Deadline: Week 2.8

Izak Chamoun

Saxion

Assessors: Jan Jaap Sandee & Timothy Sealy



Research Document

Blockchain for the Sustainable hub app

Contents

[Introduction 2](#_Toc185944584)

[Background 2](#_Toc185944585)

[Objective 2](#_Toc185944586)

[Problem definition 2](#_Toc185944587)

[Research questions 2](#_Toc185944588)

[Analysis blockchain 3](#_Toc185944589)

[How does blockchain work? 3](#_Toc185944590)

[Consensus mechanism and security 3](#_Toc185944591)

[Application of blockchain examples in practice 4](#_Toc185944592)

[Supply chain 4](#_Toc185944593)

[Financial Service 4](#_Toc185944594)

[Healthcare 4](#_Toc185944595)

[Critical evaluation: Pro’s and con’s 5](#_Toc185944596)

[Pro’s 5](#_Toc185944597)

[*Transparency and Traceability* 5](#_Toc185944598)

[*Data Security and Immutability* 5](#_Toc185944599)

[*Decentralization* 5](#_Toc185944600)

[Con’s 5](#_Toc185944601)

[Questionable 6](#_Toc185944602)

[*Efficiency in Processes* 6](#_Toc185944603)

[Analyse Praktijkcontext 7](#_Toc185944604)

[Design of the blockchain solution 8](#_Toc185944605)

[Proof of Concept (PoC) 9](#_Toc185944606)

[Bibliography 10](#_Toc185944607)

# Introduction

This document will explain blockchain: how it works, what it can be used for, and whether it is more cost-effective than traditional data processing methods. An analysis will be conducted to determine whether blockchain is a viable solution for specific applications and whether there are any restrictions that an application must meet to fully benefit from blockchain’s advantages. These questions will be answered throughout this document.

## Background

For this Smart Solutions Semester of the Egalitarian project, the idea is to create a mobile application. Users should be able to log in, register, and donate materials to interested parties who want to collect these donations.  
This document will serve as a guideline on whether the Sustainable Hub (Egalitarian project MVP) can benefit from using blockchain. It will also act as a reference for future semesters considering blockchain implementation.

## Objective

This document will explore how blockchain technology can be applied within an application and when its use can be justified. It will provide advice while keeping the MVP of the Egalitarian project in mind, determining whether blockchain would be a valuable addition.

## Problem definition

The use of blockchain technology for data transfer within this application raises several important questions. Whether blockchain is a cost-effective solution still needs to be determined through thorough analysis and expert advice. Key factors such as energy consumption, technical complexity, and the suitability of blockchain in this specific context play a critical role. Based on the findings, it can be determined whether blockchain technology would be a valuable addition to the application's infrastructure.

## Research questions

These following question’s answers will form a solid foundation to provide an educated advice on whether blockchain improves the application or not. They will also outline how and where it would be implemented.

*How can Blockchain be integrated into the app’s infrastructure, and which type of blockchain (public, private, consortium) would be most suitable?*

*Which specific features of the app (e.g., donations, user authentication) would benefit from blockchain implementation?*

*What are the development, operational, and maintenance costs of using blockchain compared to traditional data processing methods?*

*How scalable and energy-efficient is the chosen blockchain solution, and how well does it align with the app's sustainability goals?*

# Analysis blockchain

## How does blockchain work?

The blockchain uses **blocks** that can contain certain information. These blocks are connected in a **distributed network** of similar blocks that validate each other’s existence on **validity through cryptography**. (Hayes, 2024). These tie together as a chain, hence the name blockchain. These blocks cannot be tampered with as they are **immutable**. If changes are made to a block the hash that block has that allows connection with other blocks in the network would not be accepted as it would be changed if any content has been altered.

In Ethereum’s case the blockchain utilizes Smart Contracts. Smart contracts are essentially code executed on the blockchain. These blocks that carry smart contracts adhere to the rules set by the contract. A crowdfunding campaign can be managed through a smart contract. If the fundraising goal is met, funds are released to the project owner. If not, the funds are automatically returned to contributors. (Wackerow, 2024)

**Blocks:**  
Each block contains data (such as transaction details), a unique hash, and the hash of the previous block, forming a chain-like structure.

**Distributed Network:**  
Blockchain operates on a peer-to-peer network where all nodes maintain a copy of the ledger. This decentralized system ensures that no single authority controls the blockchain.

**Validation through Cryptography:**  
Transactions are validated using cryptographic algorithms, ensuring data integrity and authenticity.

**Immutability:**  
Once data is recorded, altering it would change the block’s hash, causing the chain to break. This makes tampering virtually impossible without the consensus of the entire network.

## Consensus mechanism and security

The blockchain provides features to unsure validity of blocks entering the network. Under the hood of the consensus mechanism there are 2 relevant ways to create a transparent tamper-proof ledger. (Becher, Aug 28, 2024)

Proof of Work (PoW):

Through the workings of the Proof of Work mechanism miners can offer computational power in the form of their computer to solve complex cryptographic problems. These problems when solved correctly serve as bridge for that block to be added to the chain. The miner gains the transaction fee for solving problems and adding blocks to the chain. (Nevil, may 17, 2024)

Proof of Stake (PoS):

Through this mechanism **validators** are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and **stake**. (Investopedia-Team, June 13, 2024)

**Stake**: Locking up x amount of cryptocurrency and gaining interest in the form of that coin or another. (Usually you gain transaction fees).

**Validator**: Through validators new blocks can be added, thus completing a transaction on that network. Other validators can review and check this transaction for **fraud**. (Nevil, may 17, 2024)

**Fraud**: Validators attempting to cheat a transaction will risk losing their staked cryptocurrency. Incurring massive losses.

PoS is energy-efficient compared to PoW as it doesn’t require miners.

Proof of Authority (PoA):

This consensus mechanism relies on designed trusted validators that have the ability to validate transactions and add blocks to the blockchain. A straightforward mechanism that facilitates fast transactions speed, but does come at a cost of centralization as there are a select few that have this authority. (Adams, 2023)

## Application of blockchain examples in practice

## Supply chain

Walmart is utilizing blockchain to enhance transparency and accountability within its food supply chain. By implementing a blockchain-based traceability system, Walmart can track products from farm to shelfs of stores, ensuring food safety and quality. Primary benefit for using this technology is to identify contamination sources. This system reduces the time from days to hours or even minutes. (Sristy, Nov 30, 2021) Additionally, Transparency and avoidance of fraud are also key in earning trust from customers as the blockchain serves as a digital ledger.

## Financial Service

Everledger’s blockchain technology ensures transparency and accountability to the diamond industry. By creating a secure, immutable digital ledger, Everledger allows users to trace the origin of diamonds, ensuring authenticity and sustainability. This traceability helps combat fraud and providing consumers with trust of their purchases of diamonds. The platform also enables efficient inventory management for suppliers and facilitates data sharing with retailers, tailored to their specific compliance and sustainability needs. Retailers, in turn, can verify and communicate detailed provenance and certification information to their customers. (Everledger, 2021)

## Healthcare

IBM is planning to integrate Blockchain into the healthcare industry. It’s functionality will be in the tracking and privatization of patients information through blockchain. Information will be available to the network of healthcare providers for quick querying and seamless sharing of information. A great solution blockchain solves is the pharmaceutical supply chain. Medication can be tracked on validity. This reduces the illegal distribution of medicine. (IBM, 2024)

## Critical evaluation: Pro’s and con’s

Blockchain’s key features such as transparency, immutability and decentralization still is a massive driving force in the interest of the public masses. Many nefarious activities or mistakes (Padilla, 2024) such as losing money by mistake will not be an achievable feat anymore for anyone as transactions are neatly registered. Although I must say without proper regulation, the market of cryptocurrency lays-out a breeding ground for criminal activity such as money laundering and many other illegal acts on the blockchain (Team, 2024)

Lets outline a few pro’s and con’s to summarize simply the upsides and downsides blockchain provides.

## Pro’s

### *Transparency and Traceability*

*Blockchain creates a transparent ledger of all transactions, upholding accountability in industries like supply chain management and financial services. For example Walmart uses blockchain to trace food products to ensure quality. Additionally in the diamond industry blockchain is utilized to track diamonds from origin to sale for authenticity.*

### *Data Security and Immutability*

*Blockchains cryptographic security measures do not allow tampering of data. This safety protocol is especially useful for the healthcare industry for securing patient information to not be accessed by iniquitous actors.*

### *Decentralization*

*By operating on a peer-to-peer network, blockchain reduces reliance on central authorities, enhancing system resilience and fostering trust among participants.*

## Con’s

*Energy Consumption*

*Creating a blockchain from scratch requires significant investment in skilled developers, infrastructure, and time. Maintenance and updates will also require ongoing resources.*

*Scalability*

*Expending the system will be intensive and not in everyone’s skillset as it requires unusual knowledge of the construction of blockchain. Especially it’s unfamiliar custom design it conforms to.*

*Complexity and cost*

*Implementing blockchain solutions can be technically complex and costly, making it challenging for smaller businesses to adopt.*

*Regulatory Uncertainty*

*The legal framework surrounding blockchain technology is still evolving, creating uncertainties, particularly in financial services and healthcare.*

*Centralization*

*While private blockchains provide control and security, they can reduce decentralization, which is a key advantage of public blockchains.*

### Questionable

### *Blockchain Intermediaries*

*Blockchain removes the need for 3rd party actors within systems. Such as banks as it takes only 2 parties to complete a transaction. As this point seems valid, a recent article published stating that transactions must uphold regulation restrictions to work in alignment with jurisdictional legal requirements.* (Reiff, 2024)

# Analyse Praktijkcontext

# Context description Sustainable hub

The application has several area’s where blockchain can be integrated. Such as the user information, donations. You can make a case for either one which can make the most of blockchain’s perks. Users can be tracked and make use of the privatization and safety it provides regarding the storing behind hashes the blockchain utilizes. Although it can be regarded as overkill to use blockchain for a simple login function as it’s quite complex and intensive. Also making users keep track of their own private keys is not very user-friendly. Blockchain can better be utilized for login functions if its connected to a dApp. Tracking donations is better function to solve using blockchain as donations can be viewed on chain by users making use of a private blockchain. A custom-tailored blockchain only accessible by members. This also reduces the energy consumption as less users are dabbling around on the network. (GeeksForGeeks, 2024)

# Analysis current situation

Currently, the donation process operates through a straightforward system where users create donations through a form within the app. The details of each donation are submitted and stored in a centralized MongoDB database. Data gets transferred through the backend here HTTP request are in place to facilitate this process.

# Design of the blockchain solution

## Design

A blockchain implementation for the Sustainable Hub application is designed to provide a transparent and immutable record of donations. Each donation will be stored as a block within the blockchain, containing information such as the name of the donator, the materials, amount of material, timestamp, and the donation status. The blockchain will be implemented as a private network to balance transparency and efficiency while keeping energy consumption minimal. Smart contracts will automate processes, such as recording donations and updating their statuses, this will automate the process of changing states of the donation from either pending of being picked up or if it’s already picked up.

To conform to the size of the block only keys of the accessible information will be stored on-chain. The rest will be off-chain meaning it will be in a centralized database.

## System architecture

### *Frontend layer*

*Application build on React Native. Allow users to create donations through a form. Various details about the donation will be submitted like amounts and types of material, a description, and images. A hash will be given to the user to reference the block that was created for querying.*

### *Blockchain layer*

*A private blockchain network that stores the donation immutably. Blocks contain data fields. This data in the block will be hashed using cryptographic algorithm (SHA-256). This hash will act as identifier for this block and previous blocks in that chain.*

*Data stored:*

*Block data, Block hash, Previous block hash*

### *Off-chain layer*

*Unsensitive data will be stored here regarding the users and additional data which do not require on-chain protection that the blockchain provides.*

### *Interaction layer*

Ether.js will be installed to facilitate interaction between React Native frontend and the blockchain network.

## Used technology and tools

### *Blockchain Network*

*JavaScript would be used to create the blockchain network.*

### *Smart Contract*

*Programming language: Solidity*

### *Blockchain Integration*

*Ether.js*

### *Development tools*

*Ganache tool used to test and compile smart contracts*

### *Off-chain storage*

*MongoDB*

## Considerations

Questioning whether blockchain technology should be implemented into an application needs careful consideration as it needs specific requirements to make use of the blockchain’s beneficial properties.

Is data integrity of donations worth protecting behind hashed blocks? Donations can be replaced with x functionality of any application. An application requires specific needs to actually utilize this powerful technology for the right reasons or it will only slow down and overcomplicate a simple process. Integrating a hybrid approach with on-chain and off-chain sections of blockchain can be feasible approach when using it for the right reasons, but does it weigh off against the increased complexity of creating a custom private PoA-based blockchain.

A different consideration is to use the open-source Hyperledger fabric. This 3rd party software that provides participants to define a custom blockchain workflow that has plug and play properties with storage support from known databases like MongoDB or levelDB. Many similar projects are constructed within this ecosystem. (Projects, sd)

# Proof of Concept (PoC)

Development of the PoC

Implementation details

Evaluation

Challenges and learning points

# Bibliography

Adams, J. (2023, August 11). *What Are the Different Types of Consensus Mechanisms in Blockchain?* From doubloin.com: https://www.doubloin.com/learn/blockchain-consensus-mechanism

Becher, B. (Aug 28, 2024). *What Is a Consensus Mechanism?* https://builtin.com/blockchain/consensus-mechanism#:~:text=Consensus%20Mechanism%20Definition,each%20blockchain%20transaction%20gets%20approved.

Everledger. (2021). *Diamonds*. From https://everledger.io: https://everledger.io/industry-solutions/diamonds/

GeeksForGeeks. (2024, October 17). *An introduction to Private Blockchain*. From Geeksforgeeks.org: https://www.geeksforgeeks.org/private-blockchain/

Hayes, A. (2024). *Blockchain Facts: What is it, How it works, and how it can be used.* https://www.investopedia.com/terms/b/blockchain.asp.

IBM. (2024). *Healthcare technology solutions and services*. From IBM.com: https://www.ibm.com/industries/healthcare

Investopedia-Team. (June 13, 2024). *What Does Proof-of-Stake (PoS) Mean in Crypto?* https://www.investopedia.com/terms/p/proof-stake-pos.asp.

Nevil, S. (may 17, 2024). *What Is Proof of Work (PoW) in Blockchain?* https://www.investopedia.com/terms/p/proof-work.asp.

Padilla, H. (2024, March 26). *Federal Government Made $236 billion “Improper Payments” Last Fiscal Year*. From gao.gov: https://www.gao.gov/blog/federal-government-made-236-billion-improper-payments-last-fiscal-year

Projects, H. (n.d.). *Hyperledger Fabric*. From lfdecentralizedtrust: https://www.lfdecentralizedtrust.org/projects/fabric

Reiff, N. (2024, October 26). *Blockchain Won't Cut Out Intermediaries After All*. From Investopedia.com: https://www.investopedia.com/tech/blockchain-wont-cut-out-intermediaries-after-all/

Sristy, A. (Nov 30, 2021). *Blockchain in the food supply chain - What does the future look like?* https://tech.walmart.com/content/walmart-global-tech/en\_us/blog/post/blockchain-in-the-food-supply-chain.html.

Team, C. (2024, February 15). *Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group*. From chainanalysis.com: https://www.chainalysis.com/blog/2024-crypto-money-laundering/#:~:text=The%20goal%20of%20money%20laundering,where%20the%20funds%20came%20from.

Wackerow. (2024). *INTRODUCTION TO SMART CONTRACTS.* https://ethereum.org/en/developers/docs/smart-contracts/.