distribution channels, trustworthiness, and availability of the banks make them the most popular service today. The banks offer various alternatives to supply the different demands of currency exchanges. Among other, here are the most popular alternatives.

- Direct cash exchange at a bank branch.
- International bank transfer
- Open currency account in a local bank.

Currency banks like Western Union[Banb] and Forex [Bana] represent the first bullet point, and are by far the most expensive alternatives, justified by the superior availability on convenient tourist locations like airports and city centers, to mention a few. The currency account is also a costly alternative, and it cannot be connected to a card. Only big banks offer this alternative, and every transaction has heavy fees[DNB].

For people who plan on staying in another country for a more extended period, creating a bank account in that given country can be financially reasonable compared to only using debit/credit cards. An international bank transfer can be a convenient way to fill the new bank account. International bank transfer is one of the services where the banks lately have experienced competition from companies like Transferwise[Tra], WeSwap[Wes] and Currency Fair[Cur]. They all offer international currency exchanges at far cheaper rates than the banks, but their concepts are slightly different.

- **Transferwise** Among the non-bank international currency exchange services, Transferwise[Tra] is probably the most popular. Transferwise has offered money transfers since 2011 with famous investors like Richard Branson and Peter Thiel on the team. Their concept is based on using an account with a big buffer in each of the countries, and never actually transfer the amount, but receive money in one currency, and pay out in another. They use the official mid-market rate without any markup. When a lot of people use the service, they will statistically even each other out. This way, Transferwise can eliminate the transaction fee, and charge a smaller fee than banks (around 1%) for the trouble. The solution is simple and available as a web app.

- **Currency Fair** Currency Fair[Cur] acts in the same way as the stock market. People can set bids on currencies and wait for someone to accept. Thus, the users can set their own exchange rates, and Currency Fair charges 0.15% of the total amount. Currency Fair also initiates the exchange themselves if nobody is there to take the exchange, for the cost of a flat fee of 3$ and a hidden exchange spread of 0.9%. Currency Fair thus gives the customers freedom to set a given exchange rate and wait for someone to take it, or sell instantly to Currency Fair for a slightly larger fee, but still not even in the same ballpark as what a bank would charge.
- **WeSwap** WeSwap[Wes] gives the customers a MasterCard which they can fill up with their local currency. Subsequently, the customers can trade currencies internally with other WeSwap customers who have the opposite need. The transfer fee varies between 1% -2%, depending on the urgency of the trade. This service is suitable for users who do not want to use their primary personal card for currency exchanges, or for users who do not have a bank account in the second currency.

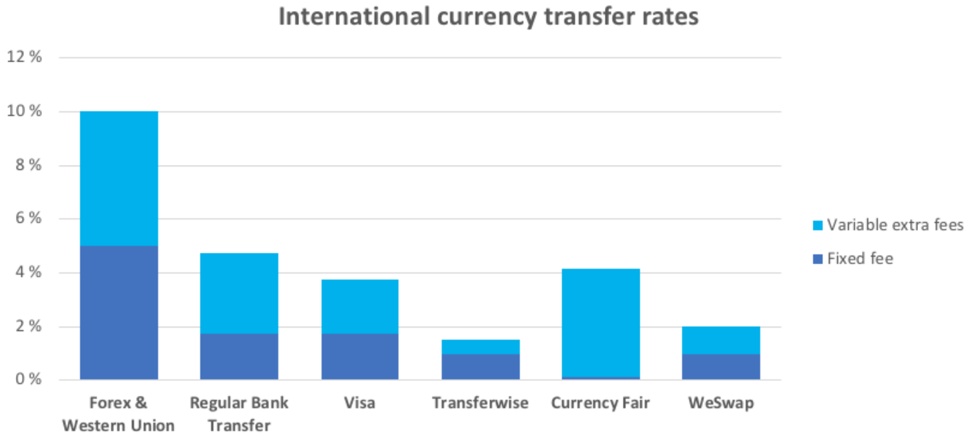


Figure 2.5: Transfer rates for some international currency exchange services

Figure 2.5 shows the rates of some popular currency exchange services. The fees vary depending on many factors, but in many cases mirror the speed, simplicity, and availability of the transfer. Currency Fair can be incredibly cheap at its best, but this is much depending on luck and urgency of the trade. Forex & Western Union are by far the most expensive alternatives, as they are physically available at airports and in cities where one would need cash quickly without an internet connection. The fastest and perhaps most stable price alternatives are direct card spending with VISA Debit for regular payments, and Transferwise for larger money transfers if an account is acquired.

Chapter 3

Private Blockchain for international currency exchange

3.1 Sonic markets introduction

This chapter will present a new private Blockchain technology for international currency exchange. The proposed system will act as a currency exchange interface between private parties and will enable faster and cheaper transfers outside of the existing inter-bank infrastructure while maintaining a secure public ledger of transaction history. Also, the system will offer transactions between cryptocurrencies and fiat currencies, and thus make cryptocurrencies more accessible and liquid. The proposed solution facilitates saving money in a pool of various currencies which in turn can proliferate the economy in countries affected by corruption, unstable currencies, and severe inflation. Throughout this thesis, the system will from here on be referred to as **Sonic Markets**. The concept and infrastructure of Sonic Markets will be introduced in the subsequent sections and chapters.

3.1.1 Interface for cheap and fast international transactions

The foundation of Sonic Markets is similar to that of Transferwise[Tra]. Sonic Markets provide currency exchanges for people and companies, by accepting money in one currency and payout the corresponding amount in another currency. To provide this service over time and to a broad audience, Sonic Markets needs to have sufficient funds in every relevant currency, a so-called "buffer". With a sufficient buffer, Sonic markets will be able to accept transactions between a wide range of currencies. The size of the buffer will vary with demand and trends, but will however statistically find an equilibrium interval in the long run as people move money back and forth between currencies. Figure 3.2 shows a transaction between two people, where the initial payment to Sonic Markets is made in USD, and the equivalent payout is made in EUR. This international currency exchange consist of two domestic bank transfers, one from person A to Sonic Markets USD account, and one from Sonic Markets EUR account to Person B, when the first transaction is confirmed. Two such domestic transfers will collectively take far less time than one international bank transfer, and in theory without extra fees and cost. The transfer time can be further reduced if the first payment is a direct payment with a visa card and not a regular bank transfer. In comparison, a direct payment will result in merely a few hours on regular days, compared to several days with a regular international bank transfer.

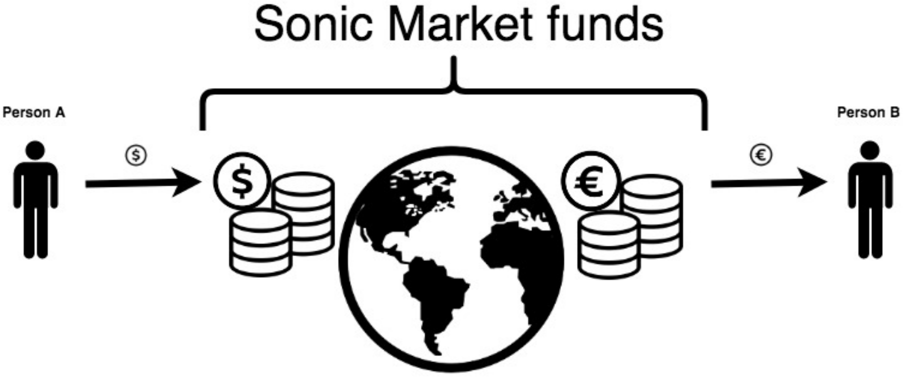


Figure 3.1: Sonic Markets act as an exchange interface

Every transaction shifts the buffer distribution of Sonic-Markets. The buffer of one currency will go up, and the buffer of another will go down. As long as all transactions are done with the real exchange rate, Sonic Markets will lose no money in the process. With a vast number of transactions initiated, the buffers will fluctuate around an equilibrium that will change with time. A small fee should be added to the transactions to facilitate maintenance and further development of the system. This fee can also be adjusted to reward transactions that push the buffers towards a more wanted portfolio. The portfolio management will be further discussed in later sections.

3.1.2 Buffer capital acquisition

The buffer capital required to engage frequent transactions for a large number of different currencies is tremendous. Holding capital at this scale is both expensive regarding interest rates/cost of capital and potential risk. To gather enough investors to lend money to fill these buffers would most likely prove to be hard, and extremely difficult to scale. However, a portfolio of these buffers collectively possesses one very desired quality. A collection of different currencies will be less affected by market fluctuations than a single currency on its own; it will be diversified[1]. A diversified portfolio of currencies can improve stability in revenues at companies where import

[1] Diversification: A risk management technique that mixes a wide variety of investments within a portfolio, in this thesis, currencies

and export is a big part of the business. Therefore, companies often hedge[2] against unwanted currency fluctuations. Currency Exchange Traded Funds (ETF)[3] is a financial instrument made for this exact purpose [Inv].

3.1.3 Sonic Hedgecoin - Cryptocurrency for currency hedging

We can accomplish the same functionality as the Currency ETF[Inv] by making a cryptocurrency that mirrors the aggregated capital of the Sonic Market buffers, see figure 3.2. For the sake of simplicity, this currency will be referred to as a Hedgecoin, for its hedging feature. Inspired by the fast "Sonic the Hedgehog", the Sonic Markets along with Hedgecoin will provide fast and cheap currency exchange and hedge unwanted currency volatility.

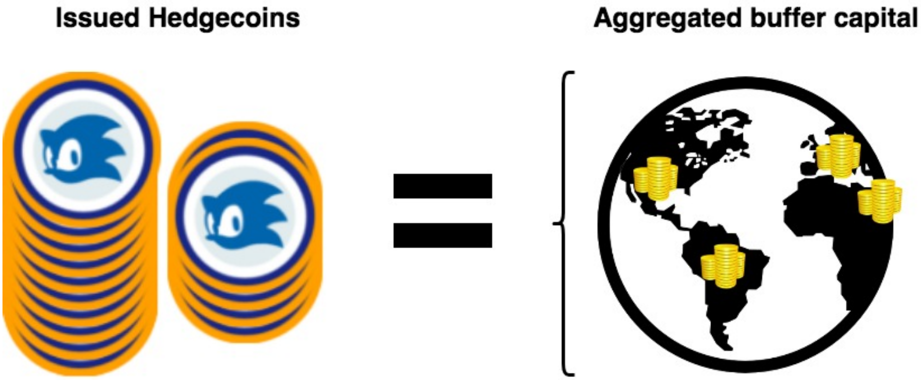


Figure 3.2: The issued Hedgecoins represent ownership of the aggregated buffer capital

Sonic Markets creates a bank account in every relevant country/currency. New Hedgecoins are issued in return for money sent/paid to these accounts. The price of one Hedgecoin equals the sum of all bank accounts divided by the number of issued Hedgecoins, and will thus vary depending on how the currencies in the buffer accounts perform relative to other currencies. The market price of the existing Hedgecoins will not change when new coins are created since customers pay market price for the new coins. However, the distribution of currencies will slightly change whenever coins

[2] Hedging: Protection against loss on investment by making balancing or compensating transactions

[3] Currency ETF: Currency Exchange Traded Funds are designed to track the performance of a single currency in the foreign exchange market against the US dollar or a basket of currencies. Currency ETFs add a layer of diversification to traditional stock and bond portfolios by hedging against economic events that might undermine normal trading [Inv]

are issued or redeemed since one of the buffers will go up or down. Hence, when one buffer increase, the Hedgecoin is more exposed to relative fluctuations of that currency, vice versa when the buffer decrease. Figure 3.3 shows an example of how the Hedgecoin can mirror a distribution of various currencies, and it is obvious that the Hedgecoin is less affected by a single currency's fluctuations given the diversification. When the customer redeems the Hedgecoins, the money is withdrawn from the buffer and transferred to the customer in the currency of choice; the Hedgecoins are also deleted. The number of issued Hedgecoins will as follows not be a fixed number.

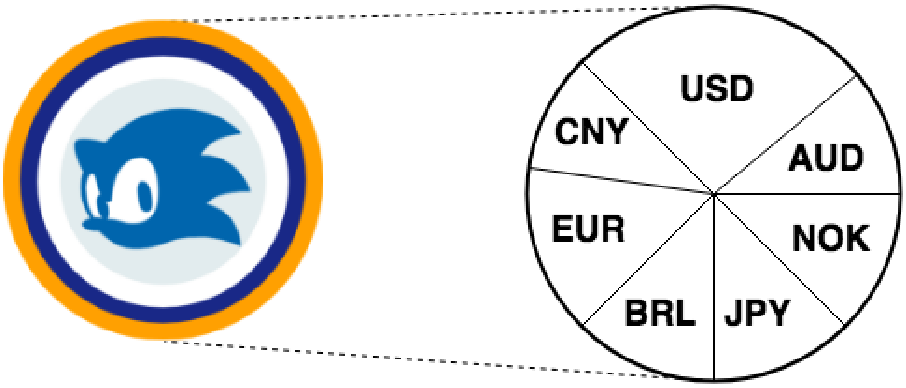


Figure 3.3: One sonic coin represents a distribution of different currencies

Non-volatile cryptocurrency

One important thing to realize is that the Hedgecoin will not be an object for price speculation in the same manner as most other cryptocurrencies. Its true value can be directly calculated as the sum of the money in the buffers divided by the number of issued Hedgecoins. The Hedgecoin price is not supposed to grow over time like other stocks or investments; it will act just like other currencies and fluctuate relatively to these.

The Sonic Market system is a service that is built independently of any particular inter-bank infrastructure. It relies solely on available services like regular domestic bank transfer and direct payments from credit/Debit cards. This infrastructure independence makes the solution highly agile for many reasons. Sonic Markets does not have to customize or integrate an Application programming interface (API) or anything to work seamlessly with any bank. Ripple[DS14] and Stellar[Ste] use a different approach, they both integrate software with banking systems which is a far more comprehensive solution that will take time, money and a much effort to complete and launch worldwide. If these solutions do succeed with time, they will be able to perform transactions faster than Sonic Markets, but not necessarily cheaper.

Chapter 4 Sonic markets technical infrastructure

Private Blockchain

A private Blockchain is maintained to record, structure, secure and preserve the transactions in the Sonic Market. Administrators and validators assigned by the Sonic Markets will be responsible for accounting the transactions and the Hedgecoins. A private Blockchain is perfect for this purpose for many reasons. Firstly, a private Blockchain can be administrated by a trustworthy company owned entity, with an opportunity to rollback. The rollback functionality essentially ensures that it will be much harder to get away with hacking an account and stealing since the consensus is not decentralized. Secondly, there is no unnecessary energy consumption related to coin mining, and only a very limited network load is required. Private Blockchains are also highly scalable and updatable, the workload can be sorted and distributed to any scale, the block size and frequency can be adjusted as needed, and the software can be updated at any time. The Blockchain ledger can also be publicly available as read-only, for transparency reasons. The consensus is not distributed in private Blockchains, the validator/administrator verifies that the transaction is not violating any requirements and signs the valid transactions.

4.1 Sonic Markets dynamics and infrastructure

The process of buying Hedgecoins is reasonably straightforward. However, the actual dynamics of the system itself comprise advanced cryptographic schemes and other vanguard algorithms to ensure integrity, availability, and confidentiality of the transaction data. Three essential entities in the Sonic market are the validator, the administrator, and the Blockchain. Sonic Markets holds several validators, and these are special trusted entities that share the responsibility of validating incoming transactions. The verified transactions are further but in blocks and passed on to the administrator who validates the block and puts it on the Blockchain. Figure 4.1 shows a simplistic overview of the system process when buying Hedgecoins, from a customer perspective.

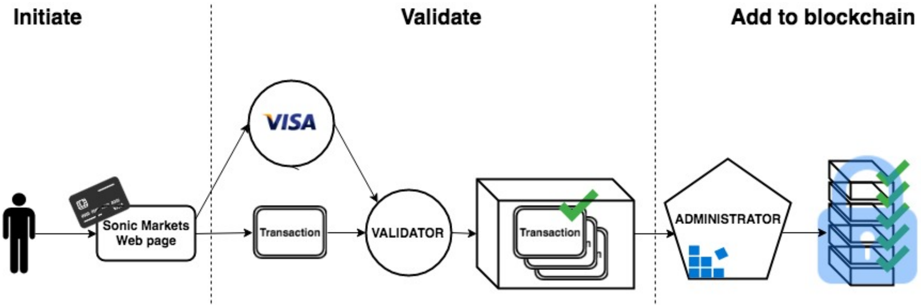


Figure 4.1: Sonic Markets Transaction process

4.1.1 Initiate

To initiate a transaction, the customer must authenticate himself/herself and enter his/her credentials into the Sonic Markets web page. The web page will display different services and alternatives, along with different payment opportunities. The customer chooses the appropriate service, enters the required information and signs the transaction with his/hers private signing key. Once the transaction is constructed and signed, it is shipped to the validator for validation.

4.1.2 Validate

When the validator receives the signed transaction from the Sonic Markets web page, it can verify that the transaction is not tampered with by checking the signature. If this transaction involves spending money from a bank account or direct payment with VISA, then VISA would also verify that the customer has sufficient funds and that the funds were transferred correctly. The verified transactions are gathered into a block and signed by the validator. The block is then passed further on to the administrator.

Sonic Markets has a set of validators to distribute the validation work-load. The administrator creates a responsibility mapping between validators and users. Each validator is assigned a share of the total image, see the yellow part of figure 4.2. This mapping is sent to all validators so that incoming transactions can be routed to the right validator.

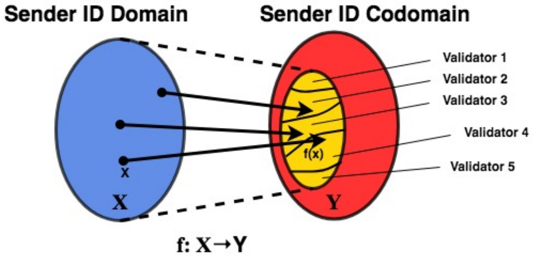


Figure 4.2: Hash of the sender ID is used to assign every new user to a validator

In figure 4.2, the sender ID is hashed (f) and mapped to the hash-function's image, which is divided evenly among the validators. Thus, any new user ID will by default have a specific validator without further assignment. The use of a hash function will make the distribution even and seemingly arbitrary. Any function f that distributes the transactions evenly in all likely cases will suffice, recognized hashing algorithms are however to prefer.

Since one particular validator verifies every transaction of a single user, this validator will have the complete overview of that user's transaction history and will thus be able to solve any double spending issues locally. The validators can thus create blocks that are completely independent without any risk om ambiguity on the Blockchain.

This setup is also very scalable, new validators can be added, and a new mapping scheme can be issued as needed. Solutions for backup storage can also be integrated to provide high availability and reliability. As illustrated in figure 4.3, a simple solution is also to send every signed block to another validator when it is passed to the administrator. That way, another validator will always have the information backed up in case of any problems. The administrator is also backed up by the collective data of all validators. Hence, if the administrator was compromised, the validators could easily reassemble the Blockchain and assign a new administrator.

4.1.3 Add to block

The administrator keeps track of all transactions, but cloud backup is also a possibility as some cloud servers are graded for financial services. When the administrator receives a block from a validator, the block signature is verified, and the transactions are once again validated. If the block passes the validation, it is signed by the administrator and added to the Blockchain. The Blockchain is privately administrated and publicly available. In that, only the administrator can add information to the Blockchain, but everyone can read the information and verify that the administrator actions are done correctly. The private Blockchain concept is completely built on

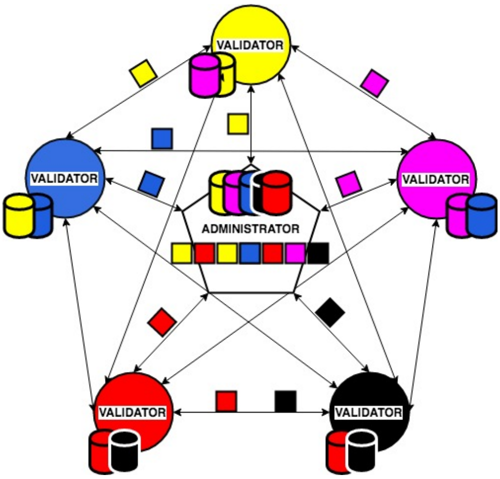


Figure 4.3: Flow of blocks between validators and the administrator

trust, so the transparency will strengthen the incentive of the administrator to act truthful and maintain security as a top priority. The architecture described above will also make hacking attacks extremely more difficult since multiple private keys are needed to alter the ledger.

Chapter 5
Sonic markets financial infrastructure

This chapter will have a more financial perspective on Sonic markets. The focus will be on how the provided service fits the current currency exchange market and how it can provide new services. We will also look at internal optimization potential and measures to reach a broader customer base with the proposed solution.

5.1 Context of proposed services

The two proposed services of the Sonic market are trading Hedgecoins and exchanging currencies. The Hedgecoin is simply an asset with currency hedging capabilities, that is useful for parties who wish to be less affected by specific currency fluctuations. While these two services may appear different, Figure 5.1 shows that one currency exchange, in essence, consist of two Hedgecoin transactions. The only real difference is the time between these two transactions. There are close to no time between transactions in a currency exchange, but when somebody wants to hedge, he or she will keep the coins for more extended periods of time before selling. Banks charge big for the risk taken while holding money during the transfer, in our case, the settlement time is close to not existing, and if any, the Hedgecoin that is held in the meantime is diversified. Thus, Sonic Market will be able to provide the real exchange rate + a small fee for the trouble.

5.2 Market bidding

Sonic Markets has no market-maker spread on the Hedgecoin. Thus Sonic Markets will immediately accept any currency transaction set to market price. Also, Sonic Markets will facilitate a bidding market where parties can set up transactions that are automatically issued when a currency reaches a certain level. As a simple example, the customer wishes to exchange 1000 NOK to USD if the NOK/USD ratio reaches 7.5. This extra feature can be handy for anyone who needs to move money but who are not in a rush, and for companies moving big loads of money who want to

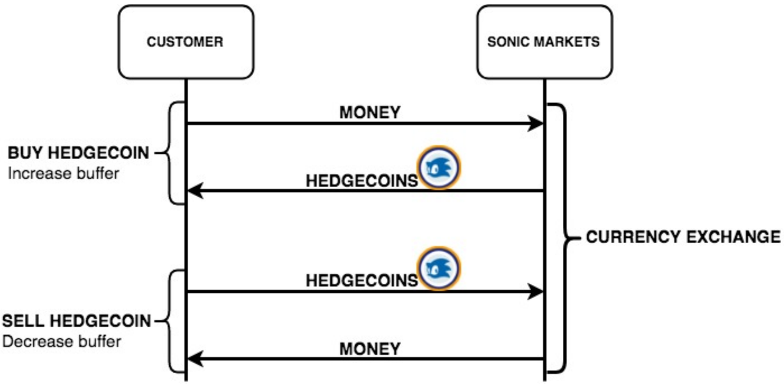


Figure 5.1: A currency exchange is the same as buying and selling Hedgecoins

diversify the given currency over a time span. The required functionality will not be incorporated into the Blockchain in the form of a smart contract like in Ethereum but will be part of the back-end functionality of the Sonic Markets. All of these are simple strategies with the intention to prevent buying a currency at a peak price. The bidding market also gives the Sonic Market an opportunity to acquire bigger buffer in a given currency if needed.

5.3 Cryptocurrencies as valid payment in Sonic Markets

Obtaining and trading cryptocurrencies are generally expensive affairs. Fees are added in many steps by several third parties, and redeeming them in the preferred currency can be tedious and laborious without passing through proxy currencies and services. Therefore, Sonic Markets will accept the top cryptocurrencies as valid payment for the Hedgecoin. An entirely new demand for the service will emerge as follows, and boost the churn rate in the buffers. Cryptocurrencies will also be more liquid and more accessible for people with less known currencies that do not have efficient cryptocurrency markets. All cryptocurrencies will trade in the same way as fiat-currencies, but the transaction time will depend on the domestic transfer/cryptocurrency processing time.

5.4 Multiple Hedgecoin types for various preferences

Although the Hedgecoin will be as independent and diversified as possible, customers do have preferences on to which currency-markets they want to be exposed. Some perhaps do not want to be exposed to cryptocurrencies, while others are not interested in Asian currencies. To accommodate different portfolio preferences, a set of different Hedgecoin types can be made. Each different Hedgecoin will have a specific portfolio profile, currency distribution, and purpose. While one Hedgecoin is trying to hedge fluctuations in the world economy, another can be a portfolio of cryptocurrencies, and a third one can hedge a specific currency, and so forth. A Hedgecoin can represent any collection of currencies to achieve the preferred currency market abilities. Each of these currencies can have a separate Blockchain to support the scalability of the system. Figure 5.2 shows a simple example of how different coins can consist of various currencies and thereby have specific characteristics and abilities. The first Hedgecoin has many different worldwide currencies and imitates the fluctuations of the world economy, a good fit to avoid the fall of one particular currency. The second Hedgecoin is heavily invested in European currencies and suits companies that wish to stabilize revenue streams for inter European business. The last example shows a portfolio with many cryptocurrencies, a diversified collection of currencies is a better alternative to invest in, compared to any single cryptocurrency.

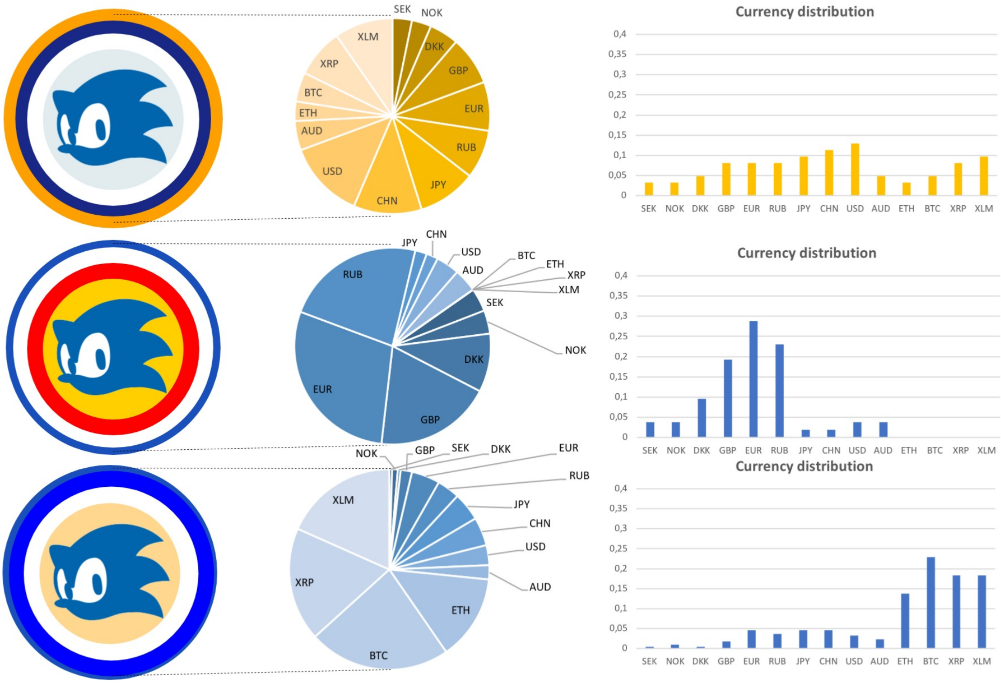


Figure 5.2: Example of currency distribution of three different Hedgecoin types, each with a specific purpose.

As mentioned, the distribution of currencies in these portfolios will continuously vary with each transaction performed and with currency fluctuations. Each type of Hedgecoin will have a preferred target distribution. This distribution is calculated by various algorithms introduced later, with a mission to find the distribution that fulfills the Hedgecoins purpose in the best manner. If the purpose is to be as diversified as possible, then the algorithms will find the combination of currencies that collectively yield the lowest variance. If the purpose is to hedge the USD, then the collection of currencies that evens out the USD fluctuations the best will be the target distribution.

A new transaction will alter the distribution of funds for a given Hedgecoin. However, the different Hedgecoins can internally perform Pareto efficient[1] exchanges of funds to get closer to the preferred distribution. As a simple example, if one Hedgecoin type would prefer to have less GBP and another would prefer to have more, they can exchange internally to both optimize their utility.

5.5 Saving money in countries with severe inflation

In countries with high inflation[Gro], saving money in the local currency can be hard and often seem hopeless. The exchange rate for these currencies are often very high, and the purchasing power is continuously getting worse. Economies with high inflation are often in high growth, and the external demand for the money is therefore often high as well. The locals would preferably store their savings in a way that is less vulnerable to inflation; an alternative could be to save in a portfolio of foreign currencies. However, it is tedious and difficult, if not impossible to get bank accounts in many different currencies, and the available financial services do not offer currency ETFs. A portfolio of cryptocurrencies is not as hard to acquire, but the available selection of coins is exceptionally volatile. The proposed Hedgecoins are perfect in this matter. People in these highly inflated countries can exchange their savings for Hedgecoins to maintain their purchasing power over time. Similarly, in exchange, companies and tourists can more easily and cheaper acquire these currencies for investments and general spending.

[1] Pareto efficiency: A resource allocation/exchange between parties where nobody is worse of. The allocation is Pareto optimal if no exchange can make any party better of without making another worse of

Chapter 6
Concept overview and market potential

Before we dive further into optimization algorithms for the currency portfolios, a summary of the proposed solution, technology and services is appropriate. Following the summary will be an overview of the Forex market and comparison between the proposed service and competing services and cryptocurrencies.

6.1 Sonic Markets overview and summary

Up until now, this paper has proposed both technical, and financial details on how Sonic markets can be implemented, as well as what features, services and financial instruments should be a part of it. The paper also progressively introduce new features, so to make sure the most critical key-components are understood sufficiently, here is a summary of the most important ones.

Sonic Markets is an international currency exchange platform and act as a mediator in the P2P, P2B, and B2B[1] currency exchange market. International currency exchanges can be done faster, cheaper and more transparent than through bank services today. Sonic Markets also facilitate saving plans in a cryptocurrency similar to currency exchange traded funds (ETF). With a financial buffer in the form of a bank account with sufficient funds in all applicable currencies, Sonic markets can receive money in one currency, and pay back in another currency without any loss in total buffer value. The buffers are funded in exchange for Hedgecoins, a cryptocurrency that represents a share of the total buffer account funds of Sonic Markets. Multiple types of Hedgecoins are offered to support various diversification needs and preferences. Each Hedgecoin mirrors a specific portfolio of currencies and aims to hedge against some currency market fluctuation. Sonic Markets will accept a few cryptocurrencies as valid payment, and will thus make these currencies more liquid and available. Sonic Markets will also help people in countries with high inflation rates, to get steadier and low inflation rate saving opportunities, through Hedgecoin.

[1] P2P - Person to Person, P2B - Person to Business, B2B - Business to Business

Private Blockchains are used to maintain and cryptographically secure the transaction history on the Hedgecoin ledgers. The private Blockchains are more scalable, reliable, faster, more secure and updatable. The Blockchains are publicly available as read-only and are further maintained continuously by the administrator and validators assigned by the system. Digital signatures enforce the integrity of the users, validators and the administrator throughout the process. The system architecture and system dynamics are highly fault-tolerant towards attacks and compromised servers. The system has an internal validator routing system for the transactions, which in theory enables unlimited scalability that can be adjusted on demand.

6.2 Potential for Hedgecoin in the Forex market

The potential for Sonic markets and Hedgecoin is great for many reasons. Due to its versatile characteristics, the Hedgecoin will be accessible to a broad audience with different needs and preferences. Some of the perhaps most obvious reasons for the great potential is listed below.

- **The Forex market is big -** The Forex market is the most actively traded market in the world, with over $5 Trillion traded daily on average[Nas]. Transferwise is the biggest non-bank currency exchange, thus the biggest of the cheap alternatives. Transferwise advertises that they move 500 million GBP each month, which is around $22 million every day. Transferwise, the biggest of these companies thus only have about 0.00044% of the Forex market. The market potential here is without a doubt enormous, even with small market shares.

- **Faster and cheaper than competitors -** The sonic markets service can be offered at a lower price than its competitors, due to the financial structure where the company itself does not hold the currency risk. As the sonic market operates outside of the international banking infrastructure, international transactions can be performed as fast as domestic transactions, which is way faster than established alternatives at the same price.

- **Agile and updatable infrastructure -** The system infrastructure is highly updatable as it consists of independent components that can easily be altered and changed without public consensus.The upgradeability applies to both hardware, including cloud infrastructure, and software concerning both security, optimization algorithms, and storage. The distributed property, storage and computational power of the servers, and frequency of backups are some of the entities that can be scaled on demand to provide reliable and efficient service.

The algorithms and software can also be updated without a Hardfork[2], and the security can be updated as needed to provide post-quantum computer secure services. The system does not waste any energy on proof of work or any time on distributed consensus; thus the complete process can be completed efficiently and fast.

- **Facilitator for the Hedging market -** The market for currency hedging is growing alongside the increased globalization. Hedgecoin will make hedging a more accessible tool for small businesses to stabilize cash flows, thereby also increasing the market for potential users of Sonic Markets.

- **Interface for the cryptocurrency market -** Cryptocurrencies are as mentioned earlier in this paper not necessarily easy or cheap to acquire. For currencies with less efficient markets, the buyer will potentially take a big hit on the spread to obtain the cryptocurrencies. Sonic Market trades at the real market price and does not have any buy or sell spread. The proposed interoperability with the cryptocurrency market will make cryptocurrencies more liquid, and make Sonic Market a highly sought after service for yet another group of potential users.

- **Support prosper economic growth for weaker countries -** The Hedgecoin can be beneficial when saving money in countries with high inflation rates. The inflation rate of Hedgecoin will be a weighted average of the inflation rates of the currencies in the portfolio, which will be low and diversified. The motivation for saving money is lost when the purchasing power deteriorates considerably with time. Since Hedgecoins does not follow the inflation of a country, money saved in Hedgecoin will relatively increase accordingly. Figure 6.1 shows some of the potential benefits of saving in Hedgecoin rather than in a high inflation currency.

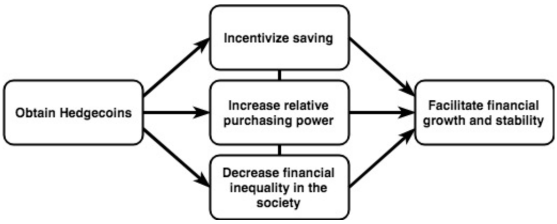

Obtain Hedgecoins
Incentivize saving
Increase relative purchasing power
Decrease financial inequality in the society
Facilitate financial growth and stability

Figure 6.1: Implications of introducing Hedgecoin to high inflation rate countries

- **Synergy effects -** All of the bullet points above introduce different customer groups with different service preferences. Having one market that serves such

[2] Hardfork: Radical change to the Blockchain protocol. The software update procedure in Blockchains with distributed consensus is more problematic

a large crowd of users with various services also introduce a synergy effect that can be valuable for company growth and popularity. Customers of one service will be more likely to use yet another service, rather than using a competing alternative. Cryptocurrency trading is also fairly new, so establishing a company that can tie the regular Forex market to the cryptocurrency market can be a lucrative business. Sonic Markets is a melting pot of what used to be distinct groups of people where the average experience with cryptocurrencies is sensibly low. The idea of combining these groups and at the same time provide a more stable cryptocurrency that has a purpose beyond speculation can prove to be valuable for the societies and companies involved.

6.3 Competitive overview of Sonic markets

Sonic Markets provide many beneficial services for a wide audience, but some of these services are already available by competitors in a similar fashion. This section will discuss pros and cons with Sonic Markets and Hedgecoin compared to competing services. Although the proposed services of Sonic Markets might have value beyond what is presented, its core functionality is narrowed down to these services.

1. Fast and cheap international currency exchange
2. Hedge currency fluctuations
3. Bridge the Forex market and the cryptocurrency market
4. Facilitate diversified saving for citizens of countries with high inflation rates.

6.3.1 Currency exchange

Is currency exchange done best solely through banks?

The market for currency exchange is huge, and a vast number of different companies provide this service at global scale. Western Union[Banb], FOREX[Bana] and banks compete on availability for the more spontaneous currency exchanges, while the competition for well planned online exchanges is quite sparse. The key factors for success in this market are price, the speed of transactions, simplicity, and legitimacy. Large banks are currently feeding most of the market through expensive and slow inter-bank transfers, but companies like Transferwise[Tra] and Currency Fair [Cur] are gaining popularity as cheaper alternatives. Blockchain technology companies like Stellar[Ste] and Ripple [DS14] are working on revolutionizing the complete inter-bank infrastructure by incorporating its services into the system of every bank. The connectivity will enable them to perform transactions in real time at close to no cost.

Banks are the go-to service for money exchange, for now

Once developed, Sonic Markets, Stellar and Ripple will be tough for the banks to beat on price and speed. The banks do however score high on availability and simplicity as the service is trustworthy, well known and located precisely where its needed the most. The bank will thus be the default choice for this service until it is commonly known that smarter and better solutions are available. For the early adopters, Transferwise and Sonic Markets serve as smarter, faster and cheaper solutions for inter-bank transfers. Given the smart financial structure, they can move money internationally with only domestic transfers, and thereby remove middle-men while saving time and resources. They are not directly connected to the banks so that the solution can be scaled end extended to new countries and currencies fast. On the other hand, Stellar[Ste] and Ripple[DS14] are connecting its service directly to the banks. This process is exhausting and comprehensive, as every bank that wants to use the system have to bridge their system with Stellar and Ripple manually. This solution will not as easily scale to new banks and currencies, but with time, it can become very powerful. If/when Ripple or Stellar manage to interconnect every global bank with their system, currency exchange can be performed within seconds for a small fee, yielding every other competing service outdated and no longer competitive.

Technology scalability

At this point, the cryptocurrency alternatives for currency exchange are not mature enough yet to manage the entire burden of a worldwide scaled autonomous system. Scalability, in general, is a common concern before implementing a standard solution, like in this case, the financial inter-bank system. Both Stellar and Ripple act like decentralized systems, where no single entity can override/control, but in reality, Ripple has a CEO and also holds an enormous amount of assets in XRP. Problems related to the consensus algorithms are mentioned in both the Ripple Consensus Algorithm paper [DS14] and the stellar basics paper, making none of them flawless and invincible. Decentralization has proven to be an expensive characteristic to retain. The decentralization aspect of Bitcoin is one of the fundamentally great ideas presented in the Bitcoin paper [Nak08], but it is also one of the worst non-scalable ideas that restrict Bitcoin from ever being what it was supposed to be, a leading global system for exchanging money.

Table 6.1 displays some of the critical characteristics for the most popular cryptocurrencies and Hedgecoin. The first column shows that the fastest two services are Ripple and Stellar, if implemented as intended, this is due to the interconnection with every bank. When it comes to transactions/second, Bitcoin is by far the worst with seven transactions/second at best. Stellar and Ripple are currently supposed to be able to handle 10 000, a number that should be enough to handle the average traffic of credit cards, but not peaks. VISA[vis] is as mentioned able to handle up to 50 000

Table 6.1: Comparison between Hedgecoin and top money transfer cryptocurrencies

	Tx time	**Tx/s**	**Tx fee**	**Mining**	**Centralized**	**Real value**	**Volatile**
Hedgecoin	Instant + domestic	Unlimited	Low fee no spread	NO	YES	YES	NO
Bitcoin	A few hours + domestic	7	0.5 - 60 USD + spread	YES	NO	NO	YES
Stellar	Instant	10 000	0.000005 USD + spread	NO	NO	NO	YES
Ripple	Instant	10 000	0.000005 USD + spread	NO	YES	NO	YES

transactions per second. Stellar, Ripple and VISA will probably be able to handle more transactions with time, as small improvements to the systems are carried out. Sonic Markets and Hedgecoin do not have any specific upper transactions/second bound. Due to the distributed validation responsibility feature, where Validators are assigned a subset of users to verify, the system is theoretically able to scale an "unlimited" number of transactions per second; due to parallelization of validators and Blockchains. In practice, each validator is limited by the bandwidth, but with a large number of validators, the collective system will not have any problem with outperforming all the other systems on scalability and number of transactions/second. To further increase the scalability, the system can maintain separate Blockchains concurrently.

Cost

The required fee varies with the demand of the cryptocurrency, Bitcoin, for example, had a transaction fee of up to 60 USD when the price peaked [Bit] during Christmas 2017. Stellar and Ripple are also very cheap for domestic transfers, but for international currency exchanges, there is a spread that has to be accounted for, this is also the case for Bitcoin transactions. How large this spread is, depends on how efficient the given exchange market is at that given point of time, but it will be in the magnitude of a few percent. The Hedgecoin, on the other hand, will only have a low fee and no spread, all transactions are performed at the known real exchange rate, thus in many cases, this alternative can be a lot cheaper. Sonic Markets is not subjected to any risk while holding the currencies, as the Hedgecoin owners own the buffer funds. Sonic Markets do not have to add any more fees than it needs to pay for server usage and software maintenance, which percentage wise will be negligible. The fees will, however, be used to incentivize favorable user behavior of users, which will be further explained in chapter 7.4 on *maintaining the optimal portfolio*.

Sustainability

Bitcoin is the only cryptocurrency mentioned in table 6.1 that is mining its coins. As discussed earlier, the Bitcoin mining is consuming enough energy to support a small country, all in an attempt to achieve decentralization. Neither Stellar, Ripple nor Hedgecoin mine their coins, but Ripple pre-mined a large amount of XRP, where investors and Ripple itself kept a large share. So it can be questioned to what degree Ripple is decentralized when it has a CEO, and the company itself owns a lot of XRP and is also able to mine more at wish. Stellar on the other hand is a non-profit organization [Ste], so it is less likely to make choices that reflect badly on the users. Sonic Markets Hedgecoins are not mined, as they are produced and destroyed to represent ownership of funds in the buffers. This paper has discussed the value of having the system fully decentralized and the limitations that follow. Among the four alternatives in table 6.1, Hedgecoin is the only without a public consensus. The private consensus is the reason why scalability is such a simple task for Sonic Markets compared to all the others. Sonic Markets is thus completely depending on having the trust of its customers to function properly. As a way to earn this trust, the ledgers are available publicly as read-only, such that any party can verify that all actions performed by the centralized authorities, e.g., validators and administrator are done correctly. Any unwanted behavior on the validator/administrator's part would result in public trust issues towards Sonic Markets, which is unwanted at all cost.

Volatility

One of the major issues with cryptocurrency systems is the price volatility. The technologies are yet immature and not functioning as they are supposed to, so much speculation is involved in what the real price of the service should be, and how it will evolve. This characteristic also attracts a new group of users, namely the speculators instead of the actual users. The cryptocurrency price volatility adds an unnecessary instability to the price of using the service. The Hedgecoin is as mentioned not volatile at the same level as any other cryptocurrency. The price reflects a portfolio of other currencies and is thus diversified and hedged against fluctuations that affect parts of the market. The speculation around the price of Hedgecoin will be the same as the speculation around the currencies in the portfolio, but the true value will be clear at any point in time. Unlike all the other cryptocurrencies mentioned, the Hedgecoin has an intrinsic value; it is backed by real cash that is backed by governments. Bitcoin, on the other hand, has value because some believe it should have.

Conclusion

To sum up, the Forex market is the biggest market in the world and includes a wide range of various services, customer groups, and preferences. Banks are currently the biggest contenders for the customers, mainly because of the simplicity, availability, and trustworthiness. Sonic Markets has some great characteristics to sustain competitive in the international currency exchange market for some time to come. The service is similar to Transferwise[Tra], but without taking any currency risk itself. Both Transferwise and Hedgecoin outperforms banks on speed and cost for international currency exchanges and can scale the business at a fast pace, as needed. Stellar and Ripple are not as easily scalable but will be the fastest and perhaps the cheapest alternative if they succeed in the future. Sonic Markets is centralized regarding consensus, but prove its legitimacy through public read-only ledgers. The Hedgecoin is not volatile, unlike Bitcoin, Stellar and Ripple. It has intrinsic value as it is backed by real funds, which thus remove the extreme speculation risk.

6.3.2 Currency hedging

The buffers are funded in return of new issued Hedgecoins. The Hedgecoins represent a diversified portfolio of various currencies, chosen to fulfill a specific purpose. Competitive alternatives to this service will be either currency ETFs or currency options. These financial products are most often offered through large investment banks who take some percentages for their expertise and advice during the process. None of these are common to buy for small businesses or the average person. The Hedgecoin is thus a simple way to adjust the exposure towards different currency markets.

6.3.3 Sonic Markets as a digital currency exchange platform

Cryptocurrency trading has until now primarily been reserved to a few currencies at the largest cryptocurrency exchange platforms like Coinbase and Poloniex. Less efficient markets do exist for most other currencies, but the prices, spread and fees get high when few are trading. Sonic Markets will support some of the top cryptocurrencies as valid payment. Any currency can thus easily be traded with cryptocurrencies, all at the right exchange rate. Sonic markets will make cryptocurrencies more liquid and attract a new large customer base for all the remaining services. Furthermore, one type of Hedgecoin can be made to mirror a portfolio of cryptocurrencies, such that a more liquid and diversified alternative can be made available for investment. The opportunity to buy cryptocurrencies with any fiat-currency will very likely increase the demand in countries without proper cryptocurrency exchange services, as the entry barrier is lowered.

6.3.4 Diversified saving for high inflation currencies

People in developing countries and other countries with high inflation may have interest in obtaining Hedgecoin for other purposes than to hedge against a particular currency fluctuation. Their goal is to not take part in the inevitable decrease in purchasing power caused by the severe inflation. This service is not available by any competitors, and similar products like options and currency ETFs are not particularly a product for the common man. These products are offered by investment banks, with high fees and most likely minimum requirements for the investments due to overhead paperwork. Investment banks are based close to large companies and governments, as they are the main customers of their business, thus rarely present in developing countries [EB15]. Hence, Hedgecoin is a product with unique availability and characteristics that can reduce the devaluation of a persons cash holdings.

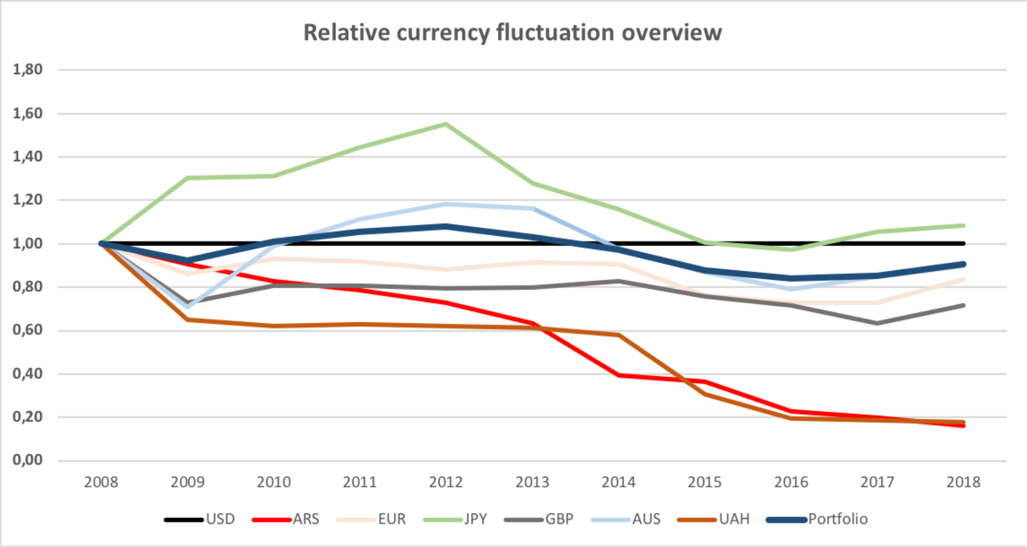


Figure 6.2: Relative change in exchange rates from 2008 to 2018

Developed countries follow the global growth

The currency exchange rate is affected by many factors like inflation, interest rate and capital gains from domestic securities, to mention some. Less developed countries, corrupt countries, and countries in war often struggle to follow the financial growth of industrialized countries, and this affects the valuation of their currency. Figure 6.2 shows the relative currency exchange rate between a set of currencies between 2008 to 2018. The USD is used as the reference currency in the figure and is therefore constantly 1. We can see that Japanese Yen (JPY) performs well in the years after 2008 and that 1 dollar worth of Yen in 2008 is worth 1.5 dollars in 2012, before diving back down towards 2008 level. The Euro (EUR), British pound (GBP) and Australian Dollar (AUS) are also big currencies that all fluctuate around the same relative exchange rate in this period.

War and corrupt governments yield financial instability

The Argentine peso (ARS) and the Ukrainian Hryvnia (UAH) deviate from the rest. These two countries have been exposed to high inflation rates and political issues for the last decade, and this has affected the relative currency exchange rate. As a trivial example from the data in Figure 6.2, if a Ukrainian person exchanged all of his savings into USD in 2008, he would have five times as much money in 2018, compared to saving it in UAH. Calculations for the effective annual interest rate is defined as:

$$\textbf{EAIR:}\ 5 = (1+r)^{10} \implies r = \sqrt[10]{5} - 1 = 0.17$$

So merely exchanging currency would correspond to an investment with an annual effective interest rate at 17%, a pretty substantial investment. On the contrary, it is not easy for a Ukrainian person to exchange all of his savings into USD, but it would be easy to exchange it into Hedgecoins. The thick purple line in Figure 6.2 mimics a diversified portfolio, a simplistic version of what a Hedgecoin could resemble. In this example, it is just an even distribution of GBP, EUR, USD and JPY, which is not the optimized partition in any way. This portfolio is statistically more stable than any single currency and also performs in accordance with an average currency, in terms of returns. It is important to stress that the primary intention of the Hedgecoin is to deliver a stable alternative, that neither performs well nor bad. In the example above, it is worth mentioning that the relative value of the USD has increased well since 2008, due to the USA regaining financial strength after the financial crisis in 2007. This is most likely one of the main reasons why EUR, GBP, and AUS all decline compared to the USD in the period 2008 to 2018. As a remark for the comparison, Ukraine, and Argentina are both in the top 20 most inflated countries in 2018 [Eco], but they are far from the worst. African and embattled countries are all high on the list, but hyperinflationary Venezuela is in serious financial issues and is topping the list with 8900% inflation rate[KAF18] from March 2017 to March 2018.

6.3.5 Overview, what markets are Sonic Markets competing in?

The venn-diagram in Figure 6.3 displays some of the competitors in the provided services. We can see that both Ripple and Stellar are, or will be, competitors in the currency exchange markets at some point. Their advantages and disadvantages are discussed in the subsections before this. Investment banks like Goldman Sachs and ABG compete in the hedging business but may fall short on the availability to the general public and the market outside wealthy countries. Large financial institutions like Barclays provide competing products in both the currency exchange and hedging business. Barclays will score high in availability for most of the standard financial services like currency exchange but are more exclusive in the hedge division and worldwide availability. Online services like Poloniex, Coinbase, Transferwise, and

Western Union (WU) all have a well-established infrastructure and are competing hard on pricing. Hedgecoin provides a unique combination of services and technical characteristics/abilities. These synergies can prove to be valuable in the competition for customers.

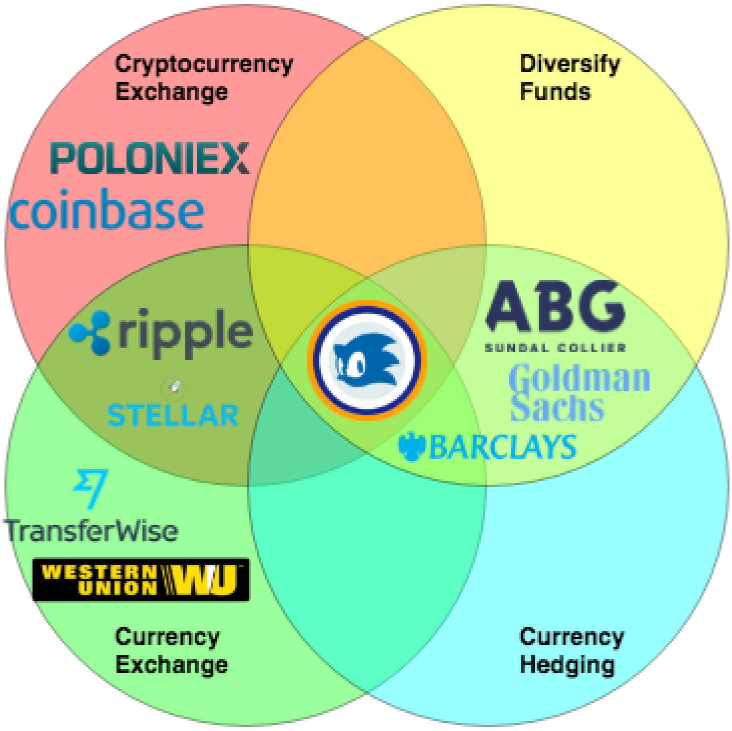


Figure 6.3: Venn diagram displaying provided services by various financial institutions

Chapter 7
Portfolio optimization

To ensure that the Hedgecoin is a valuable product that delivers as expected, we need to have some strategy and control over the portfolios. We cannot assume that the demand for Hedgecoin will be similar to the optimal currency distribution, so we need a few instruments to shape the demand, transaction flow and general dynamics of the system to provide the best possible product. The optimization part of the system is two-folded, firstly we need to find the optimal portfolio regarding our preferences. Secondly, we need a way to maintain our portfolio as close as possible to the optimal equilibrium. The two next subsections will describe how such a portfolio can be found, as well as some measures that can help maintain this portfolio distribution.

7.1 Portfolio optimization - What is the optimal portfolio?

Understanding complex systems

Any portfolio of currencies will have its own set of characteristics such as volatility, exposure towards events in various countries, technology trends, politics and so forth. These micro- and macroeconomic factors are incredibly complex, interconnected and continuously changing. A system like this is impossible to predict with certainty, but strategic choices on the portfolio composition can be made to gain valuable statistical risk related abilities, like diversification and stability. The right composition and distribution of currencies can be tough to find for any specific purpose. We can utilize optimization algorithms to improve the statistical capabilities of our portfolio, but we can never be certain that our strategy and assumptions are sufficient and encompassing since the complexity and dynamics are incomprehensible.

Assumptions

One of the main assumptions for the optimization algorithm presented in this paper is that the relationship between fluctuations of currencies to some extent persist in time. In other words, if two currencies tend to follow similar trends now and in the past, they are highly likely to do so in the future. If we can understand the underlying dynamics between the different currencies, we can design a model that utilize this information to our advantage. In this particular case, the model will combine the currencies that collectively create more stable portfolios or that neutralize specific currency fluctuations.

7.2 Portfolio optimization algorithm

The algorithm explained in this subsection will utilize the correlation between each pair of currencies, and calculate the portfolio that mathematically has the lowest variance, thereby the less volatile portfolio. We can utilize available information from time-series and eventually other sources of information to improve the statistical capabilities. If two currencies tend to follow similar or opposite trends now and in the past, they are highly likely to do so in the future. Information about the underlying dynamic of the system can be exploited to build statistically "smarter" portfolios.

Diversification

Stocks and currencies alike all other assets fluctuate relatively in value with time. While the expected growth rate (expected return) is hard to pinpoint, it is essential information to any investment. Stable assets like government bonds yield low returns, but the associated risk is also low. On the other hand, Investing in a start-up company can yield high returns, but the associated risk is accordingly extremely high. The risk is expressed through the volatility of the time-series, high risk implies big changes from data point to data point, and vice versa. Every investment or asset thus have an expected return rate and a risk in the form of a standard deviation.

Figure 7.1 shows a diagram with two assets, the USD and the Euro. The initial values in the diagram are fictional and made for explanation purposes only. In the diagram, the Euro has a low expected return of 2%, and a standard deviation of 6%, the USD has an expected return of 10% and a standard deviation of 10%. In our example, the return of the USD will be Gaussian distributed around 10% with 10% as a standard deviation. It is thus a 68% probability that the USD will have between 0 and 20% return over the next year. The dots in the diagram represent different portfolios consisting of USD and Euro. The USD is riskier than the Euro, so a portfolio of USD and EUR will inevitably be less risky than the USD, but also with a lower expected return. This way, an investor can choose the distribution of USD/Euro that best suits the preferred risk profile of the investment. In the displayed diagram, the correlation coefficient is set to -0.5, which means that the USD and the Euro are somewhat negatively correlated if one goes up, the other is a bit more likely to go down. A combination of two such assets thus cancel each other out to some extent, making the combined solution less risky than the least risky single asset, but still yield returns proportional to the distribution of the two assets. This concept is famously known as portfolio diversification and introduces one important and interesting feature. From figure 7.1 we can see that a portfolio of approximately 67% USD and 33% Euro (67/33) has the same risk profile as the Euro, but has a higher expected return. In this example, all the efficient portfolios have between 30-100% USD, depending on the preferred risk profile. This set of portfolios is known as the efficient frontier and is represented in figure 7.1 as the red line from 30/70 to 100/0. Portfolios with less than 30% USD are not optimizing the expected return for the given risk profile, as they could reduce the risk and increase expected return by adding more USD to the portfolio.

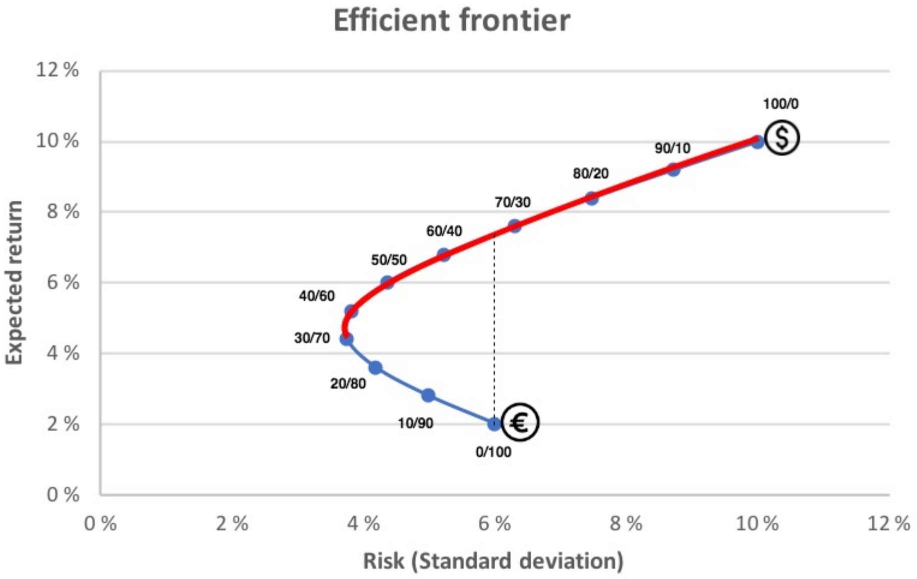


Figure 7.1: Efficient frontier example. Two currencies and their corresponding set of portfolio alternatives

Expected return

The expected return of a given currency i is defined as:

$$E[r_i] = \mu_i \tag{7.1}$$

As stressed in the previous sections, the Hedgecoin is not an investment that is supposed to yield high returns every year. It is built to hedge against currency fluctuations and to diversify portfolios. The expected return of a given currency or portfolio is not as important for our purpose since our main focus is on creating stable portfolios. Nevertheless, the expected return of a portfolio P with currencies i and proportional weight ω_i is defined as:

$$\mu_P = E[r_P] = \sum_{i=1}^{n} \omega_i E[r_i] = \sum_{i=1}^{n} \omega_i \mu_i \tag{7.2}$$

Risk

The Risk is more interesting in the case of Hedgecoin. We want to build a portfolio with various currencies that cancel each others fluctuations out as much as possible and thereby reduce the risk. Based on mean-variance analysis theory [MTS00] we define the risk as the variance of the relative currency returns, for currency i:

$$\sigma_i^2 = Var(r_i) = E[(r_i - E[r_i])^2] = E[(r_i - \mu_i)^2] \tag{7.3}$$

The covariance of two assets/currencies, i and j is defined as:

$$\sigma_{ij} = Covar(r_i, r_j) = E[(r_i - E[r_i])(r_j - E[r_j])] = E[(r_i - \mu_i)(r_j - \mu_j)] \tag{7.4}$$

The variance of portfolio P is further defined as:

$$\sigma_P^2 = E[(r_P - \mu_P)^2] = E[(\sum_{i=1}^{n} \omega_i r_i - \sum_{i=1}^{n} \omega_i \mu_i)^2] = E[(\sum_{i=1}^{n} \omega_i (r_i - \mu_i))^2] \tag{7.5}$$

$$\sigma_P^2 = E[\sum_{i=1}^{n} \omega_i (r_i - \mu_i)^2 + 2 \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \omega_i \omega_j (r_i - \mu_i)(r_j - \mu_j)] \tag{7.6}$$

$$\sigma_P^2 = \sum_{i=1}^{n} (\sigma_i \omega_i)^2 + 2 \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \omega_i \omega_j \sigma_{ij} \tag{7.7}$$

When we are dealing with more than two currencies, it is cleaner to perform calculations as cross multiplications of vectors and matrices, which also further simplifies the expression:

$$\sigma_P^2 = \vec{\mathbf{w}} \times \mathbf{C} \times \vec{\mathbf{w}}^\intercal = \begin{bmatrix} \omega_i & \cdots & \omega_n \end{bmatrix} \times \begin{bmatrix} \sigma_{ii} & \cdots & \sigma_{in} \\ \vdots & \ddots & \vdots \\ \sigma_{ni} & \cdots & \sigma_{nn} \end{bmatrix} \times \begin{bmatrix} \omega_i \\ \vdots \\ \omega_n \end{bmatrix} \tag{7.8}$$

In the expression above, $\vec{\mathbf{w}}$ is a normalized vector with the proportional weights of the different currencies. As a trivial example, a 50/50 Euro and USD portfolio would have this vector $\vec{\mathbf{w}} = \begin{bmatrix} 0.5 & 0.5 \end{bmatrix}$. Matrix $\mathbf{C}$ is the covariance matrix, a symmetric matrix with the covariance of every pair of currencies in the portfolio. These covariances are calculated with equation (7.4).

Find the optimal portfolio currency weights

The calculation in equation (7.8) will yield the variance and hence the statistically associated risk of a portfolio given the provided weight vector $\vec{\mathbf{w}}$. As seen in figure 7.1, different weight vectors have different expected returns and different risk profiles. In the example from figure 7.1, the vector $\vec{\mathbf{w}} = \begin{bmatrix} 0.3 & 0.7 \end{bmatrix}$ returned the lowest risk and is thus the most interesting portfolio for our purpose. When the number of currencies increases, we end up with an extremely complex problem, as we are looking for an optimal point or plane in a multidimensional space. The brute force approach of calculating every portfolio vector is extremely cumbersome and not attainable when the number of currencies gets large. The extensive necessary computational power is $\mathcal{O}(x * m^n)$, x is the computational power required to calculate the portfolio variance for one vector, m is the number of currencies in the portfolio, and n is the precision for each currency in the vectors. A portfolio of 8 currencies with percentage precision will have to perform 8^{100} calculations, which is more than a billion times the number of atoms in the universe. The brute force is not feasible, so we need a better approach.

Luckily, there are optimization algorithms to cope with this type of hard problems more efficiently. Quadratic programming is an example of a nonlinear optimization process that finds optimal solutions to our weight vector [Ber99]. Quadratic programming is widely used and available for most programming languages and statistical computing platforms.

Limitations and problems

While the presented risk optimizing strategy is simple to understand and work great in theory, it does have some limitations and is prone to errors that might be hard to understand and control. Here are a few of the most critical limitations to the mentioned mean-variance analysis:

- When computing the covariances for the covariance matrix, we can see from equation (7.4) that both currencies need an expected value. This issue will theoretically seem trivial, but in practice, how does one define the expected value of a currency? Is it the value of the currency the day before, or the average value over the last month? Alternatively, is it an exponentially weighted average of the last week? There is no real answer to this question, and we are left with making assumptions and hypotheses of what models our dynamic system in the best manner. All assumptions introduce bias and limitations, that can and will interfere with the validity of the result. The same issue occurs when determining the standard deviation if the problem is attempted solved with correlation coefficient ρ_{ij} and standard deviations σ_i and σ_j instead of covariance σ_{ij}.

$$\rho_{ij} = \frac{\sigma_{ij}}{\sigma_i \sigma_j} \rightarrow \sigma_{ij} = \rho_{ij}\sigma_i\sigma_j$$

- Mean-variance-optimized portfolios tend to concentrate on a few assets/currencies with the seemingly best characteristics. We lose some of the benefits from the diversification when we have overweight of a few dominating currencies. This further results in instability in the portfolio distribution, small changes in the characteristics can result in large upheaval and expensive re-allocations.

We need a more general optimization algorithm to be able to add more sources of information besides time-series of historical currency data. We also need an approach that is less affected by human errors, assumptions and lack of understanding. In an attempt to solve these issues, we will proceed with a genetic algorithm.

7.3 Genetic algorithm

Since the beginning of life on earth, nature has evolved into complex communities with intelligent life. Through countless generations and mutations, natural selection has enabled living creatures to adjust to any environment and survive extreme conditions. We can also utilize the principles of evolution to find superior portfolios with great characteristics. Genetic algorithms are heuristic search methods that can be used to find solutions to complex problems where exhaustive deterministic search methods are too comprehensive[FR07]. The genetic algorithm will return a population of solutions ranked on a set of known attributes.

7.3.1 How genetic algorithms work

Genetic algorithms start out with a big population of candidates, in our case a large set of different randomly generated portfolios. The algorithm uses a fitness score of each portfolio to determine how good its characteristics are and thereby its chances of reproducing. Mutations and crossovers are performed on these portfolios through several rounds. A mutation is and random change to the portfolio weights, while a crossover is two portfolios swapping a part of their distribution, see figure 7.2.

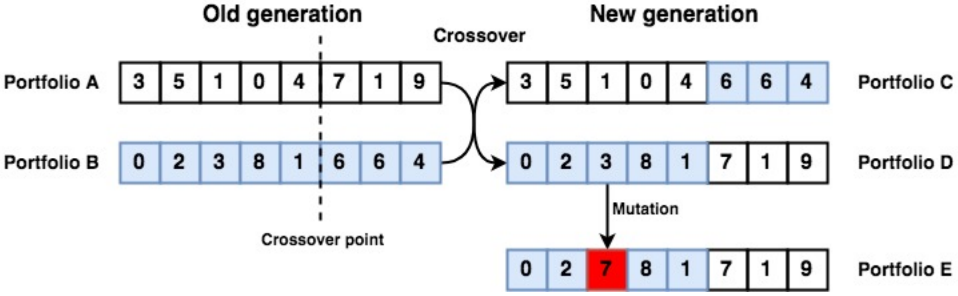


Figure 7.2: Crossover and mutation steps of a genetic algorithm

A good solution mixed with another good solution will hopefully yield better solutions in the long run. Each step in the evolution, the best candidates are chosen to form the next generation. The selection process will lead to good solutions, but not necessarily the absolute optimal solution; this all depends on how large the mutations are in the beginning and how extensive the search is. A local maximum is better than nothing when the exhaustive search space is way too large. Figure 7.3 shows the steps of the genetic algorithm.

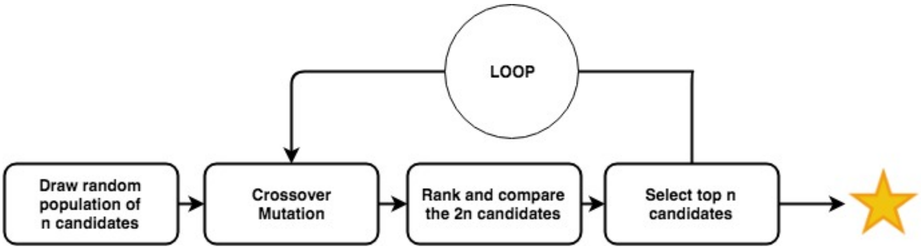

LOOP
Draw random population of n candidates
Crossover Mutation
Rank and compare the 2n candidates
Select top n candidates

Figure 7.3: Basic steps and dynamics of a genetic algorithm

7.3.2 Fitness-function and selection process

The fitness-function decides what portfolios to keep, and what to discard. Therefore, we need to tune the fitness-function, and the valuation criteria such that it accurately classify portfolios on the given characteristics. The fitness-function makes it easy to add new features that can be taken into account in the ranking procedure. Portfolios with favorable capabilities will be rewarded with high scores, while negative capabilities are punished and will thus struggle to reproduce. It is important to choose the right level of mutation at each generation to avoid too fast convergence, and potentially getting stuck with unnecessary local maximum solutions.

A genetic algorithm that only uses the mean-variance analysis alone will most likely get the same results as quadratic programming. The fitness-function enables us to add many more features in the selection of the best portfolios. We can, for example, use different correlation coefficients like Spearman's rho or Kendall's tau[ATA99], higher order of moments, or different time intervals when calculating the standard deviations. The results are more likely to be more stable when several approaches are used to find the result. We can also add new information sources, like historical media coverage data and even the scores from a machine learning analysis of related data. The possibilities are endless, but a strong data foundation and common sense are important to get a useful result.

All portfolio selection processes are based on some core assumptions to be valid. While most, if not all, are profoundly flawed and biased, it is important to remember that a randomly diversified portfolio will be more stable than a single currency in the long run.

7.4 How to maintain the optimal portfolio

The optimal portfolio composition is continuously changing and hidden behind an immensely complicated system of information. After the portfolio selection explained in the previous subsection, we want our current portfolio composition to adjust to this new portfolio distribution. We also want to maintain it at best effort, and keep it as an equilibrium state. As discussed in the previous subsection, there is much uncertainty involved in the selection process, so extreme measures to keep the exact portfolio is neither necessary nor sustainable. The goal of this part is to explain some of the measures that can be done to ensure more stable portfolio distributions and buffers that at all time can provide the expected service and keep a collectively stable profile, compared to any single currency.

Create incentives for favorable customer behavior

Sonic markets transactions will continuously shift the buffers in various directions. To be able to withstand the strain from the market in all situations, substantial buffer capacity is required. How large transactions the system can support is dependent on the size of the buffers, and its ability to restore its initial position through transactions in the opposite direction.

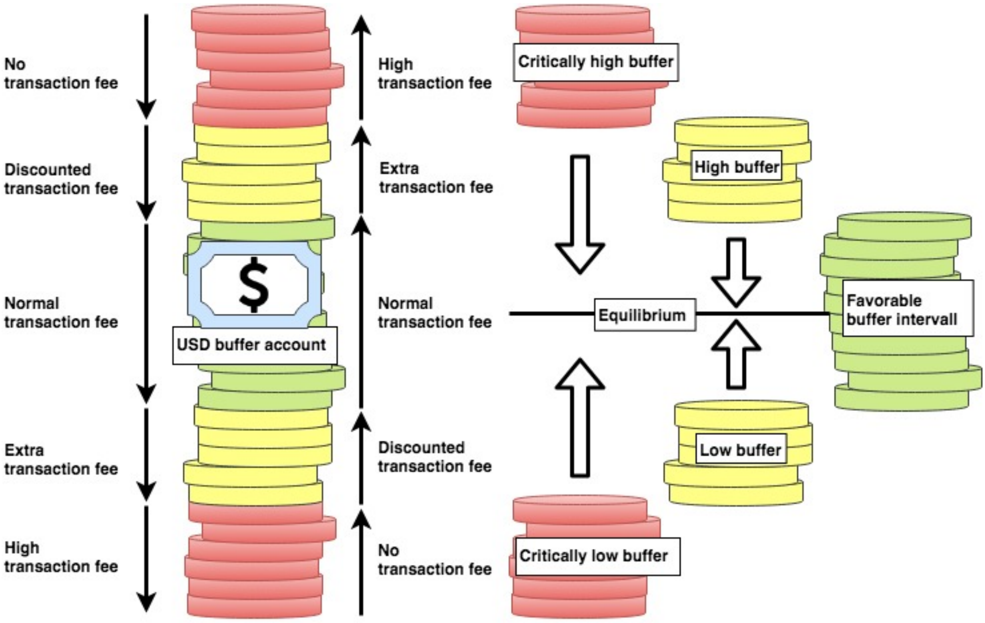


Figure 7.4: Buffer account and fee regulation to maintain favorable buffer capasity

Sonic Markets sets the equilibrium buffer capacity according to the demand for Hedgecoin in the various currencies. Figure 7.4 shows an example of the USD buffer account and its corresponding incentive-based fee regulation scheme. The fee depends on how the transaction will affect the buffers, if the transaction shifts the buffers in a direction that is more favorable, the transaction will be discounted or even free. If the transaction shifts the buffers to a less favorable state, the transaction fee will increase. The incentive-based fee regulation scheme thus encourages the customer to push the buffers towards the equilibrium, which is the currency buffer level that corresponds to the optimal buffer composition calculated in the previous subsection.

Currencies with too low buffers will have higher incentives to initiate exchanges or buy Hedgecoins due to the fee regulation and will thus be more likely to fill their respective buffers and drive the buffer capacity towards the equilibrium. Currency traders, companies and private parties are likely to exploit the low transaction fees as arbitrage opportunities and will also push the buffer account towards the preferred equilibrium state. Sonic Markets will also at all time initiate the pending market transactions from the bidding market that are Pareto efficient, to balance the buffers.

Location specific marketing

Another instrument to stabilize the buffers can be location specific online marketing. Sonic Markets can target customers from countries where the buffers are low, and similarly decrease where the buffers are high. This will further increase the demand at the location and hence increase the buffer. Due to the fee regulation scheme, these locations will also make good deals on the exchanges.

Chapter 8 Private Blockchain implementation - Proof of concept

This chapter will present the implementation of a proof of concept for a private Blockchain, while the subsequent chapter will present the implementation of a diversification optimization algorithm similar to the one presented in the previous chapter. The two implementations are by no means complete or coordinated to fulfill their respective purpose, but the main functionality and main concepts are implemented and in place. The next sections will walk through the ideas that are implemented in code, with some code snippets and figures to understand the essentials of the programs. For clarifications or deeper understanding of the provided code snippets, please see the attached zip-file for the complete code.

8.1 User

As seen in the code snippet below in listing 8.1, the user class includes only basic information about the user. Each user has a name, a unique user-ID, signing and verification keys for the digital signature, a wallet to manage the funds, as well as a transaction history record. For simplicity reasons in this proof of concept, most of the information about the users, the Blockchain and the transactions are stored in text files.

Listing 8.1: User init method

```
import wallet, Transaction,Crypto
class User():
    def __init__(self,UserID=int(0),name="Firstname␣Lastname"
            ,funds=wallet.wallet()):
        self.crypto = Crypto.Crypto()
        self.TransactionHistory = []
        self.userID = UserID
        self.name = name
        self.funds = funds
        self.__SigningKey = self.crypto.getKeyFromPem(self.userID,"sk")
```

8.2 Transaction

The transaction is an essential concept of Blockchains in general. All essential information stored on our Blockchain is formatted and packed into transactions, the rest is overhead and data used to maintain the structure and validity of the totality.

Listing 8.2: Transaction init method

```
import datetime,os,Crypto,random

class Transaction:
    def __init__(self,TransactionID,senderID,receiverID,sender_currency="X"
                ,receiver_currency="X",amount=0,text="",time=datetime.datetime.now()
                ,signature=None,nun=None):
        self.crypto = Crypto.Crypto()
        self.TransactionID = TransactionID
        self.valid = False
        self.senderID = senderID
        self.receiverID = receiverID
        self.hash = "Not-Set-Yet"
        if nun==None:
            self.nonce = self.makeNonce()
        else:
            self.nonce = nun
        self.sender_currency = sender_currency
        self.receiver_currency = receiver_currency
        self.amount = amount
        self.text = text
        self.Transaction_time = time
        self.signature = signature
        self.transactionText = self.transactionstring()
```

From the code snippet in listing 8.2 above, we can see that a transaction object contains quite a few attributes. Not all of the attributes of the transaction object is part of a transaction that goes into the Blockchain, but they have some responsibility in the creation of the transaction or in the dynamics of creating the Blockchain. As briefly mentioned in chapter 4.1, a transaction needs a sender, receiver, time-stamp and some content or text. In our case, we need to know what type of currency is exchanged into what, as well as the amount. The transaction can also include an optional text. The transaction must also include a digital signature to verify that the sender is legitimate. The usage of the transaction class will be further explained in the next sections.

8.3 Digital signatures

The program includes a class called Crypto that includes the necessary cryptography mechanisms like key management and hashing. ECDSA is used as the digital signature algorithm in this proof of concept. The signature algorithm was available as an importable package and was simple to use for our purpose. Elliptic curve algorithms are preferable due to its short keys. The code snippet from listing 8.3 below shows briefly how the keys are generated and stored as *.pem* files. The content of a .pem file is shown in listing 8.4

Listing 8.3: Key generation

```
import time,binascii,hashlib,ecdsa,os,random,sys

class Crypto:
## KEY GENERATION
    def generateKeys(self): # signing key and verification key
        sk = ecdsa.SigningKey.generate(curve=ecdsa.SECP256k1)
        vk = sk.get_verifying_key()
        return sk,vk
## store key to file
    def saveKeyAsPem(self,key,UserID,type):
        try:
            a = key.to_pem()
            open(self.getKeyFileLocation(UserID, type), "wb").write(a)
        except:
            print("Invalid␣type")

## make and store keys as .pem files
    def makeAndStoreKeysForUser(self,UserID):
        sk,vk = self.generateKeys()
        if not self.keyAlreadyExist(UserID,"sk"):
            self.saveKeyAsPem(sk,UserID,"sk")
            self.saveKeyAsPem(vk,UserID,"vk")
```

Listing 8.4: Elliptic curve signing key, text version of .pem file

```
———BEGIN EC PRIVATE KEY———
MHQCAQEEICLT7LQEqft0CoybSzt9plCZbrdWV0PTKou8tXCtASmCoAcGBSuBBAAK
oUQDQgAEUus/9S9/z0j75HiOduEpe+m/Cv9LLJYP9f03uCs9BneHHMwvyAUzB4TK
OQklaTiXlrcI720Ftf2zkDNOXF3vNw==
———END EC PRIVATE KEY———
```

Once the keys are generated, the signing and verification process is also relatively straightforward. As seen in the code snippet below in listing 8.5, the signing algorithm takes the signing key and the message to be signed as input. The signing key is private and only known by the real owner. The verification key is public and lets everyone verify that the signed message is unaltered after signing.

Listing 8.5: Signature creation and verification

```

    def signMessage(self,signingkey,message):# Returns signature
        return signingkey.sign(message.encode())
```

```
## Returns true if the verification key (public) corresponds to the
## message and the signature
    def verifySignature(self ,signature ,message ,verificationKey):
        try:
            print(verificationKey.verify(signature ,message.encode()))
            return True
        except:
            print("Invalid␣signature")
        return False
```

When all the general transaction information is added, the transaction can be signed with the owners signing key. The signature is then added to the transaction data to enforce integrity. The transaction is now ready to be shipped to the validator for validation.

8.4 Exchange

The Exchange class and the SystemController class corresponds to a currency exchange such as Sonic Markets. They are responsible for all user interaction, the delegation of transactions to validators, as well as the administrator validation and Blockchain maintenance. Figure 8.1 shows how most of the functionality is encapsulated and managed from the exchange class.

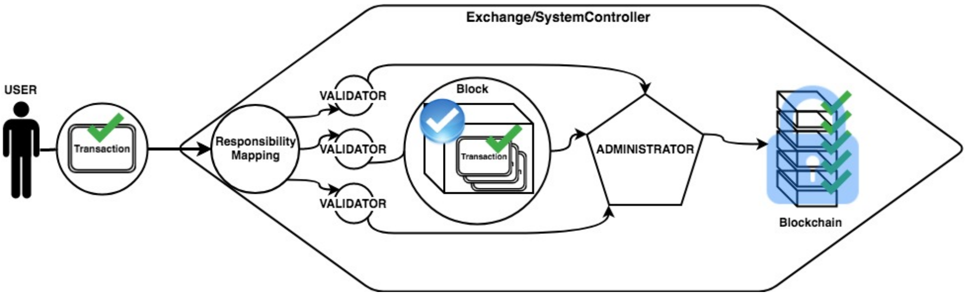


Figure 8.1: Overviews

Responsibility mapping and distribution process

When transactions are signed and shipped by the user, they are sent to the exchange. In the proof of concept, the user writes the transaction to a file called "Pending transactions". The exchange then pulls transactions from this file in bulks and sends them to their respective validator. The program routes the transactions in the same manner as proposed in chapter 6.1.2. However, the program is not online, so the different validators are therefore simulated as parallel computer threads.

Listing 8.6: Sorting, distribution and threaded validation

```
class SystemController:
    def sort_dist_validate_block_hash(self):
        self.clearValidatorLists()
        sortedSnapshot = self.snapshot_and_sort()
        self.distribute_transactions(sortedSnapshot)
        threads = []
        for i in range(len(self.ValidatorList)):
            t = threading.Thread(target=self.ValidatorList[i].validate)
            threads.append(t)
            t.start()
```

The code snippet in 8.6 shows how the program organizes the transactions and distributes them to different validators. A snapshot of the received transactions is pulled out from the file, sorted and arranged by the sender ID. They are further distributed to the transaction list of different validators before the validators execute the validation process in parallel with threads.

Validation process

The distributed responsibility of validation per user, and validation in batches/snapshot makes solving the double spending problem easy. All validators have a disjoint responsibility, so if the administrator finds an error in the block sent by validator 1, it only affects the data from validator 1, all other validators and similar transactions and users are unaffected. This enables Sonic Markets to process transactions in close to real time as there is no public consensus like in Bitcoin.

When validating the transactions, the validator gathers all transactions of each particular user and checks whether the user has sufficient funds to initiate the transactions. If the transaction signature is valid and the funds are sufficient, the transaction is added to the list of valid transactions and will be added to the next block of the validator. If not, the transaction will be rejected and discarded. The code from 8.7 process all pending transactions from a single user in that specific time interval. The program keeps track of all processed transactions when evaluating the next in the list, and will thus be protected against double spending.

Listing 8.7: Validation process, filter out invalid transactions

```
class Validator:
    def validateUserTransactions(self, transactions):
        valid_transactions = []
        invalid_transactions = []
        no_transactions = len(transactions)
        if no_transactions>0:
            user = self.exchange.Get_Member(transactions[0].getSenderID())
            if user is None:
                return valid_transactions,invalid_transactions
        else:
            return valid_transactions,invalid_transactions
        tempUserWallet = copy.deepcopy(user.getWallet())
        for trans in transactions:
            rest = int(tempUserWallet.getWalletContent()
                [trans.getMoneyInfo()[1]])\
                  -int(trans.getMoneyInfo()[0])
            if rest>=0 and self.validSignature(trans): transaction
                tempUserWallet.setFunds(trans.getMoneyInfo()[1],rest)
                validTrans = True
                for i in valid_transactions:
                    if i.TransactionID == trans.TransactionID:
                        validTrans = False
                if validTrans:
                    valid_transactions.append(trans)
                else:
                    print("Double␣spending,␣you␣will␣never␣see␣this")
            else:
                invalid_transactions.append(trans)
        return valid_transactions,invalid_transactions
```

8.5 Block

When the validator validates the transactions, they are collectively added to a block. The code from listing 8.8 shows how the block is constructed.

Listing 8.8: Init method for the Block class

```
class Block:
    def __init__(self,transactionlist,BlockID,lastHash,
    signingkey,time=str(time.time()),sig=None):
        self.crypto = Crypto.Crypto()
        self.BlockID = BlockID
        self.version = "1"
        self.timestamp = time
        self.hash_last_block = lastHash
        self.transactionlist = self.removeDuplicatedLines(transactionlist)
        self.merkleHash = self.crypto.MerkleHashMaker(self.transactionlist)
        self.transactionstring = self.makeTransactionString()
        self.blocksize = 152+len(self.transactionstring)
        self.headerString = self.makeBlockHeader()
        if sig==None:
            print("sig␣er␣None")
            self.signature = self.crypto.signMessage(
            signingkey,self.headerString)
        else:
            self.signature = self.crypto.fromHexToBytes(sig)
        self.hash_this_block = ""
```

The Block init method inputs the list of validated transactions, BlockID which is just the last Block of that particular validator + 1. The version number is added to clear any formatting issues in case of software updates at later points in time, the time-stamp is essential information to maintain the correct order of the transactions on the block. The hash of the last block is added to secure the integrity of the Blockchain; if one bit is wrong in a block, the hash will change entirely in the trailing blocks, yielding them invalid. The Merkle root hash is also described in the introductory chapter about Blockchains, chapter 4.2.2. Primarily, the Merkle root hash protects the integrity of the block transactions without having to store all transactions on the block. The code from listing 8.9 shows how the Merkle root hash is generated. The validator signs the block at last.

Listing 8.9: Merkle root hash generation algorithm

```
    def MerkleHashMaker(self, transactionlist):
        leafnodes = []
        for i in range(len(transactionlist)):
            leafnodes.append(transactionlist[i].__repr__())
        if len(leafnodes)==0:
            return self.addPadding("",64)
        startArray = leafnodes
        while True:
            endArray = []
            for i in range(0,len(startArray),2):
                if i == len(startArray)-1:
                    ConcatString = startArray[i]
                else:
                    ConcatString = startArray[i]+startArray[i+1]
                hashedConcatString = self.HashStringSHA256(ConcatString)
                endArray.append(hashedConcatString)
            startArray = endArray
            if len(startArray) == 1:
                break
        merkleHash = startArray[0]
        return merkleHash
```

Figure 8.10 shows an example of how the program outputs a block. The block contains only one transaction between user 7 and user 2 of USD 1000.

Listing 8.10: Example of a Block with one transaction

```
══════════════════════════╣ Block 1 ╠══════════════════════════
|            Version : 1                                       |
|          Timestamp : 1525685651.942175                       |
|         Block size : 423                                     |
|    no transactions : 1                                       |
|  ..............                              ..............|
| Merkle root hash : c0776eb08df7b4e01209e433d86928a5d9d9bfb
                     34d194f9c91e3a7bcbd9db140                 |
|  Last Block hash : c544c40e98bdee76946528b822f6a80cd4becdb
                     874636cf238ee786eb9b3707a                 |
| Header signature : 2a95acd5ccf50d90fd9f62d0508ce3845757624
                     2dbb7f008ab84bf82762869ddec9de8b1f88f88
                     f4de7c58f0970626c0eaf9e451b46abd4c38df9
                     88e85b5920b                              |
|———————————————————— Transactions ————————————————————|
 T.ID: 2 T.time: 1525685815.549895  SndID: 7 RecvID: 2
 Amount: 1000 USD to NOK
 Nonce: 0a43c2
 Text: Default message,Blockchain is fun
 signature: 51136c3c337d16d73d074121dbc7f40bff7c0772cdfecf5b
            f34f95ee3c48c15619f1025d41f9259c5bcc4eae828db060
            7a349c32e1d4eb4a2d4e72f495e08cba                    |
|—————————————————————————╢ End ╟—————————————————————————|
```

8.6 Blockchain

New blocks are added to the Blockchain as shown in code snippet 8.11. The transactions are then publicly available through the *TransactionsOnBlock.txt* file. A complete example of the actual Blockchain is long and can be found in the attached zip-file.

Listing 8.11: Appending new blocks to the Blockchain

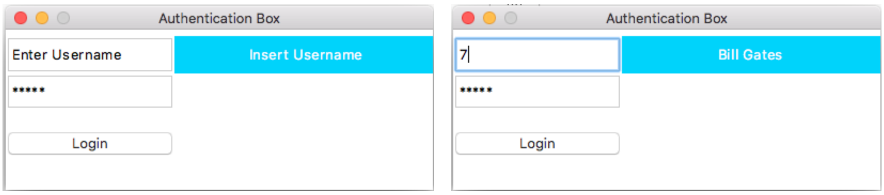
```
# Make block, add to BC, write to file
    def makeBlockAddToBlockchain(self):
        TList = self.getAllSignedTransactionsFromFile()
        if len(TList)==0:
            print("No-transacation->No-Block")
            return
        if os.stat(os.getcwd() + "/textfiles/Blockchain.txt").st_size > 0:
            lastBlock = self.BlockChain.BlockList[-1]
            Blokk = Block.Block(TList, self.BlockChain.lastBlockID+1,
            lastBlock.hash_this_block, self.AdminSigningKey)
        else:
            Blokk = Block.Block(TList,0,"Last-Hash-Sonic-Genesis-Block",
                    self.AdminSigningKey)
            print(Blokk)
        if self.BlockChain.validateBlock(Blokk):
            self.BlockChain.AddBlockToBlockchain(Blokk)
            self.moveFromSignedToBlock(TList)
        else:
            print("Error")
```

8.7 Graphical user interface (GUI)

All the most important technical components of the private Blockchain implementation is already covered in the previous sections. A brief and highly graphical overview of the Sonic Markets GUI will now be presented. The GUI is only made to be able to create transactions fast and simple, and not to create great visual experiences; I am not a graphical designer.

User login

The user login page is simple and contains a field for username or userID, and a field for password, as seen in figure 8.2. When a valid userID is presented, the name of the corresponding user is presented. This is obviously not great for the anonymity of the users, but it made login easier while testing the application.



Enter Username | Insert Username

*****

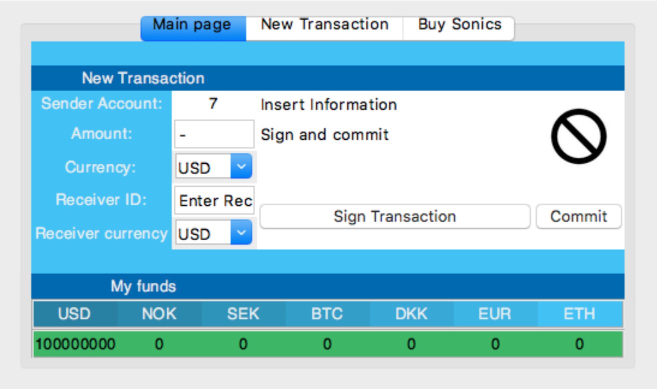
7 | Bill Gates

*****

Figure 8.2: Sonic Markets - Login page

Filling in transaction information

Once logged in, the user is presented with the following display from figure 8.3. The application displays the sender ID and the corresponding funds of the logged in user. No amount or receiver ID is yet filled in, so there is not enough information provided to complete a valid transaction, as also pointed out by the symbol in the upper right corner.



New Transaction

Sender Account: 7
Amount: -
Currency: USD
Receiver ID: Enter Rec
Receiver currency USD

Insert Information
Sign and commit

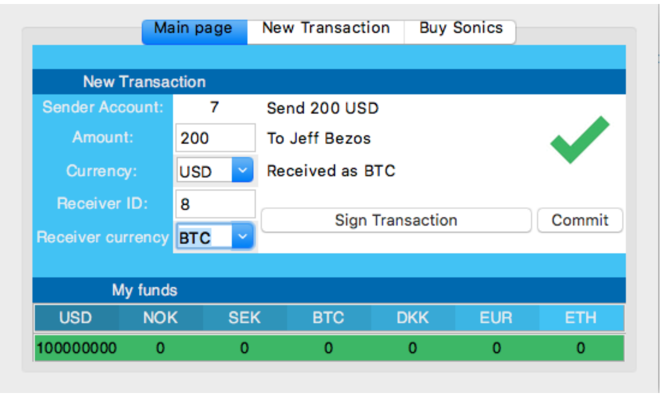
⊘

My funds

USD	NOK	SEK	BTC	DKK	EUR	ETH
100000000	0	0	0	0	0	0

Figure 8.3: Sonic Markets - Initial window

When the information is inserted with valid receiver ID and amount, we get a display similar to the one in figure 8.4. The application auto-fills the name when the receiver ID corresponds to one of the verified users of Sonic Markets. The symbol from the upper right corner also implies that the information we provided is good. Before we can commit and send out the transaction to the validator for validation, we need to sign it.



New Transaction

Sender Account: 7
Amount: 200
Currency: USD
Receiver ID: 8
Receiver currency BTC

Send 200 USD
To Jeff Bezos
Received as BTC

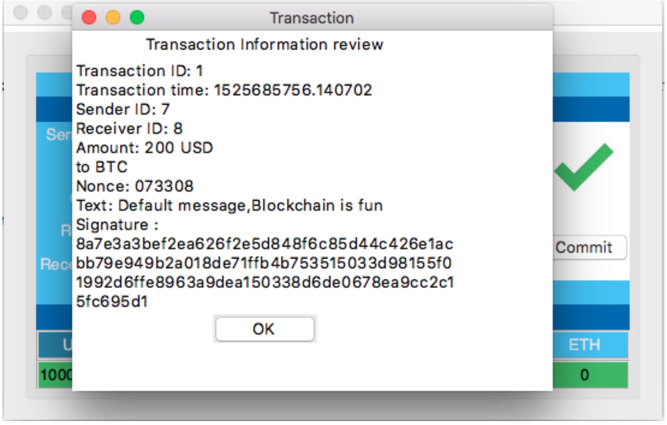
✓

My funds

USD	NOK	SEK	BTC	DKK	EUR	ETH
100000000	0	0	0	0	0	0

Figure 8.4: Sonic Markets - Transaction information fields filled in

When the *SignTransaction* button is pressed, the window from figure 8.5 is displayed. The complete Transaction information is presented, along with a digital signature of the transaction. The private signing key of the user is used to create this unforgeable signature.



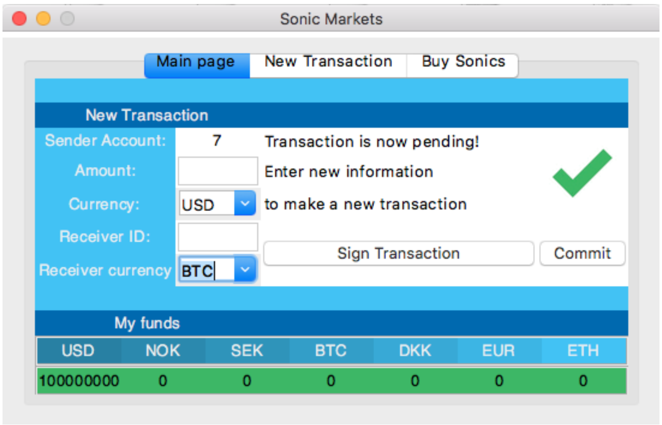
Transaction

Transaction Information review

Transaction ID: 1
Transaction time: 1525685756.140702
Sender ID: 7
Receiver ID: 8
Amount: 200 USD
to BTC
Nonce: 073308
Text: Default message,Blockchain is fun
Signature :
8a7e3a3bef2ea626f2e5d848f6c85d44c426e1ac
bb79e949b2a018de71ffb4b753515033d98155f0
1992d6ffe8963a9dea150338d6de0678ea9cc2c1
5fc695d1

Figure 8.5: Sonic Markets - Transaction Signature

If the user wants to commit to the transaction and send it to the validator for validation, the *OK* button is pressed, followed by *commit*. The window from figure 8.6 displays the application window after the transaction is signed and committed. Once committed, it enters the pending state where it is sent to the validator, or in the case of our proof of concept, simply written to the *PendingTransactions.txt* file. This file is read by the exchange and distributed to the different validators. After validation, it will be added to the *signedTransactions.txt* file, before it is finally added to the *Blockchain.txt* and *TransactionsOnBlock.txt* files.



Sender Account: 7
Amount:
Currency: USD
Receiver ID:
Receiver currency BTC

Transaction is now pending!
Enter new information
to make a new transaction

USD	NOK	SEK	BTC	DKK	EUR	ETH
100000000	0	0	0	0	0	0

Figure 8.6: Sonic Markets - Pending Transaction

8.8 Implementation overview

The private Blockchain implementation is a simple proof of concept where many of the essential ideas from the proposed Sonic markets from chapter 5 to 9 are left out to maintain a reasonable scope and complexity. The primary purpose of the implementation was to create a private Blockchain with fully functioning key management and enough dynamics and overhead to provide a feeling and understanding of the great concepts and potential behind Blockchain technology. Many details and several hundreds of lines of code are needed to glue together the seemingly simple dynamics of the proof of concept application. The scope was set appropriately to have enough time to get a detailed understanding of Blockchain technology and to include an implementation of the diversification optimization algorithm, yet to be explained in detail in the next chapter.

Chapter 9
Diversification optimization algorithm implementation

The art of making a functioning portfolio diversification program is incredibly complex and beyond what can be successfully implemented in the last chapter of a master thesis. On the other hand, a wholehearted attempt to utilize the theoretical core concepts in practice will hopefully yield some interesting results, good or bad.

The purpose of the diversification optimization algorithm is to find the portfolio with the best distribution within a set of currencies, with respect to variance. Ideally, we want to find a portfolio that reacts as little as possible to specific events and fluctuations in parts of the market, as well as portfolios that counteract these fluctuations. Throughout the next few sections, we will go through how data is collected and structured into a suitable format, followed by different correlation analysis tactics and at last, everything about the genetic algorithm. Furthermore, Before we can do any analysis of the data, we need to collect it.

9.1 Data collection

The idea of diversifying time-series of data is well documented for stocks, but not as much for currencies. The same rules apply to both stocks and currencies, as they are both assets exposed to speculation on a global scale. The code in the diversification algorithm refers to the assets/currencies/stocks as *stocks*, as I want to further explore the potential for portfolio optimization in the stock market after the thesis without having to change all variables in the code. It is not unusual for large portfolios to include both stocks and currencies.

9.1.1 Web scraper

Web APIs that deliver currency and stock information are often very expensive, as this type of information is in commercial use by traders and investment banks. www.oslobors.com is Oslo's stock exchange and lets users download daily historical data for up to 5 years for stocks and currencies. Instead of manually downloading every stock or currency, the whole process is automated with a python script.

The downloading script works like this:

- Create directory with today's date
- Create a URL for every stock/currency
- Access URL and download the historic data in XLSX files, into the new directory

The link in the code below shows the required link to download five years of USD historical data. If we look closely at the code, we can find a few interesting text fields ow which we can change. We can observe *USD* at two places, the format *.xlsx* and an extended number representing the data time span. We can adjust these fields to get the URL for other currencies at various time spans and in different formats. For our purpose, we want the maximum time span of five years and the *.xlsx* format, so the only thing we have to adjust is the field with the currency ticker, like "USD","EUR", and so forth.

Listing 9.1: URL for data download

```
https://www.oslobors.no/ob/servlets/excel?type=history&
columns=DATE%2C+CLOSE&format[DATE]=ddd.mm.YY&format[CLOSE]
=%23%2C%23%230.00%23%23%23&header[DATE]=USD&header[CLOSE]
=Siste&view=DELAYED&source=feed.ob-local.index.CURRENCIES&filter
=ITEM_SECTOR%3D%3DsUSD.NB%26%26DELETED!%3Dn1&stop=now&start=
1367964000000&space=DAY&ascending=true&filename=data.xlsx
```

The code snippet from listing 9.2 shows some of the code used to download the historical currency data. The first method creates the URL for each specific currency, where the mentioned *curls.txt* file contains the complete URL without the currency ticker. The second method is part of requesting the data from the URL and storing it with suitable names.

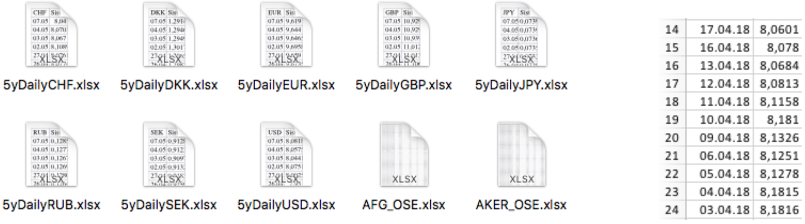
Listing 9.2: Currency data downloading code

```
# Build and customize the URL to the specific ticker
def createCUrl(ticker):
    urls = []
    url = FileManager.read_file('%s/%s' % ('text_files', 'curls.txt'))
    for elem in url:
        elem = elem[:-1]
        urls.append(elem)
    return '%s%s%s%s%s' % (urls[0], ticker, urls[1], ticker, urls[2])

def downloadAndWriteStockDataToFile(ticker, dir_to_write,stock):
```

```
if stock:
    company = ticker[0]
    market = ticker[1]
    url = createUrl(company, market)
else:
    url = createCUrl(ticker)
result = requests.get(url,stream=True)
if stock:
    filename_xlsx = '%s_%s.xlsx' %(company, market)
else:
    filename_xlsx = '5yDaily%s.xlsx' % (ticker)
FileManager.write_file_bytes('%s/%s' %(dir_to_write, filename_xlsx)
, result.content)
```

When this code is executed, the file system will have a directory with all the requested historical currency and stock data, see figure 9.1. Each file contains five years of daily historical exchange rates for each currency mentioned in the *currency_tickers.txt* file, see the complete code for further understanding. All code from the diversification optimizer can be found in the attached zip-file, only snippets of the code along with the overview will be described in this chapter.



14	17.04.18	8,0601
15	16.04.18	8,078
16	13.04.18	8,0684
17	12.04.18	8,0813
18	11.04.18	8,1158
19	10.04.18	8,181
20	09.04.18	8,1326
21	06.04.18	8,1251
22	05.04.18	8,1278
23	04.04.18	8,1815
24	03.04.18	8,1816

Figure 9.1: Downloaded historical data files, directory view and file view

9.2 Data structuring

Structuring the data in a clear and consistent way is vital to get good results. As also seen in the right image of figure 9.1, stock exchanges are closed during the weekend, so there are no changes in the exchange rate over the weekends. This little leap affects the way we must calculate our correlation matrix. The results will, unfortunately, vary with what approach we go with, which is also a great example of how fragile these calculations are towards assumptions, number errors and inaccurate number rounding. The stock data include more data points per date like high, low, weighted average, to mention some. The currency data only have one data point, so there is no need for ambiguity or assumptions on what field to use in our case.

A time-series of historical currency data can also be viewed as a vector in an n-dimensional space, where n equals the number of days in the record. It is crucial that our data vectors be flawless and ordered such that each data point corresponds to the same data point all across every currency vector. If any data points are missing in the data, it can result in big errors during the calculations. We need to make sure that missing points are interpolated and not just set to zero, consider the impact such a deviation would make when squared while calculating the variance.

9.3 Covariance matrix

We can start calculating the covariance matrix when all data is structured perfectly. From chapter 7.2, we remember that the covariance σ_{ij} equals the product of the standard deviations of the stocks and their correlation coefficient, as also seen in equation (9.1).

$$\rho_{ij} = \frac{\sigma_{ij}}{\sigma_i \sigma_j} \rightarrow \sigma_{ij} = \rho_{ij}\sigma_i\sigma_j \tag{9.1}$$

As discussed in chapter 7, there are several pitfalls in these calculations, and especially in the covariance matrix part of the calculation. For simplicity, the newer data is not weighted more than old data. Unlike with built in statistical tools, the expected value of the currency is not set to be the mean value of the complete period, $E[(r_i - \bar{r})^2]$, as this method potentially focus to much on old data. A better way to pick up the recent trends of the relative currency behaviour is to use the mean value of the previous n days as a measure for what should be the expected value, see equation 11.3. Equation 11.2 displays the variance, which is just the standard deviation squared, used to measure risk.

$$STD^2 = \sigma_i^2 = Var(r_i) = E[(r_i - E[r_i])^2] = E[(r_i - \mu_i)^2] \tag{9.2}$$

$$\mu_i = \sum_{j=1}^{n} \frac{r_{i-j}}{n} \tag{9.3}$$

Another thing to consider is whether we should assume that the standard deviation is fixed or varies with time. In real life, the standard deviation is continuously changing and impossible to determine, but in most models, also including this, we will assume it is fixed and behaves as usual.

The calculations behind the standard deviation of a currency is given below in code snippet 9.3 and corresponds to equation 9.2 and 9.3.

Listing 9.3: Standard deviation calculation for stocks and currencies

```
def calculate_standard_deviation(self, vwap_values, running_average_size):
        squared_difference_array =
            np.zeros(shape = (len(vwap_values)), dtype = np.float)
        for i in range(running_average_size, len(vwap_values)):
            iter_target_vwap = vwap_values[i]
            iter_vwap_log = vwap_values[ i - running_average_size : i]
            squared_difference_array[i] =
            self.single_calc(iter_target_vwap, iter_vwap_log)
        summation, counting_list_size =
        sum(np.absolute(squared_difference_array)),\
            (len(squared_difference_array)-running_average_size)
        return math.sqrt( summation / counting_list_size)

    def single_calc(self, target_vwap, vwap_log):
        mean_vwap_log = np.mean(vwap_log)
        if mean_vwap_log == 0:
            return 0
        return (target_vwap - mean_vwap_log)**2
```

When the standard deviation of each currency is calculated, we know from equation 9.1 that we now only need the correlation coefficient to produce the covariance and the covariance matrix. There are several ways to calculate the correlation coefficient, all depending on how the data is expected to behave, if we have many outliers and whether the data follows a specific distribution. In this implementation, NumPy is used to do the calculations. NumPy is a library for Python that adds support for large, multi-dimensional arrays and matrices. It also has built-in multiple ways to calculate the correlation coefficients, like Spearman's ρ, Kendall's τ as well as the general Pearson correlation.

Listing 9.4: Covariance matrix generation

```
import numpy as np
# Creates covariance matrix from currency history data
    def create_covariance_matrix(self, stock_list):
        nr_of_stocks = len(self.stock_list)
        covariance_matrix = np.zeros(shape = (nr_of_stocks, nr_of_stocks))
        for i in range(nr_of_stocks):
            for j in range(i, nr_of_stocks):
                standard_deviation_product =
                    self.stock_list[i].standard_deviation *
                    self.stock_list[j].standard_deviation
                temp_corr =
                    np.corrcoef(self.stock_list[i].vwap_values,
                    self.stock_list[j].vwap_values)[0][1]
                temp_covariance = standard_deviation_product * temp_corr
                covariance_matrix[i][j] = temp_covariance
                covariance_matrix[j][i] = temp_covariance
        return covariance_matrix
```

The code that generates the covariance matrix is seen in listing 9.4. The covariance matrix is a symmetric $N \times N$ matrix where N equals number of possible currencies. Location (i,j) and (j,i) corresponds to the covariance between currency i and j, which is the product of the standard deviations of i and j and the corresponding correlation coefficient, more specifically $\sigma_{ij} = \sigma_{ji} = \rho_{ij}\sigma_i\sigma_j$.

9.4 Genetic Algorithm

The genetic algorithm generates a set of random portfolios. These portfolios then go through a mutation process where only the portfolio with the highest score survives to the next generation. The process continues for a set number of generations, depending on how large mutations are. The code from listing 9.5 displays the high-level processes of the genetic algorithm.

Listing 9.5: Genetic algorithm

```
def run(self):
    counter, old_population = 0, []
    n = self.generate_population(self.number_of_candidates,
    self.number_of_assets)
    for i in range(len(n)):
            old_population.append(n[i])
    while counter < self.iter_max:
        self.plotter.plot(counter, old_population)
        best_candidate = \
            sorted(old_population, key = lambda candidate :
            candidate.fitness_score,
                    reverse = True)[0]
        new_population = []
        for candidate in old_population:
            intermediate_candidate =\
                self.evolve_candidate(candidate, old_population,
                    self.present_stock_values, self.lower_budget,
                    self.upper_budget,
                    20 ,best_candidate ,self.covariance_matrix)
            intermediate_candidate.set_fitness_score(
                self.evaluate_fitness(intermediate_candidate))
            if intermediate_candidate.fitness_score >
            candidate.fitness_score:
                new_population.append(intermediate_candidate)
            else:
                new_population.append(candidate)
        old_population = new_population
        counter += 1
    result_portfolio_dictionary = self.create_dictionary(best_candidate)
    return result_portfolio_dictionary
```

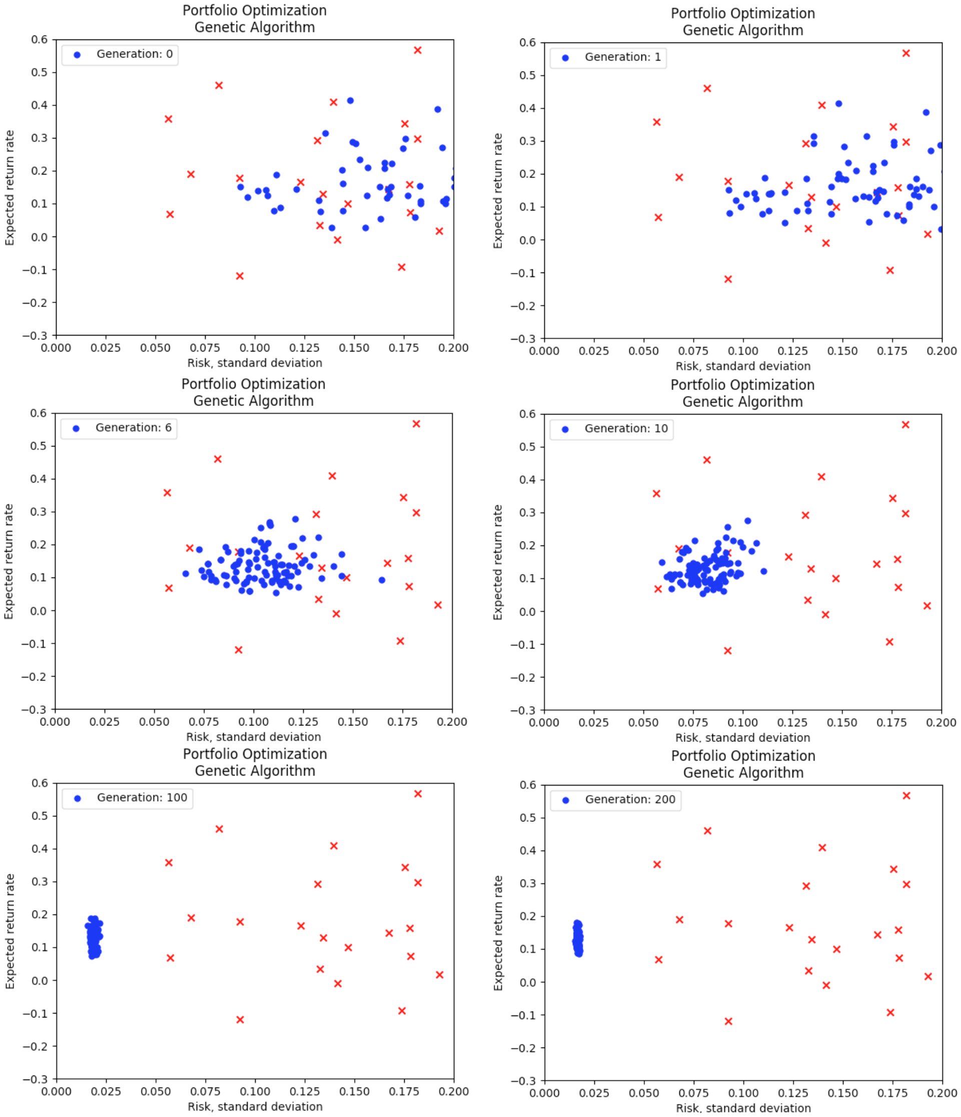


Figure 9.2: Simulation of the genetic algorithm

Figure 9.2 shows how the characteristics of the portfolios change throughout the mutation process. The upper left graph in figure 9.2 displays the first generation, where the random portfolios are represented as blue dots, and the single assets/stocks/currencies are represented as red crosses. The initial portfolios are not very good, their distribution is quite sparse, and the worst portfolios cannot even fit within the selected window. Some small changes are visible by generation 1, but in generation

6 we can see considerable improvement. Most portfolios are expected to be less risky than the average single currency. By generation 10, the cluster of portfolios is getting denser, and slowly approach a less risky state. After 100 generations, all of the portfolios are theoretically less volatile and less risky than any single currency. By generation 200, the cluster of portfolios seem to have hit the optimal portfolio composition, or at least very close to it.

The fitness score in this simulation is based entirely on reducing the variance; no effort was made to find a portfolio with a higher expected return. For currencies, our primary goal should be to find compositions of currencies that go well together and form stable portfolios. Good stocks, on the other hand, are expected to yield a preferably high return over time. The data from the simulation in figure 9.2 are from the 25 most liquid stocks at Oslo Stock Exchange Benchmark Index (OSEBX). As we can see, the portfolios together perform better on the risk, but all portfolios end up at around $13\% \pm 5\%$. This result is as expected since the average return rate on OSEBX the last five years have been 13%. If we used historical currency data instead of stock data, the expected return rate would correspond to how NOK performed compared to the world economy. When it comes to the risk axis, the optimized portfolios of currencies are expected to perform more stable than any single currency. The tendency to the diversification effect was shown in figure 6.2, but will be even greater when optimized with the genetic algorithm.

Can we trust these results?

As discussed throughout the chapters on portfolio optimization, behind these data results are many assumptions and calculations that may contain small or significant errors. Even the approach is flawed and simplistic in comparison to the complex system it is modeling. The best portfolios are only best given the very limited available data. The foreign exchange markets are continuously changing, so the optimal portfolio will change accordingly. The optimal portfolio will only be "optimal" for a very limited time span.

Due to the deterioration of the portfolios with time, it is crucial that the portfolios be frequently updated to maintain the superior characteristics. Having additional reliable data sources and more suitable correlation calculations for the fitness score can make the results more trustworthy and stable, and thereby more durable.

Chapter 10 Conclusion

Sonic Markets and Hedgecoin

The future of Blockchain technology is exciting and promising. Currently available Blockchain technologies are struggling with decentralization related issues, leading to non-sustainable solutions, scalability limitations and limited adaptability towards changes. Private Blockchain technology can solve these issues by having centralized and private consensus responsibility. The Blockchain can be redundantly stored in a distributed manner, and also provide read-only access to all users for transparency, as a better way to encourage truthful behavior without immense energy usage. Sonic Markets and the proposed Hedgecoin provides a highly scalable, adaptable and sustainable way to exchange money fast and secure internationally. Sonic Markets provides a set of different Hedgecoins that reflects a diversified portfolio of currencies, each composed to hedge against fluctuations of a specific currency or market optimally. Hedgecoin is also beneficial for decreasing exposure towards currencies with high inflation rates, and thus facilitate economic growth for countries in financial distress. The proposed solution will be able to provide better services than banks for currency exchange, but will not be able to compete on speed with Stellar and Ripple if they ever manage to build a worldwide infrastructure with every bank. Hence, Sonic Markets is a great alternative to the currently available solutions but may fall short on some features if the complete financial infrastructure gets decentralized and completely interconnected in the future.

Implementation of private Blockchain

The implementation of the private Blockchain serves as a simple proof of concept for the proposed Sonic Markets. The system is implemented with well functioning key management, control flow, and corresponding graphical user interface, to create, sign and initiate transactions. The transactions are then validated by different validators and added to the Blockchain by the administrator. The core functionality and key concepts of a Blockchain are present in the implementation and serve as an example of how simple and efficient the private Blockchain can be under the right circumstances.

Implementation of portfolio optimization program

Like with all data analysis, having sufficient and encompassing data is key for a good result, portfolio optimization for currencies is no different. Many assumptions lay the foundation for the presented diversification optimization program implementation, where the data and the analysis set limitations on how trustworthy the results are. In the case of the presented code, we are limited to historical data only, along with assumptions on how this data is distributed and should be handled. The genetic algorithm that is implemented in this thesis has great potential for further improvements concerning data sources and correlation methods. The genetic algorithm proves that it can find many optimized portfolios for the given data, that at least in theory should perform better than any single currency in terms of volatility.

Future work

The next step for the proposed system is to make a commercialized beta version within a few countries, and from there gradually expand to more currencies and larger transactions. As a way to gain trust as a financial service fast, one idea is to team up with a large company, preferably an international company. This will increase the media exposure, funding and hopefully increase the chances of building a competent team to evolve Sonic Markets further. Such a team would include cryptographers, software architects, data scientists, currency trading experts and many lawyers. The perhaps biggest bottleneck for the proposed system is the legal issues related to the expansion.

More efficient ways to store the Blockchains can also be further investigated, in that, redundant distributed storage, as well as servers that can provide users with real-time information on the Blockchain, to support the proposed transparency. There are no apparent issues related to storage of the complete Blockchain. Further development of the portfolio optimization algorithm is also necessary. More sources of information can be added to the genetic algorithm, like for example statistics from the global news picture. Data trends on positive and negative mentions on large companies and industries that may affect long-term evolution can prove to be valuable in creating stable portfolios. Furthermore, simulations can be done on the available parameters to get a better understanding of what features and methods are best suited to predict the optimally diversified portfolios.

Due to the novelty of this proposal, we intend is to publish part of this work in a peer-reviewed conference or journal shortly after submission of the thesis.

References

[ATA99] Stephan Arndt, Carolyn Turvey, and Nancy C Andreasen. Correlating and predicting psychiatric symptom ratings: Spearmans r versus kendalls tau correlation. *Journal of psychiatric research*, 33(2):97–104, 1999.

[B^{+}14] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 2014.

[Bana] Forex Bank. Currency converter. https://www.forex.no/Forex/Pages/Currency/CurrencyComverter.aspx?id=1226&epslanguage=en. [Online; accessed 31-October-2017].

[Banb] Western Union Bank. Currency converter and market alerts. http://onlinefx.westernunion.com/Currency-calculator. [Online; accessed 31-October-2017].

[bct] Average number of transactions per block. https://blockchain.info/charts/n-transactions-per-block?timespan=all. Accessed: 2018-03-09.

[Ber99] Dimitri P Bertsekas. *Nonlinear programming*. Massachusetts Institute of Technology, Athena scientific Belmont, 1999.

[Bit] Bitinfocharts. Bitcoin avg. transaction fee historical chart. https://bitinfocharts.com/comparison/bitcoin-transactionfees.html. [Online; accessed 12-April-2018].

[bmo] Bmoney. http://www.weidai.com/bmoney.txt. Accessed: 2018-03-06.

[But15] Vitalik Buterin. On public and private blockchains. *Swiss Federal Institute of Technology (ETH) Zurich Ecole Nationale des Ponts et Chauss ´ees (ENPC) Paris*, 2015.

[Coi] Coinbase. https://www.coinbase.com/. Accessed: 2018-03-11.

[Cur] Currencyfair. Fast, secure money transfers. https://www.currencyfair.com/. [Online; accessed 31-October-2017].

[DJ01] Scott Vanstone Don Johnson, Alfred Menezes. The elliptic curve digital signature algorithm (ecdsa). *Department of Combinatorics and Optimization, University of Waterloo, Canada, Springer-Verlag 2001*, 2001.

[DNB] DNB Den Norske Bank. Payments to and from foreign countries. https://www.dnb.no/bedrift/priser/betalinger-til-fra-utland.html. [Online; accessed 31-October-2017].

[DS14] Arthur Britto ripple labs Inc David Schwartz, Noah Youngs. Ripple consensus algorithm. https://ripple.com/files/ripple_consensus_whitepaper.pdf, 2014. Accessed: 2018-03-14.

[EB15] Groupe BPCE Estelle Brack, Economist. Investment banks in africa. http://aff.mfw4a.org/africa-finance-forum-blog/time/2015/02/09/blogpost/investment-banks-in-africa.html, 2015. [Online; accessed 18-April-2018].

[Eco] Trading Economics. Inflation list. https://tradingeconomics.com/country-list/inflation-rate. [Online; accessed 18-April-2018].

[FR07] Prof. Dr. Bernard Lapeyre F ´elix Roudier, Prof. Dr. Didier Sornette. Portfolio optimization and genetic algorithms. *Swiss Federal Institute of Technology (ETH) Zurich Ecole Nationale des Ponts et Chauss ´ees (ENPC) Paris*, 2007.

[gas] Ethereum average gaslimit chart. https://etherscan.io/chart/gaslimit. Accessed: 2018-03-10.

[GD17] Neon Steinecke Gunther Dutsch. Use cases for blockchain technology in energy and commodity trading. https://www.pwc.com/gx/en/industries/assets/blockchain-technology-in-energy.pdf, 2017.

[Gro] World Bank Group. Inflation, gdp deflator: linked series (annual %). https://data.worldbank.org/indicator/NY.GDP.DEFL.KD.ZG.AD?end=2016&start=2016&view=map. [Online; accessed 31-October-2017].

[Inv] Investopedia. Currency etf. https://www.investopedia.com/terms/c/currency-etf.asp. [Online; accessed 19-March-2018].

[KAF18] Rachelle Krygier and Washington Post Anthony Faiola. Venezuela hopes to tackle the world's worst inflation by deleting zeros from its currency. https://www.washingtonpost.com/news/worldviews/wp/2018/03/23/venezuela-hopes-to-tackle-the-worlds-worst-inflation-by-deleting-zeros-from-its-currency/?noredirect=on&utm_term=.a220652feb53, 2018. [Online; accessed 18-April-2018].

[KS17] Toshendra Kumar Sharma. Private vs public blockchain. https://www.blockchain-council.org/public-and-private-blockchain/difference-private-public-blockchain/, 2017. Accessed: 2018-03-12.

[Lan18] Ashley Lannquist. Blockchain in enterprise: How companies are using blockchain today. *Blockchain at Berkeley*, 2018.

[LN] Lightning network. https://lightning.network/. Accessed: 2018-03-14.

[maja] Bitcoin mining pools. https://www.buybitcoinworldwide.com/mining/pools/. Accessed: 2018-03-11.

[Majb] Majority attack. https://en.bitcoin.it/wiki/Majority_attack. Accessed: 2018-02-20.

[MTS00] Harry M Markowitz, G Peter Todd, and William F Sharpe. *Mean-variance analysis in portfolio choice and capital markets*, volume 66. John Wiley & Sons, 2000.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[Nas] Nasdaq. Forex market overview. http://www.nasdaq.com/forex/education/foreign-exchange-market-overview.aspx. [Online; accessed 31-October-2017].

[NRJ] Bitcoin energy consumption index. https://digiconomist.net/bitcoin-energy-consumption. Accessed: 2018-03-06.

[pri] Extensive irs-chainalysis partnership further revealed. https://www.ethnews.com/extensive-irs-chainalysis-partnership-further-revealed. Accessed: 2018-03-11.

[RS17] shlakshman@deloitte.com Rajarshi Sengupta, rsengupta@deloitte.com Lakshman Shankar. Blockchain – revolutionary change or not? *Deloitte - Technology*, 2017.

[SCP] Stellar consensus protocol. https://www.stellar.org/papers/stellar-consensus-protocol.pdf. Accessed: 2018-03-14.

[SHA] Descriptions of sha-256, sha-384, and sha-512. https://web.archive.org/web/20130526224224/http://csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf. Accessed: 2018-03-06.

[Ska] Skandiabanken. Priser banktjenester. https://skandiabanken.no/bruke/priser/. [Online; accessed 31-October-2017].

[Ste] Stellar basics. https://www.stellar.org/how-it-works/stellar-basics/explainers/. Accessed: 2018-03-14.

[Tan16] Colin Tankard. What the gdpr means for businesses. *Network Security*, 2016(6):5–8, 2016.

[Tra] Transferwise. Send money with the real exchange rate. https://transferwise.com/. [Online; accessed 31-October-2017].

[vis] Visa's test results: Record peak volume and expected smooth sailing for tokens. https://www.digitaltransactions.net/visas-test-results-record-peak-volume-and-expected-smooth-sailing-for-tokens/. Accessed: 2018-03-09.

[Wes] Weswap. Cheaper travel money for all. https://www.weswap.com/en/. [Online; accessed 31-October-2017].

[Zha18] Wolfie Zhao. Bank of england eyes private blockchain oversight. *Coindesk*, 2018.