VIA UNIVERSITY COLLEGE
ICT ENGINEERING

# Project Description

## Nordic Blockchain

Students:

Luca Francioni (240068)

Supervisor:

Poul Væggemose

**Revision History**

| Description | Version | Init | Revised | Approved | Date |
|---|---|---|---|---|---|
| Start of document | 0.1.0 | POV | * | * | 06/10/2018 |
| SMART P., Corrections, Milestone extension | 0.2.0 | POV | | | 15/10/2018 |
| Delimination added for testing | 0.3.0 | POV | | | 11/15/2018 |
| Updated to respect BPR2 planning | 0.4.0 | MIVI | | | 14/03/2019 |

## Sommario

## 1. Background description

With the invention of the bank in 2000 BC in Assyria, India and Sumeria merchants have been able to deposit and withdraw large sums of money with guaranteed security and loans for farmers and new-born traders traveling between the cities; a necessary structured organization that would simplify the exchanging and trading significantly, gaining the attention and better development during the medieval and Renaissance in Italy in Florence, Venice and Genoa due to their centralized trading and huge sums of money would move between continents.

Even in the modern world, banks have a fundamental role in the everyday routine both for normal individuals and entrepreneurs, so much that the financial crisis of 2007-2008 and subsequent failure of multiple worldwide banks brought with them most of their customers and entrepreneurs that depended from them.

Such catastrophe brought to the individuals the feeling of the need of a better banking system, secure by design and that could not be manipulated by private or government sectors: Bitcoin came out from unknown individual/s and with it, the Blockchain technology that changed the fundamental approach to economy that continues to find better employment even today in bank systems, schools, government structures including healthcare and much more.

International transactions are a big security concern by multiple banks, such security methods are nothing more than a strict compromise between necessity and security but often becoming a problem through its limitations; multiple banks and companies adopted different service providers or gateways and integrating these into the mobile and portable technologies, incrementing the necessity of security but making harder the inter-bank operations.

A Blockchain, whose purpose is to create consensus of the operations between multiple nodes and secure by design, becomes a necessity in the modern banking systems to allow substantial transactions to be both secure and verifiable by multiple different banks but without renouncing to the viability of the service.

## 2. Definition of Purpose

The purpose of the project is to create a blockchain based background system capable of becoming the new standard offering flexible – yet secure and fast – processor for transactions and consensus of the bank systems; usable for any service that employ either sending or receiving assets (money) trough the already existing customer-focused services.

## 3. Problem Description

The project focuses on a valid starting point for bank software industry, proposing a solution to the base design problem of implementation of a blockchain in a bank contextual executive management.

The project focus is to create the Blockchain technology with specific core functionalities, cryptography and the Peer-to-Peer network architecture. Every blockchain node is responsible to update its ledger and perform the various security procedures, being able to submit new transaction records and affirm persistence in all the nodes such that every global entity can consult its content.
It will contain and be developed towards the necessity of a bank's system.
Additional blockchain features may be added based on necessity and time.

- How to create a registry-like system for transaction recording?
- How can the Blockchain communicate with other nodes?
- How to guarantee a strong security measure towards ledger's modification?
- How can a block be authenticated through a cryptographic algorithm?
- How can a block be inserted and registered?
- How can the system be flexible towards offline nodes or with unstable connectivity/limited hardware capabilities?
- How can the entire system be stable and scalable?
- What data will the transaction contain?
- How can a transaction be secured?
- How can a transaction be confirmed by an automated process?

## 4. Delimitation

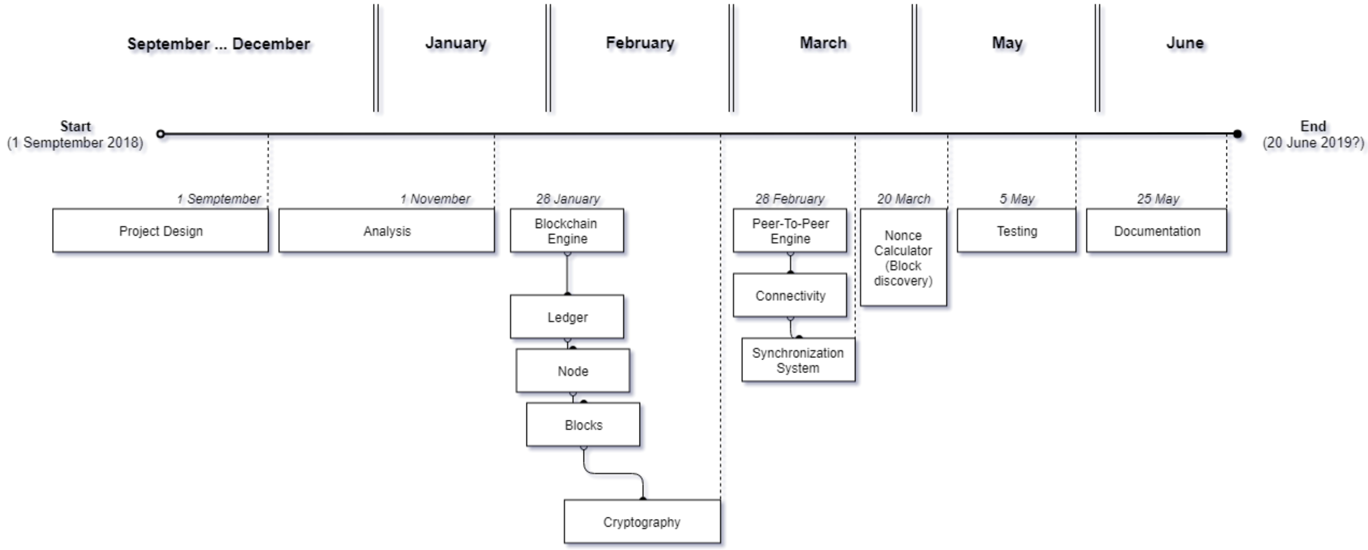
- Blocks will not contain information that are not strictly needed by the bank's system.
- Blocks will not contain real-world data.
- Blockchain will not include extensive APIs for the blockchain manipulation (e.g. Frontend, API Wrapping).
- The project will not try to solve the "51 percent attack".
- Project will not develop the "Lightning Network".
- The Blockchain will be tested only between 2 or more nodes.
- The Merkel Root Block will be arbitrary in this project.
- Project will not use CPR numbers, only purpose generated data.
- The bank entities and systems are going to be emulated inside a virtual network, trough "Test Stubbing" the end-points for traffic simulation.
- Segregated Witness protocol may not be implemented in the prototype.
- Manual override of transaction confirmation/rejection is not included in the prototype.

## 5. Choice of models and methods

| **WHAT**<br>*Partial problem* | **WHY**<br>*Why study this problem?* | **WHICH**<br>*Level of outcome expected?* | **WHICH**<br>*Which models/theories are expected to solve the problem?* |
|---|---|---|---|
| How can the Blockchain communicate with other nodes? | Main feature of the project is to maintain connectivity. | Nodes will be able to communicate with each other and send or receive updates. | Setup inter-connectivity and protocol design for the P2P communications using WebSocket as protocol base. |
| How can a block be authenticated trough a cryptographic algorithm? | Main feature of a blockchain that guarantees security. | System will be able to authenticate blocks. | Usage of Asymmetric and One-Way Cryptography that is IEEE/ISO/FIPS approved. |
| How can a block be inserted and registered? | Core functionality of the Blockchain. | Blockchain will always have enough blocks for the operations. | The block creation and synchronization is delegated to the node. |
| How can the system be flexible towards offline nodes or with unstable connectivity/limited hardware capabilities? | Certain bank may not have the best technology availability or systems may go down temporarily. | Every node will update itself to the latest version. | Blockchain technology standards are flexible by design, it will automatically update its blocks and their content as soon as they are back into the network through the P2P network. |
| How can the entire system be stable and scalable with potential infinite size? | The project's service is essential and must be able to run without unplanned interruptions and new nodes might join any time in any amount. | Blockchain will offer up to global bank participation. | Implementation of Segregated Witness mechanism may mitigate scalability problem. |

| | | | |
|---|---|---|---|
| How to allow and handle external connections for the various operations? | Between nodes there must be a protocol that is optimized for this project. | Development of a new protocol or adaptation of an existing solution. | Usage of custom designed JSON payloads residing in an SSL protocol wrapped WebSocket. |
| What data will the transaction contain? | The data inside the transactions are vital for the bank's systems interpretation. | Every transaction can be interpreted and recognized by any type of bank system. | Use Case Modelling. Identification of core components of a transaction by real world examples. |
| How can a transaction be secured? | The data inside the transaction must be safe from tempering. | Every transaction must be untouchable by unauthorized entities. | Usage of Asymmetric Cryptography, such as RSA. |
| How can a transaction be confirmed by an automated process? | The transactions must be confirmed through a strict process. | The transaction must be processed before being confirmed and considered valid. | Implementation of a new kind of "miner", processing the transaction in several cryptographic steps. |

## 6. Project Plan



## 7. SMART Goals

To define the goals to reach for this project, the S.M.A.R.T (Specific, Measurable, Attainable, Relevant, Time-Based) principles are applied and described below.

- **Goal:** documentation must be clear and as much comprehensive as possible.

  Within the start of December the documentation will be ready and refined, complete with all needed information that will allow me to proceed with a project design and a clear objective and steps to follow during the implementation.
  The documentation will be revised every week for eventual modifications while distributing its workload during all the week; such that the company and me will benefit from the written details.

- **Goal:** project design must be comprehensive and clear for whoever will work on the project.

  The design should have the most comprehensive library of details of the implementation as possible, allowing me to define my steps and goals/milestones better and to allow my supervisor and company representative to understand the implementation and the functionalities of the various parts of the project.
  Such task will be possible by first design parts of the project and then to revise them periodically based on the needs of the other parts and will also be periodically evaluated by both my supervisor and the company representative.
  Such task can be completed within the second half of January, but might be edited multiple times until the end of the whole project.

## 8. References

Rostyslav Demush, 2018. “*How Companies Can Leverage Private Blockchains to Improve Efficiency and Streamline Business Processes*” [Online]
https://perfectial.com/blog/leveraging-private-blockchains/

Rostyslav Demush, 2018. “*Blockchain Scalability Issue: Why Is There a Problem and What Can Be Done About It?*” [Online]
https://perfectial.com/blog/blockchain-scalability-issue/

Adreas Ellervee, Raimundas Matulevicius, Nicolas Mayer, 2017. “*A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology”* [Online]
http://ceur-ws.org/Vol-1979/paper-09.pdf

Joseph Poon, Thaddeus Dryja, 2016. “*The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*” [Online]
https://lightning.network/lightning-network-paper.pdf

Wikipedia, Wikimedia Foundation, 2018. “*History of Banking*” [Online]
https://en.wikipedia.org/wiki/History_of_banking

Suraj Kumar, 20/12/2017. “*Merkle Tree – Introduction to Blockchain*” [Online]
https://medium.com/@skj48817/merkle-trees-introduction-to-blockchain-c80c0247046

Languasco A., Zaccagnini A., 2004. “*Introduzione alla Crittografia*”, Ulrico Hoepli Editore S.p.A. Milano