TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Marje Salumets 204805IVCM

Threat Modeling of the Supplain.io Blockchain Protocol: Preserving Data Trust, Privacy and Security in Physical Supply Chains

Master's thesis

Supervisor: Kaido Kikkas, PhD
Expert in field: Ats Onemar, CISA

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Marje Salumets 204805IVCM

Supplain.io plokiahela protokolli ohumudeli koostamine: säilitamaks andmete usaldusväärsus, privaatsus ja turvalisus füüsilistes tarneahelates

Magistritöö

Juhendaja: Kaido Kikkas, PhD
Praktiline juhendaja: Ats Onemar, CISA

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Marje Salumets

25.03.2022

Abstract

Today, many companies are trying to solve the problem of data sharing for physical supply chains. Due to supply chains being long and complex, often examples occur where end-users are not fully aware of how and by whom their data is processed. Many companies believe that including blockchain technologies to speed up the flow of information in supply chains, while maintaining the reliability, privacy, and security of data exchange, resolves this problem.

The blockchain is certainly the correct solution and future technology helping the logistics sector achieve the desired goal of being able monitoring parcel movement at any stage and securely transmit data throughout the supply chain without seeing extensive information while validating end-users' identities. Parcel services is just one example of how the blockchain can be used and there are surely many others, but in current work, an example process of sending a package from E-shop to customer is used with the supporting process of how to maintain the dependent infrastructure.

Popular technologies, such as Bitcoin and Ethereum, are certainly able to solve the problem in supply chains but due to consensus mechanisms in use, both are not able to exchange data quickly neither securely. Proof of work (POW) technology eliminates known vulnerabilities enabling the security attacks such as Denial of Service (DDoS) or Man in the Middle (MitM) to happen as recognized in today's traditional centrally managed systems, but at the same time being vulnerable to other known attack vectors such as 51% and Sybil attack.

This work will look closer at Nominated Proof of Stake (nPOS) consensus technology and how it is used in Polkadot. This is an open source technology and can be customized for different use cases. A small start-up company Supplain.io tries to solve the data transfer problem in supply chains with Polkadot-based blockchain technology guaranteeing trust, security, and privacy. The protocol created by Supplain is still in the design phase but mature enough to assess whether the service meets required security needs and would not be vulnerable to attack vectors applied to blockchains known today.

To determine the possible attack vectors a theoretical Threat Modeling method is used. If there are findings of applicable threats to Supplain service, an assessment based on ISO27005 Information Security Risk Management standard will be conducted and presented along with mitigation proposals.

This thesis is written in English and is 78 pages long, including 7 chapters, 3 figures and 5 tables.

Annotatsioon

Supplain.io plokiahela protokolli ohumudeli koostamine: säilitamaks andmete usaldusväärsus, privaatsus ja turvalisus füüsilistes tarneahelates

Tänasel päeval üritavad paljud ettevõtted lahendada füüsiliste tarneahelate jaoks andmete jagamise probleemi. Kuna tarneahelad on pikad ja keerulised, siis tihti peale leiab näiteid, kus lõppkasutajad ei ole täielikult teadlikud, kuidas ja kelle poolt nende andmeid töödeldakse. Selleks, et info liikumine tarneahelas kiiremaks muuta, samal ajal säilitades andmete usaldusväärsus, privaatsus ning turvalisus, on paljud ettevõtted liikunud suunal siduda füüsiliste tarneahelate andmevahetus plokiahela funktsionaalsusega.

Plokiahel on kindlasti see viis ja tuleviku tehnoloogia, mis aitab ettevõtted soovitud eesmärgini, kus on igas etapis võimalik tuvastada logistiliselt paki liikumine ja terve tarneahela ulatuses andmeid turvaliselt edastada ilma, et seotud osapooled näeksid liigset infot ja valideerides lõpp osapoolte identiteedi. Pakkide saatmine on kõigest üks näide, kuidas plokiahel saab kasulik olla, neid kasutusjuhte on mitmeid, kuid käesolevas töös kasutamine näitena just paki saatmiste protsessi ning selle eesmärgi täitmiseks vajamineva inventari hooldusprotsessi.

Tänapäeval populaarsed tehnoloogiad, nagu Bitcoin ja Ethereum, on kindlasti võimelised tarneahelaid oma probleemi lahendamise juures aitama, kuid tänu oma konsensuse mehhanismile ei ole võimelised tagama kiiret ega ka turvalist andmete vahetust. Proof of work (POW) ehk töö baasil tagatav konsensus tehnoloogia elimineerib küll tänases tavapärases keskselt hallatavas juhtimissüsteemides tuntud turvalisust ohustavad ründevektorid nagu Distributed Denial of Service (DDoS) ehk teenusetõkestusrünnak või Man-In-The-Middle (MitM) ehk vahendusrünne, kuid samal ajal on see tehnoloogia haavatav plokiahelas vastu tuntud ründevektoritele nagu 51% ja Sybil rünnakud.

Käesolevas töö näitab, kuidas Polkadot on oma plokiahela konsensuse mehhanismi loonud hoopis Nominated Proof of Stake(nPOS) ehk nomineeritud panuse põhise valideerimise tehnoloogiale ning kuidas väike start-up ettevõte Supplain.io lahendab tarneahelates andmete edastamise probleemi Polkadotil baseeruva plokiahela tehnoloogiaga, mis garanteerib andmete usalduse, turvalisuse ja privaatsuse tarneahela täies ulatuses. Supplaini poolt loodav protokoll on veel toote disainimise faasis, mis tõttu on praeguses faasis vajalik hinnata, kas teenus vastab eesmärgistatud turvalisuse nõuetele ning ei oleks haavatav täna teadaolevatele tuntud plokiahelatele kohalduvatele ründevektoritele. Selle väljaselgitamiseks on võimalik kasutada ohtude modelleerimise tehnikat, mis võimaldab kaardistada võimalikud teoreetilised ründevektorid. Juhul, kui selle käigus tuvastatakse Supplaini tootele mõju omavad ohud, siis hinnatakse need vastavalt ISO27005 inforturvariski halduse standardile ning esitatakse koos leevendavate meetmetega.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 78 leheküljel, 7 peatükki, 3 joonist, 5 tabelit.

List of abbreviations and terms

51% attack	51% is an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power
BABE	Blind Assignment for Blockchain Extension, proof-of-stake protocol
Bitcoin	Decentralized digital currency
Blockchain	A shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network
Consensus mechanisms	A fault-tolerant mechanism that is used in computer and blockchain system
DFD	Data Flow Diagram
DDoS	Distributed Denial of Service attack
DIDs	Decentralised Identifiers
Digital Twin	A digital twin is a virtual representation that serves as the real-time digital counterpart of a physical object or process
DNS Spoofing	Attack against Domain Name System
DOT	Polkadot cryptocurrency
Ethereum	Decentralized digital currency
Full node	A program that fully validates transactions and blocks
GRANDPA	GHOST-based Recursive Ancestor Deriving Prefix Agreement, the block finality protocol in Polkadot
ISO27005	ISO/IEC 27005:2018 Infromation Security Risk Management standard
MitM	Man in The Middle Attack, enables for the unauthorized third party to steal data

nPOS	Nominated Proof of Stake
Parachain	An application-specific data structure that is globally coherent and validatable by the validators of the Relay Chain.
PASTA	The Process for Attack Simulation and Threat Analysis
Polkadot	A network protocol that allows arbitrary data to be transferred across blockchains
POW	Proof of work technology
POS	Proof-of-Stake mechanism
STRIDE	Threat modeling framework and acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Escalation of privileges
SCM	Supply Chain Management
Sybil Attack	Attack against decentralized systems
Token	Coin like objects used instead of coins in cryptocurrencies
TMM	Treat Modeling Method
TTP	Tool, Techniques, Procedures
W3C	World Wide Web Consortium

Table of contents

List of figures

List of tables

1 Introduction

The rapid development of technology and the fast-growing need for different services is showing its relevance in supply chains. Happy customer requires seamless collaboration and coordination across multiple stakeholders. No matter what your business type is or what kind of products is wished to sell, a well-organized, reliable, trusted supply chain is a crucial factor. The challenge of keeping the data confidentiality, integrity and availability has never been greater due to huge growth of business industries and long freight distances which involves many stakeholders like logistics companies, customs, law regulations, middlemen (traders), producers, banks, retailers etc. [1] Any disruption in supply chains could turn out costly to companies due to loss of time, money, and trust. Not to add the factor that keeping the data accurate and up to date adds another level of complexity. [1]

At the moment many enterprises are seeking transparent, resilient, and agile solutions that complies with the functionality of different systems, is scalable and enables fast communication providing confidentiality, integrity and availability of data while preserving privacy. The contribution of a large number of stakeholders makes the whole communication chain more complex. It is not possible to manage shared data among all suppliers centrally since the parties are standalone companies who have their own private systems, business secrets and tailored technology in use with different confidentiality and availability need. Many systems are not compliant with each other, and the traffic is not possible to unite. All that makes it very hard to find any solution to manage it centrally which brings us to decentralized methods like Blockchain. The potential of blockchain applications in Supply Chain Management (SCM) is high. The technology can facilitate the main targets of cost, transparency, security, trust, speed, dependability, risk reduction, sustainability, and flexibility. [2] Every year the attack methods against supply chain are turning out to be more intelligent, harder to discover and the number of attacks is increasing. It is well noted by the literature that the ability to identify and assess risks decreases as soon as the product or service leaves the organizations' premises or responsibility domain [3]. Including the Blockchain technology to assure integrity of end-to-end communication between different parties is hoped to make the interaction of supply chain members more secure.

Blockchain is not the easiest solution since the popular products at the moment like Bitcoin and Ethereum are slow and complex. [4] In a blockchain system data is stored within a digital ledger in batches named as “blocks”. [4] All information added or changed will be time-stamped to verify its authenticity and all blocks will be tied to chronological order. Every entity is encrypted and linked to a preceding block. This makes altering any data impossible without changing the whole chain of blocks which makes the system secure. Strict sequence of stored data enables for everyone to see the full change history, preventing anything changed or removed without the awareness and consent of all systems in the network. [5]

Supplain.io began with a vision of a world where every organisation can connect with their partners right here and now without relying on centralised third parties that expose them to potential risks. Supplain is a blockchain framework with security, privacy, and performance standards required to accelerate the mass adoption of this technology and support a lasting ecosystem. It is not yet “another blockchain application” but a protocol that facilitates leading-edge technologies, models, and methodologies to help developers, enterprises, and individuals connect their data and access powerful tools. Supplain will begin as a fork of Polkadot. [6] Polkadot is a true multi-chain application environment that mixes the concepts for public and private blockchains differently from the previous hybrid or consortium blockchains. As a result, Supplain aims to create a privacy-preserving yet interoperable framework that would standardise the method of data exchange and enable autonomous business execution across any supply chain. The entire industry becomes more connected, simplified, yet significantly more powerful. [6]

The blockchain technology is proven to be more secure [7] than centrally managed systems by mitigating many known attack vectors like DNS spoofing, Ddos and ManInTheMiddle (MITM) attack by design but at the same time creating new blockchain oriented attacks like 51%. Besides technical vulnerabilities and security flaws blockchain technology is not resilient to the non-technical risks like human error, intentional and unintentional mistakes, and external factors such coming from the environment, like the legal regulations and the location. [8] The Supplain framework is in the design phase, at this point it is possible to change every aspect before starting the real production or development of the code. Changes made in the design phase are not that costly or time consuming than later in the development phase. Plus, the design phase is a correct point to involve cyber security personnel to evaluate and measure the risks that might somehow have the impact on the product.

This research will be theoretical, and the outcome will give answers for the Supplain.io stakeholders if desired high-level security and privacy preserving goals are met. Threat model, based on STRIDE and PASTA methods [9], will demonstrate how applicable attack vectors may have impact on the Supplain framework and what may be the possible consequences. All threats will be evaluated according to ISO27005 Risk Matrix [10] to calculate possible prioritized value and risks evaluated as critical or high a risk mitigation plan will be proposed with possible countermeasures. The result will show if the promised high-level security and privacy preserving goal is met or not. In case the result meets the desired level of Security and Privacy requirements presented in Appendix 2, it gives assurance for the Supplain team to proceed with product development as planned, but in case of negative result or major non-conformities the team still can make changes in design of the framework without wasting any extra time or money.

1.1 Problem Statement and research questions

The blockchain technology is proven to be more secure [7] than centrally managed systems by mitigating many known attack vectors but at the same time creating new blockchain oriented attacks. Besides technical vulnerabilities and security flaws blockchain technology is not resilient to the non-technical risks like human error or external factors such coming from the environment (ex. Regulation). [8] The blockchain technology may natively provide the maximum-security capability, but if it is not configured properly or implemented with flaws, then the desired level of security is not achieved. Supplain.io is solving the data trust, integrity and privacy preserving problem for end-users across the whole supply chain using blockchain technology. [6] The goal is to achieve complete data trust and meet the desired security and privacy requirements they have defined for the Supplain framework. List of requirements is presented in Appendix 2 – Security and Privacy Requirements. To evaluate if the security requirements meet the design of the framework in this paper two use cases will be evaluated to understand how security and privacy controls are implemented in the Supplain.io protocol and analyse how and by whom Supplain.io protocol can be compromised or misused.

This research will be theoretical and determine the possible attack points, applicable threats, and an overview of human errors by using Threat Modeling methodology and the goal is to define and avoid threats evaluated as "high" and "critical" that may lead to service disruptions, data breach or any other way Supplain may experience the reputation damage or financial loss.

The result of the research will:

- Provide an overview of applicable threats.
- Prove conformity with privacy and security requirements.
- Helps to develop an action plan to mitigate critical and high risks.

In case of positive outcome of the research the threat model will demonstrate weak security areas, where the malicious actor can be involved and indicators where security measures need to be considered or hardened. Supplain.io will consider these findings and can eliminate those before production. In case of negative results (the end-to-end communication turns out to be secure all the way), then it is a proof of concept for using secure blockchain protocol to assure trust in supply chains.

1.2 Scope

The scope of the thesis will describe the details of the research area and explain the limitations.

Supplain.io is created to achieve trusted communication between stakeholders in the physical supply chains. The research will define and evaluate any applicable threats or technical attack vectors, that somehow might compromise the integrity of the Supplain.io service. Supplain will begin as a fork of Polkadot that mixes the concepts for public and private blockchains differently from the previous hybrid or consortium blockchains. Unlike Polkadot, which primarily focuses on providing consensus and pooled security for public chains, Supplain seeks to adopt the same model for private chains. In essence, private parachains are identical to public parachains except that private parachain authorities will act as Collators and Fishers for their own private parachain and members need to be willing to publicise their dispute details. [6] In the future Supplain.io is planning to provide pooled security and consensus for both private and public parachains, but this work concentrates only to applicable threats applicable for Supplain's private parachains and only parts of Polkadot, that apply to Supplain service and will not evaluate the whole Polkadot blockchain technology.

1.3 Ethical Issues

Ethical issues section confirms the will of the Supplain.io team to participate in this research and declares limitations and expectations from their side.

Supplain.io is very happy to be part of the project and they have no limitation of sharing this information publicly. All information used in this paper is originally shared among all interested stakeholders in the Supplain.io white paper via their homepage. This research work will be used as initial security analysis to avoid major design flaws and as assurance the required high-level security and privacy preserving functionality will be achieved.

1.4 Related work

The topic of assuring the trust using blockchain technologies for communication in supply chain is quite new. [11] There are a lot of studies released between 2018-2022 that bring out the benefits of using blockchain technology in the scope of physical supply chain management. There is no doubt that the decentralized method for having more control over supply chains is the correct approach and many possible security risks and human errors are being mitigated by using this technology. [12]
The research done by Esteban Ramirez "Preserving Information's Integrity and Confidentiality with Blockchain in the service in Supply Chain" [3] shows that blockchain, like any other piece of technology in the world, is vulnerable to cyberattacks. The vulnerabilities depend on the type of blockchain, the consensus method used and the underlying technological platform. Public blockchains (mostly cryptocurrencies) are less secure than private blockchains, the difference is the limited and restricted access that the latter have. [3] As mentioned by Mr. Ramirez in a proposal for further studies, the link between supply chain and blockchain needs to be

established. The Supplain Team has brought us closer to solving the trust problem in supply chains and the Supplain framework gives the possibility to continue his research by bringing it to the next level and providing more detailed analysis of the concept. The risk management and risk registry shown in his research is also applicable for the current thesis, but due to the design of Supplain.io lets us dig deeper therefore using more complex attack vectors designed for blockchains can be evaluated. Therefore, Threat Model analysis is essential to identify potential vulnerabilities (unutilized weakness), threats (activated weaknesses), and risks (the effect of threat) that the model will impose. Additionally, it will help in identifying mitigation and protection mechanisms. [2]

While Esteban Ramirez concentrates more on technical risk, the initial information provided for the Supplain.io is done by a real person and therefore the importance of human error is significant. The thesis conducted by Teelika Šutov "Reckoning Supply Chain Human Errors in Blockchain Technology Development" shows the possible human interventions. [8] As a result of the research on human error in the supply chain the author concluded that the effect of human error is important within the application of blockchain technology in the supply chain, as it is inevitable in processes. Human error can be unintentional or intentional, and both types of human errors can affect the automatic processes in the supply chain and blockchain. As a result of these errors, unchanged false data is transmitted throughout the chain when queries and databases communicate while triggering automated processes in the digital communication chain.[8]

The implementation of blockchain techniques in the logistics and transportation field is highly expected presuming it will mitigate trust issues and security risks. [12] While it is proven to mitigate risks known in todays' centralized management of Supplay chains, then it does not mean it will not bring along new attack vectors designed explicitly to blockchains.[13] In 2019 Mubashar Iqbal and Raimundas Matulevicius from University of Tartu conducted research "Blockchain-based Application Security Risks: A Systematic Literature Review" where at first it is explained what security risks of centralized applications are mitigated by introducing blockchain-based applications and secondly is reported what are the security risks of the blockchain-based applications which appear after introducing the blockchain technology. [13] The result will give a preliminary checklist presenting the possible risks while implementing blockchain based applications on Bitcoin, Hyperledger or Ethereum. Since the Polkadot’s Parachain solution is advanced technology of Ethereum, like it is described in current Thesis 2.1 Polkadot’s Parachain chapter, then the same risks defined will apply for Proof- of-Stake consensus mechanism and Smart Contracts. All applicable risks are used as input for Threat Catalogue.

The research team of M.Iqbal and R. Matulevicius have released another study about blockchain based applications risks in 2019 “Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk”. [14] The researchers compare Ethereum and Hyperledger architecture to mitigate data tampering risk in the healthcare application with ISSMR Domain Model. The work is limited only to data tampering risk assessment although it can be used for evaluating other attack vectors like Ddos or MITM. Researchers are using a risk-based threat Modeling approach, but at this current stage of Supplain.io framework system-based threat Modeling is justified and for that reason in current work a hybrid combination of STRIDE and PASTA methods have been chosen. The research goal is the same as described by M.Iqbal and R. Matulevicius – results of the study could be considered when evaluating the software design to produce secure software. [14]

For the future work the authors propose to build a comprehensive reference model for security risk management to systematically evaluate the security needs. This model would explain the protected assets of the blockchain-based applications, and countermeasures to mitigate their risks.[14] The service developed by Supplain.io will provide the opportunity to analyse in more detailed way what kind of threats may become cybersecurity risks, but since the framework in current phase is not mature enough to make conclusive decisions applicable for different use-cases built on Polkadot Parachains, then current work cannot be used as comprehensive reference model but more like an useful input for future development.

2 Background

The technology used while implementing blockchain on top of business services is very complex and high cost. Even trials for 3 months cost more than 100 000€. [3] Not to mention the challenge how to configure many different solutions communicate with each other and at the same time doing it fast without the possibility of data loss or fraud. [1] Supplain.io is developing a framework that will make access to blockchain technology for all the stakeholders much easier and affordable. Since many principles are adopted from Polkadot blockchain it is needed to understand how Polkadot works and what are the main components to provide the functionality of the Supplain’s Relay Chain.

2.1 Polkadot Parachain

The major advancement for Supplain blockchain originates from significant improvements required for a privacy-preserving, regulatorily compliant solution suitable for handling sensitive personal and business information. To achieve this, Supplain will be built on a blockchain-based solution primarily derived from Polkadot's concept of parachains - multiple interoperable yet independent blockchains pooling their resources for security and consensus. [6]

2.1.1 Relay Chain

Polkadot is a scalable heterogeneous multi-chain.[15] Concept of the multi-chain is demonstrated on Figure 1 (page 25). Unlike previous blockchain implementations which have focused on providing a single chain of varying degrees of generality over potential applications, Polkadot itself is designed to provide no inherent application functionality at all. Rather, Polkadot provides the bedrock “relay-chain” upon which a large number of validated, globally coherent dynamic data-structures may be hosted side-by-side. These data-structures are called “parallelised” chains or parachains. [16] Polkadot may be considered equivalent to a set of independent chains (e.g., the set containing Ethereum, Ethereum Classic, Namecoin and Bitcoin) except for two very important points [17]:

- Pooled security.
- trust-free interchain transactability.

These points are why Polkadot is considered to be “scalable”. [17]

Polkadot provides a rather bare-bones piece of infrastructure leaving much of the complexity to be addressed at the middleware level. This is a conscious decision intended to reduce development risk, enabling the requisite software to be developed within a short time span and with a good level of confidence over its security and robustness. [6] [17] The Sudo module [15] was removed by a runtime upgrade on July 20, 2020, transitioning the governance of the chain into the hands of the token (DOT) holders. From this point, the network has been entirely in the hands of the token holders and is no longer under control of any centralized authority. [15]

While some similarities are shared with Ethereum 2.0[19], one key differentiator is that it uses heterogeneous sharding. Each parachains can be customised through the Substrate development framework, enabling the optimization for a specific use case, and running in parallel rather than crossing all the shards. This is important in blockchain architecture - one size does not fit all and all blockchains make trade-offs to support different features and use cases. [19] [20]

All parachains connect to the relay chain, which validates the state transition of connected parachains, providing shared state across the entire ecosystem. If the Relay Chain must revert for any reason, then all of the parachains would also revert. [19] Ensuring the validity of the entire system can persist, and no individual part is corruptible. [20] Interoperability is also possible to other ecosystems through bridges, which are specifically designed parachains to interact with another ecosystem such as Ethereum, Bitcoin and Cosmos.

2.1.2 Shared Security

The shared state ensures that the trust assumptions when using Polkadot parachains are only those of the Relay Chain validator set and no other. [15] The Relay Chain is responsible for the network’s shared security, consensus and cross-chain interoperability. It is secured by Validators and Nominators staking the native DOT tokens (Polkadot’s cryptocurrency). Collators are selected by each parachain to produce the next block for the parachain. [19] Demostrated later on on Figure 2 (page 28) as part of the concept of Supplain model.

2.1.3 Collators

Collators maintain a “full-node” for a particular parachain; meaning they retain all necessary information to be able to author new blocks and execute transactions.[15] Under normal circumstances, they will collate and execute transactions to create an unsealed block and provide it, together with a proof of state transition, to one or more validators responsible for proposing a parachain block. [16]

Collators will also watch the progress of block-producing and consensus protocols in BABE and build on what they think is the latest relay chain block that will be finalised. Collators do not directly participate in the consensus for the relay chain and therefore never stake DOT. [16] The Blind Assignment for Blockchain Extension (BABE) assigns validators randomly to block production slots using the randomness generated with blocks. [15] The validator will prove that it assigned to the slot and create a relay chain block which includes the candidate recipients from the various parachains.[16]

2.1.4 Validators

Validators secure the Relay Chain by staking DOT, validating proofs from collators and participating in consensus with other validators. These participants will play a crucial role in adding new blocks to the Relay Chain and, by extension, to all parachains. This allows parties to complete cross-chain transactions via the Relay Chain. [15]

The number of parachains is determined by the number of validators on the relay chain. A small number of validators are randomly assigned to each parachain and rotate within a given time interval. The hope is to reach 1000 validators, which would enable around 100 parachains. With each parachain being capable of around 1,000 transactions per second. Ultimately scalability for the ecosystem is determined by how scalable the relay chain can be. [19]

Validators perform two functions. First, verifying that the information contained in an assigned set of parachain blocks is valid (such as the identities of the transacting parties and the subject matter of the contract). Their second role is to participate in the consensus mechanism to produce the Relay Chain blocks based on validity statements from other validators. [20]

Any instances of non-compliance with the consensus algorithms result in punishment by removal of some or all of the validator's staked DOT, thereby discouraging bad actors. Good performance, however, will be rewarded, with validators receiving block rewards (including transaction fees) in the form of DOT in exchange for their activities. [20]

2.1.5 Nominators

A nominator is a stake-holding party who contributes to the security bond of a validator. [15] Nominators stake their DOT tokens with validators they trust, with the validators likely charging a small commission to cover running costs. If a validator is found to have performed misconduct a percentage of their stake but also the nominators stake will be slashed depending upon the severity. [19] Both the validators own stake and the nominated stake will be slashed, so it is possible to lose all DOT staked against a validator if they perform maliciously. It is very important not to just try and maximise rewards and being oblivious to the risk, not only to lose all DOT-s, but making the entire system less secure. There have already been several minor slashing incidents so far, so something to really consider.[20]

Nominators have no additional role except to place risk capital to signal that they trust a particular validator (or set) to act responsibly in their maintenance of the network. They receive an increase (or reduction) of DOT-s in their deposit according to the bond's growth to which they contribute. [21]

2.1.6 Fishermen

Fishermen are not directly related to the block authoring process. Rather they are independent "bounty hunters" motivated by a large one-off reward. Fishermen are checking proposed blocks in every part of the network.[15] If they find a compromised block, then the creator of the block gets slashed, and the fisherman receives a portion of this slashed stake as reward. Fishermen are particularly important when a group of validators colluding and proposing a compromised parachain block. Fishermen are required to stake a small amount of DOT to prevent sybil attacks from wasting validators' time and compute resources. [15]

2.1.7 How Consensus works

The number of validators in the relay chain is determined by governance, currently it is 197 validators with the hope to extend this to 1,000. [15] After a certain period of time, referred to as an era, which is currently every 24 hours, an election is held to determine who gets to be a validator using Nominated Proof of Stake (NPoS). [15] Nominators stake their funds against validators they trust and the reward scheme and selection method are designed to have each validator backed by a similar amount of stake.

As the total number of validators is limited that can participate in consensus for performance reasons, a small amount is randomly assigned to validate each parachain. When the validator receives the unsealed block and proof of validity from the collator, it will check if the block follows state transition rules of the parachain. A parachain's state is stored in a Merkle tree. [15] If some value changes, one can verify the change by only looking at the new values and the paths in the tree that it affects. Based on this property, a validator can verify a state transition without having access to the entire state.[17] Please look at Figure 1where is demonstrated the whole Polkadot's consensus mechanism.

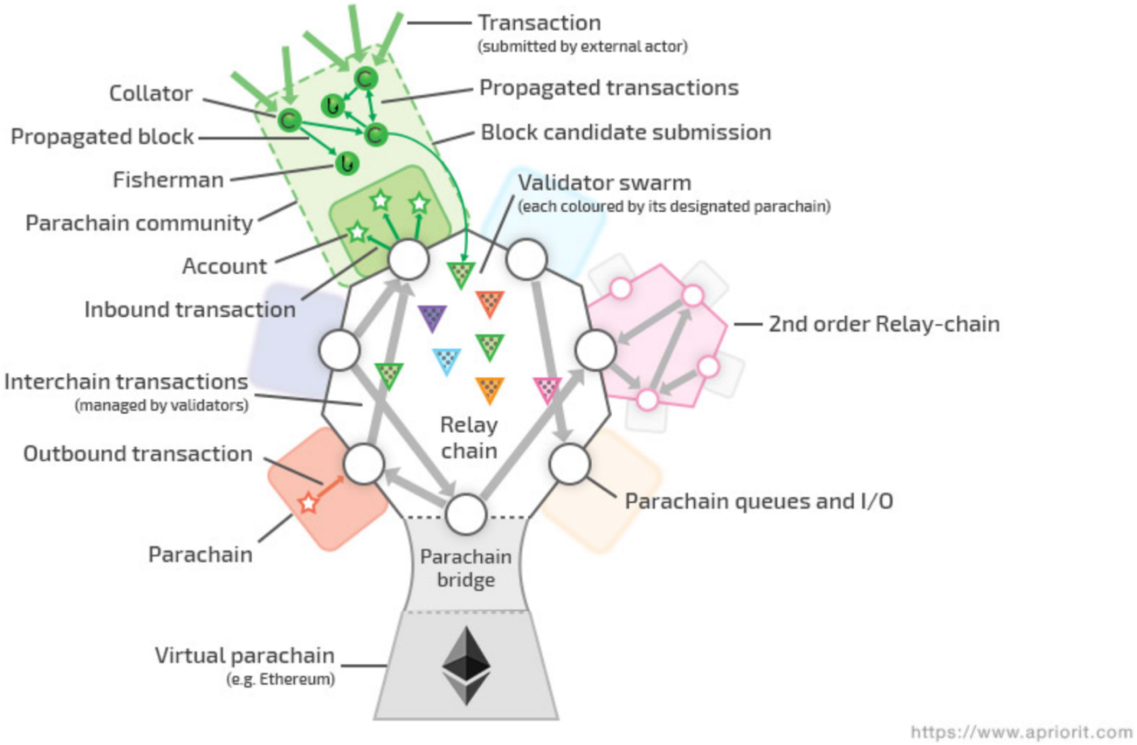


Figure 1: Concept of Polkadot. [18]

At this point there are no guarantees that anyone other than the collator and parachain validators have seen the proof of validity block. If these collude, then the rest of the parachain network need not have the parachain block and then most collators cannot build a new block and this block's invalidity may not be discovered. Rather than send the proof of validity block to every validator in the relay chain (hoping to achieve 1000 validators) instead erasure coding is used for performance reasons. [16]

GRANDPA is the finality gadget that is implemented for the Polkadot Relay Chain and works to agree on a chain, out of many possible forks, by following some simpler fork choice rule. [17] Rather than voting on every block, instead it reaches agreements on chains. As soon as more than 2/3 of validators attest to a chain containing a certain block, all blocks leading up to that one are finalized at once. [16]

Erasure coding takes the parachain block and proof of validity and creates a set of smaller messages which can be reconstructed to the original message.[17] The number of smaller messages is equal to the total number of validators and the fraction required to reconstruct the message is one-third. In addition, it also sends the candidate recipient to every validator so that it will be included in the Relay Chain transaction queue. This process happens for each parachain simultaneously. [15] All of the availability and validity checks should take place in less than one minute from the time a block is authored to the time it is finalized. [17] Once final, the block benefits from the shared security environment that allows chains to interact with each other in a trustless manner. If an invalid block is detected after it has been finalised then the relay chain would need to be reverted along with every parachain. This is particularly important when connecting to external blockchains as those don't share the state of the relay chain and thus can't be rolled back. [17]

2.2 Supplain relay chain

Supplain.io is a startup company, which is developing a secure protocol which will enable an end-to-end secure communication channel through the blockchain technology to guarantee the truthfulness and transparency in supply chains. [6] For example: Customer makes an order from a random web shop. The E-commerce provider forwards the package info and delivery data to Omniva. Both turn to the Supplain.io Relay Chain, where they will receive secure keys to start their communication through the blockchain. Supplain is distributed, privacy preserving standalone blockchain focused on staying thoroughly permissionless or has exchanged transparency for access control. [6]

In the previous chapter the Polkadot Relay Chain model is covered in detail and that's why in this chapter the focus is only on the specific value and differences that Supplain will produce. The core description will give the description of the protocol, but the final, production ready, version may change in time according to the market's requirements, external factors such as regulations and the final level of security controls desired.
The primary difference in Supplain's model is that the involved parties can create both public and private parallel sub-chains (or parachains).
For Supplain model two fundamental concepts will be included:

- Digital Twin - as a new form of the digital ledger for record-keeping and data exchange.
- W3C Decentralised Identifiers (DIDs)- for handling key management, delegation, and other identity-related concerns.

These technologies make it possible to introduce lasting yet replenishable records that can be duplicated, customised, and simply transferred, with the possibility to control which parties can read the specific data.

Supplain will provide no inherent application functionality by itself. It will provide a "bare-bones" piece of infrastructure, allowing decentralised application developers more freedom to build on the protocol while minimising predefined restrictions. This is a deliberate decision intended to reduce development risk, allowing the software to be developed within a short time and with confidence in its security and reliability. [6]
There is an opportunity for Supplain to be interoperable with most other networks in a similar manner to Ethereum. [13] In short, validators sign Supplain's transactions and feed those to other networks by a transaction-forwarding contract or in another way, the usage of specially formatted logs coming from a "break-out contract" to allow a swift verification that a specific message should be forwarded. [6]

2.2.1 Roles

Supplain intends to implement the same four fundamental roles for network upkeep as Polkadot: validator, nominator, collator, and fishers.

However, the fishers' role may only be required for public parachains, given that in private parachains, the outside parties cannot monitor all transactions in real-time. Other roles are defined the same, as in Polkadot [15], except for Collators. In the case of Supplain's private parachains, the majority (but possibly all), private parachain participants will become collators for their chains. Since all data within private parachains will remain secret, outside parties cannot fulfil this role. [6]

2.2.2 Consensus

The premier example of a consensus mechanism for multiple cooperating blockchains is Polkadot's parachains. In this model, disparate application-specific parallel sub-chains (or parachains), each with their own block production, become clients for the main Relay Chain, providing immutability, timestamping, and cross-chain services. This enables smaller chains with fewer participants to pool their security together, with built-in cross-chain capabilities. [17]

Supplain will be designed as a fully open and public network that could operate without any organisation or trusted authority. Therefore, a Proof-of-Stake mechanism [16] will be utilized to determine the network's validators and their incentive systems. The private parachain authorities will also act as collators and fishers for their own private parachains, but the final consensus would still be delegated to the main Relay Chains' validators. [6] On Figure 2 it is presented how the roles act in terms of private parachain.

Supplain leaves it to parachain protocols to specify their own means of spam prevention and does not impose a transaction fee by itself. [6]

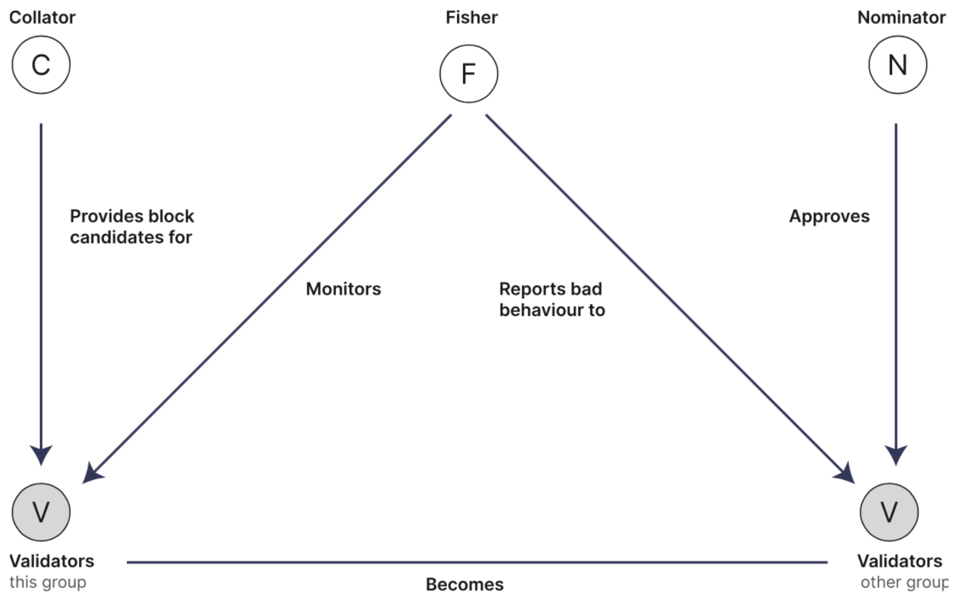


Figure 2: Supplain roles. [6]

Supplain will introduce its own token to measure how much “stake” any account has. These tokens will be used to elect the validators through a Nominated Proof-of-Stake (NPoS) scheme.[16] Similar to Polkadot, Supplain's validators will be bonded heavily by their stakes, with bonds remaining in place long after their duties cease (up to three months). This allows future misbehaviour to be punished until the chain's periodic checkpointing.[6]

Like Polkadot, Supplain is a multi-chain that allows parachains to have varying levels of information channelled between them. This means that transactions executed in one parachain can initiate new transactions in a second parachain or the Relay Chain. [6] Interchain transactions are resolved using a simple queuing mechanism based around a Merkle tree [8] to ensure fidelity. It is the task of the Relay Chain maintainers (Collatiors) to move transactions on the output queue of one parachain into the input queue of the destination parachain. However, the passed transactions referenced on the Relay Chain are not Relay Chain transactions themselves. [6] There will also be mechanisms to prevent a parachain from spamming another parachain with transactions. [6]

2.2.3 Private Parachains

In essence, private parachains are identical to original Polkadot parachains except those authorities will act as Collators and Fishers for their own private parachain. Still, private members need to show a free will to publicise their dispute details resolution. Otherwise, the resolution fails.[6] A agreement between the parties for their private parachains state transitions is needed to reveal details of any transaction to the Relay Chain Validators as they can validate any new private parachain blocks backed by the parachains participants' cryptographic signatures. In return, the Relay Chain can provide highly secure timestamping, consensus, immutability, and cross-chain services.[6]
In case of disagreement, the parties may reveal the required subset of state and the corresponding smart contract binary code to resolve the block's transactions via Validators to verify the complete state transition. Given that private parachains' goal is for trusted entities to streamline their business interactions, such revealing should only be required in case of surreptitious behaviour or major technical misconfiguration. Parties operating their private partitions as parachains must still pay transaction fees for their consensus and anchoring to the Relay Chain.[6]

2.2.4 Digital Twins

Supplain introduces the Digital Twin smart contract interface, a new form of digital ledger for record-keeping and data exchange within parachains. [22]
The goal of this interface is to standardise the interactions for both physical and digital transactions within the parachains. In addition, Digital Twins need to come with different viewing and editing rights.

Digital Twins serve two essential purposes:

1. By recording each transaction on a unique smart contract interface with different permissions, we enable parachain participants to exchange data using a private and standardised method.

2. By recording both physical and digital transactions onto this smart contract interface, we allow the opportunity to track and trace all transactions in a unified and standardised method.

3 Methodology

In this section the research methodology is introduced. Threat Modeling is a proactive strategy for evaluating cyber security threats. [23] A hybrid combination of STRIDE and PASTA Threat Modeling methods will demonstrate how applicable attack vectors impact the Supplain framework and what may be the possible risks. [24] All threats will be evaluated according to ISO27005 Risk Matrix [10] to create a prioritized risk table and calculate the possibility of likelihood. Once a threat gains some value, then it becomes a risk. For all risks evaluated as critical or high the risk mitigation plan will be proposed with possible countermeasures.

3.1 Threat Modeling

Threat Modeling looks at a system from a potential attacker's perspective, as opposed to a defender's viewpoint**.** In short, it is pen test on paper. [23] To understand how the risks are applying to technical systems a Threat Model methodology is needed to understand where the possible attack points are, how threats may impact systems, classifying threats and applying the appropriate countermeasures. Threat Modeling is a core component of Software Development Life Cycle (SDLC) helping increase the security level of the product. [24]

Similar to Risk analysis a Threat Modeling is also a continuous process needing periodical and regular overview. [25] In this research the primary threats will be identified, then the work does not stop here. Cyber criminals are very smart and cyber space is rapidly evolving. Ensuring the systems are resilient to cyber threats, then continuous assessment is needed. When asking questions like "What could possibly go wrong?" or elaborating on the topic "Are we doing enough?" is already Threat Modeling. [25] It can be theoretical brainstorming, or it can be performed while following known methods. There are many different methods with different approaches.

Three categories for Threat Modeling are:

1. Attacker Centric
2. Risk Centric

3. System/software centric

For Attacker and Risk centric approaches a PASTA method is more used, but it can be also NIST 800-154 proposed by the CISSP training program, for system and software centric approach the most known and widely used is STRIDE. [27]

A threat categorization such as STRIDE can be used to define threat categories such as Auditing & Logging, Authentication, Authorization, Configuration Management, Data Protection in Storage and Transit, Data Validation, and Exception Management. [24] It is a very popular framework and also adopted by Microsoft creating best practises for secure software development. Security engineering and risk management are part of the secure software design. [26] This is not only the responsibility of software developers but the software as a whole including application architects, information security officers, chief technology officers, risk managers and business owners.[27] Software security is not the end goal but a continuous process that aims to reduce risks to an acceptable level of the business. Threat Modeling is misunderstood as software security methodology. For this reason, it is either missing as Secure Software Development Lifecycle (S-SDLC) activity or it is considered as complimentary of other consulting security engagements such as pen testing and secure code reviews, but it should be organic as locking your workstation when leaving away from the desk. Defining applicable threats using the structured approach enables identifying where attackers are able to compromise the systems or data flows. [28]

STRIDE is the most well-established Treat Modeling Method (TMM) and represents the state of the practice. At its core, STRIDE requires breaking down a system into its various elements, assessing each of these elements for their vulnerability to threats, and then mitigating this threat. [29] In practice, a typical STRIDE implementation includes Modeling a system with Data Flow Diagrams (DFDs), mapping the DFD elements to the six threat categories, determining the specific threats and documenting the threats and steps for preventative actions. [23][24] In many cases different methods are combined together as hybrid models due to lack of different capabilities. In a modern threat model, the analysis of use and abuse cases and of business impacts caused by vulnerability exploits are essential to identify countermeasures and mitigating business risks. [29] This is why STRIDE alone is not adequate for designing secure software because threats and attacks have evolved from the basic threats. Consider the example of an attacker using an interface that takes credit card information not to steal credit card data but to enumerate which credit card numbers are valid so they can be used for online purchases or counterfeit credit cards. This is a type of threat that STRIDE does not categorize because is tied to business impact not technical impact. [27] The attack surface of today's applications has also become wider including all the available application interfaces and channels that are exposed to a potential attacker. The Process for Attack Simulation and Threat Analysis (PASTA) is a process for the threat analysis of cyber threats by focusing on business impacts and with the ultimate objective of protecting the company digital assets such as data and critical business functions. [28] This is not a standalone threat model for software developers but rather a risk framework that can be used by organizations as a whole. PASTA is a very mature and throughout method, it is more used for threat assessment for mature companies and for software products already in production. STRIDE on the other hand can be used for “green” products in design phase and theoretical assessment since it does not require very detailed input.

For this work part of PASTA method is followed to create Asset Inventory and Threat Catalogue and STRIDE will be the method for this research to map the threats, attackers, systems and risks. Although STRIDE and PASTA are covering the risk assessment module, the risk prioritizing is left to decide for the modeler or the members of the threat Modeling team. Threat evaluation is a very important input for mitigation activities and therefore following a structured well known assessment method like ISO27005 [10] will give the correct input. Specially this is needed when evaluating non-technical weaknesses like human errors. For threat evaluation and prioritization a Risk Matrix will be used to determine possible probability and impact score and define requirements for the risk acceptance criteria.

ISO/IEC 27005 provides the necessary skills and knowledge to build up complete Risk Management Process, but it is not in scope of current thesis. ISO27005 scope for this work: Prioritization of risks; Evaluating probability and impact; Conditions for accepting risks.

Threat Modeling will be performed in 3 major steps:

1. **Decomposition of Supplain.io**

Identifying critical assets, procedures and systems. This section describes the critical activities required to deliver the service

- Inventory of system assets, procedures, and data (PASTA)
- Define Attack Surface (STRIDE)
- Define Trust boundaries (STRIDE)
- Data Flow Diagram (STRIDE)

2. **Threat analysis**

Threats and vulnerabilities may not always be static or easily noticeable.

- Identification of threats (STRIDE)
- Creating Threat catalogue (PASTA)
- Identification of possible Threat actors (human or event) (STRIDE)
- Tools, techniques, procedures (TTP)
- Define how attackers might move from resource to resource (STRIDE)

3. **Risk Assessment**

- Calculates probability and impact using Risk Matrix
- Prioritization
- Risk justification and conditions for accepting risks.
- Mitigation proposals for Critical or High risks

3.2 Data collection and activity plan

Sources for the Threat Modeling are identified as either associated with Threat Identification (e.g., such as a direct or indirect attack), Organisational (e.g., insider threats, assets, systems) or the consensus mechanism in blockchain (e.g., platform and system threat) systems.[25] Each of these can lead to specific weak points and are linked with technical, human, and physical levels. [26]

For this research qualitative data collection methods are used to gather in-depth insights on the topics. This includes interviews with open-ended questions, observations expressed in words, and literature reviews that explore concepts and theories to understand concept.

One of the main goals of Threat Modeling is to gain understanding how the system works in detail. This means mapping data to assets, procedures and people. The main difference between Threat Modeling and Pen Testing is that the first one is able to detect design flaws and the second one is used for code bug hunting. [30] These two can't replace each other, but one is not complete without the other. It can be really challenging to bring together infra people with developers and start a discussion on theoretical nonconformities that may lead to attacks. Usually in the design phase, a company does not have yet security people onboarded and the focus is more on delivering the product to the mark as fast as possible. Typical start-up thinking "Launch product now, deal with the security later" may lead to monetary loss and extension of deadline. [31] For the security people it is very hard to perform security workshops to lead the conversation in the desired direction and at the same time keep it constructive because it is exhausting and difficult. Even if the development team does not have all the right or correct answers now, then playing with different attack scenarios may help to research the desired security and privacy goals.[28]

With the Supplain Team multiple interviews and workshops were conducted. Mainly via Teams or Google Meet due to the general restrictions of COVID-19 situation in Estonia for physical contacts. The data collection plan did not go as fluently as initially planned and deadlines were exceeded due to the COVID, but the main goal was achieved. Many meaningful discussions among focus groups were performed and necessary information to complete the research was acquired. Activities performed for the data collection:

- Defining focus groups: Designers, Developers, system administrators (Infra)
- Constructing questionnaires
- Individual interviews with focused groups
- Team discussion with focus groups: Asking structured open-ended questions
- Creating topology of systems for Asset Identification
- Workshop with technical Team Leads to analyse of data flow, creating Data Flow Diagram (DFD)

- Workshops for mappings of human interaction
- Defining risk acceptance criteria and criteria for product deployment

The author of this research worked together with Supplain Team from December until April 2022 to assure enough data is collected. Meanwhile the infrastructure changed a lot from comparing the initial design to build the service on Ethereum platform to the final decision to go with Polkadot.

4 Decomposition of Supplain.io

During the Threat Modeling exercise, it is possible to identify design flaws and errors of the Supplain framework. By decomposing the product using Data Flow Diagram (DFD) it is possible to identify the attack surface and understand the how critical assets, associated processes and entities will become together. [30] The contextual knowledge of data flows and trust boundaries will help to analyse the possible attack points and vectors. In this section it is described the security and privacy requirements Supplain wishes to achieve and by creating Data Flow Diagram [29] it is possible to understand how data is shared end to end and where are security controls needed. Bad design may lead to vulnerabilities and the sooner these errors can be identified and eliminated the easier it makes the developers work in later software production stages.

4.1 Security and privacy requirements

Supplain aims to become a blockchain framework with high security, privacy, and performance standards required to accelerate the mass adoption of this technology and support a lasting ecosystem. Unlike other blockchain implementations which are slow and heavy to maintain the Supplain is seeking a very fast communication mean for all the stakeholder exchange data. The goal is to gain tamper proof data, evidence, trusted parties, and transparency of transaction. Supplain is aiming for a program, that is secure by design and will be applicable to elementary security need. These requirements may change in time while the system development and design will improve and become more mature.

Security and privacy requirements are based on OWASP requirements for developing web application but adapted and changed for fulfilling the objective of developing decentralized open-source protocol for private blockchain. [2´7] Requirements are presented in Appendix 2.

4.2 Defining Attack Surface and Trust Boundaries

The Attack Surface presented in Appendix 3 will give overview of external entities, data storage and data flow needed to perform 1st Use Case and shopping from known online store and 2nd Use Case, where is needed to maintain and update Supplain node. The goal of this step is to gain an understanding of the application and how it interacts with external entities.

Defined use cases:

1st Use Case: A customer orders from a known E-shop. Package will be sent out from the warehouse with a digital label and Courier, who is working for the Logistics provider Company, will make the delivery.

2nd Use Case: System admins for both companies, E-shop and Logistics provider, are maintaining Supplain nodes in their local premises and are downloading updates from GitHub. System admins will give feedback and proposals for new updates.

Trust boundaries represent the access rights that need to be granted by entities. In the context of Threat Modeling, it means a specific location on a data flow diagram where data changes its level of trust. It can be:

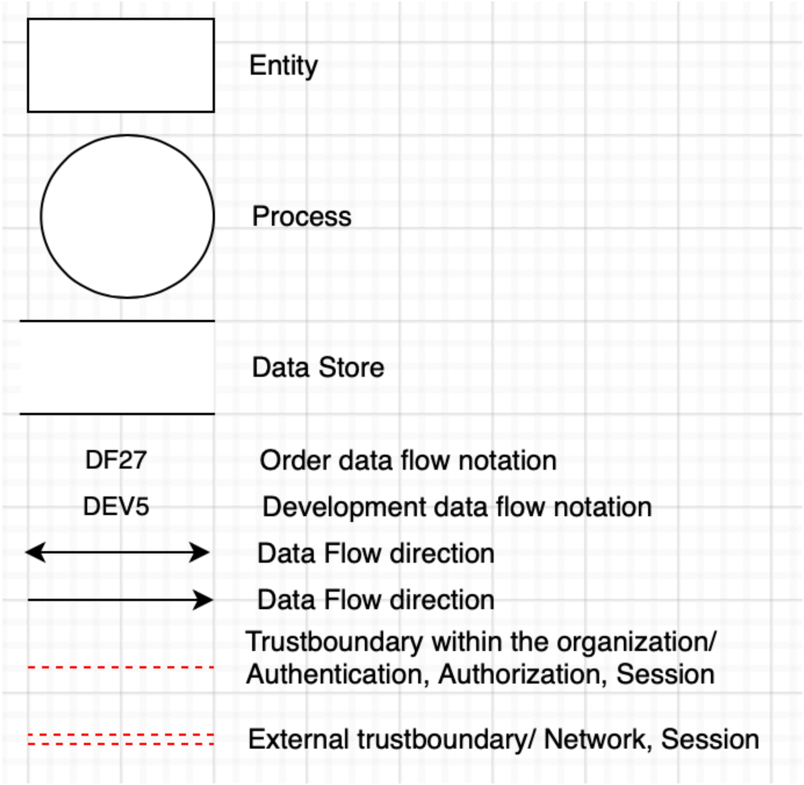
- Authentication
- Authorization
- Session

4.3 Data Flow Diagram

The DFD allows to gain a better understanding of the application by providing a visual representation of how the system processes data. Data flows show how data flows logically through the application, end to end. [31]

There are many different symbols to choose from, but for this work the author chose Yourdon DeMarco style, since it is most known and adopted by Microsoft. [32] Figure 3 (page 38) is presenting the notation used for creating DFD.

DFD-s are presented in Appendix 4 for 1st use case and Appendix 5 for 2nd use case.


Entity
Process
Data Store
DF27
Order data flow notation
DEV5
Development data flow notation
Data Flow direction
Data Flow direction
Trustboundary within the organization/
Authentication, Authorization, Session
External trustboundary/ Network, Session

.

Figure 3: The notation of DFD. [32]

5 Threat Analysis

This section will describe how applicable threats were identified and how are these findings presented in Threat Catalogue. Using STRIDE and PASTA methods will help to map attack vectors and attacker profiles to dataflows and gain understanding what kind of tools techniques and procedures are possible to use. Risk mitigation proposals for threats identified as Critical or High are presented together with the evaluation of the threat impact and the probability by the Risk Matrix adopted from ISO/IEC 27005.

5.1 Identification of threats and STRIDE types

In cooperation with Supplain Team applicable threats and vulnerabilities are categorized and identified in the Threat Catalogue in Appendix 6. Information was gathered by conducting interviews with systems developers, scrolling through CVE catalogues [34], best practises of patching processes, statistics, reading on experience of other organization and information found in public channels. Some points, that helped to detect threats and vulnerabilities:

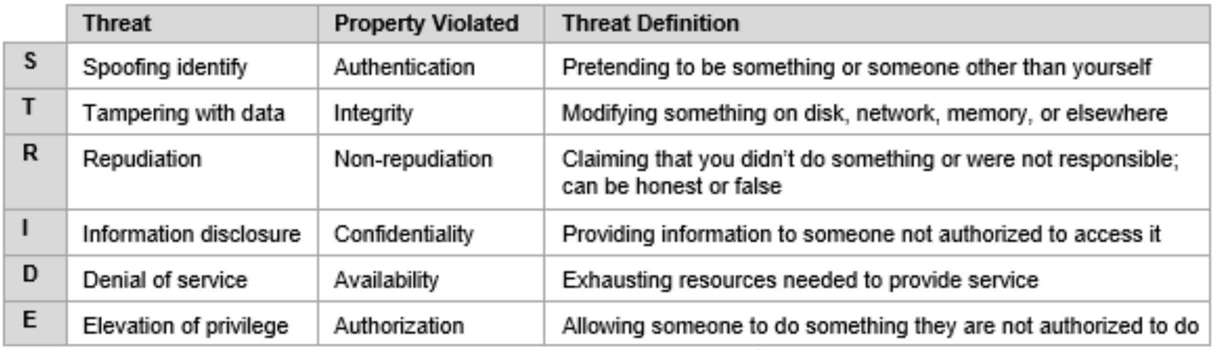
- Threats are changing in systems space and time
- Threat can be environmental or human driven
- Threat can be intentional or unintentional
- Some threats can affect multiple systems, be involved with different vulnerabilities, and paralyze entire infra
- Vulnerability is weakness in systems that can be exploited for harming purposes

Should be taken in account threats that have occurred in the past and learning points from previous incidents. [35] Since the Supplain product is in the design phase, then the applicable threats and vulnerabilities are identified based on knowledge gathered from

Polkadot whitepaper. [16] All threats mentioned are theoretical and may not be applicable for the final product. This list is not complete since the Polkadot is also in the development phase and they are proposing for further research to perform security testing, pen testing and bug hunting on the Polkadot Relay Chain for proving the strength of consensus mechanism. [36] There are some security issues that are addressed, but all of them are referred to as needs further research.

Threats are mapped with possible attackers to determine what kind of attack tools, techniques and procedures they may use and how serious are the consequences. Also presented what systems are affected by the threats. The Threat Catalogue will give an overview of applicable attacks. Attacks are divided into following categories by threat types following the STRIDE method.

Table 1: The STRIDE method. [27]



	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

5.2 Threat Catalogue

Threat Catalogue is a generic list of applicable threats that may somehow compromise the availability and integrity of the Supplain service or prevent the team for reaching desired security and privacy goals presented in Appendix 2 - Security and Privacy Requirements. In the table there is shown how to verify if security control is verified. To help to identify and verify threats against requirements the threats are divided into categories.

Threats will be presented in following categories:

1. Attacks towards systems and users
2. Attacks against source code
3. Attacks against privacy
4. Human error

Identified threats are assigned a unique ID and type defined by STRIDE. To find out in what way and what kind of attack vectors is possible to activate on Supplain service it is important to define possible attacker profiles and what kind of tools, techniques and procedures they might trigger to fulfil the attack. Attacker profiles are described in Table 2.

Table 2: Attacker Profiles.

Attacker	**Profile**
Insider	Someone, who has access internally to systems connected with Supplain service. Can be E-shop admins and technical staff or employees of Logistics provider or member of Supplain Team or stakeholders in Private Parachains and Relay Chain. Insiders' activity may be: a) Accidental, b) Malicious, c) Accidental or malicious
Supplier	System, partner or contractor, who has ability to make an impact on Supplain Service. Like programming code, Linux server or GitHub cloud service. Suppliers' activity may be: a) Accidental, b) Malicious, c) Accidental or malicious.
Customer	Someone, who makes an order from an E-shop. Activity may be: a) Intentional b) Accidental
Malicious hacker	Person with excellent technical skills. Hacks systems for personal gain, mainly financial. Activity: Malicious
ATP	Advances Persistent Threat. State sponsored, organised crime. Activity: Malicious
Force majeure	A person or event that might somehow have impact on Supplains' service, but it is not predictable. For an example: intentional activity like Government is changing the law that regulates blockchain services or accidental, like COVID19 crisis. Activity: accidental
System Failure	Service interruption due to hardware or software failure of system technical components supporting the service. Activity: Accidental

To fully understand how attacker can move from resource to resource and a lateral movement will be defined. For attacks oriented towards blockchain it is less relevant due to fact of decentralization principle, but it is very useful when evaluating the threats that can be executed on services provider side, like E-shop and Logistics provider. Threat Catalogue is presented in Appendix 6 along with mitigation proposals to gain better understanding how a threat can become a risk with the probability assessment how likely it will happen.

5.3 Risk Matrix and risk mitigation proposals

The goal is to be aware of the threat level and reduce the classification to an acceptable level. This is not always possible as sometimes although the score is reduced, it remains in the same classification (ex: reducing the score from 9 to 6 means it remains a medium level threat). Since the risk assessment principles apply for threat assessment in Threat Modeling, then criteria are described along with the inherited activities based on the ISO27005 probabilistic risk assessment. This will give answers to 3 questions:

1. What can happen?
2. How severe is the impact?
3. Will it happen again?

While the ISO27005 proposes different methods for the risk treatment like risk avoidance and risk sharing, this work is limited with means only used for risk mitigation. The scope is to take appropriate measures or suggest additional security controls where needed to reduce the probability and/or impact of the risk.

Usually when an organization is defining the probability of the threat occurrence, the input is based on previous knowledge and weaknesses found in the past taking into account security measures already applied. Performing probability assessment of software that is still in the design phase it is taken into consideration the data flows designed in terms of predefined use cases, information collected from public sources and literature overview. Considering the following:

- Knowledge and statistics of Polkadot developers
- Intentional threats: driven by motivation and skills of an attacker
- Unintentional threats: location, weather, human error, technical failure
- Characteristics of vulnerabilities
- Efficiency of applied security measures

Probability assessment based on the criteria presented in Table 3 (page 43) together with criteria for the impact presented in Table 4 (page 44) will give overview of preventing, detecting and relieving security measures, that will help to mitigate threat realisation. Results of calculation using Risk Matrix will be presented in Table 5 (page 44) along with the detailed description.

5.3.1 Criteria for evaluating Probability

Criteria is described based on principles defined by ISO27005 but tailored for current use cases.

Table 3: Criteria for probability assessment.

Grade	Meaning
5	Certain - bound to experience further incidents of this nature. 85-100%
4	Probable - likely to experience incidents of this nature; happened before. 63-85%
3	Possible - It is distinctly possible to happen. 50%- 62%
2	Unlikely - Uncommon, but genuine chance. 25-50%
1	Rare – conceivable, but unlikely experienced. 1-25%

5.3.2 Criteria for evaluating Impact

Criteria is described based on principles defined by ISO27005.

Table 4: Criteria to evaluate impact.

Grade	Meaning
5	Catastrophic - long term effect on service, external environment, critical financial losses, reputation damage, hostile public and media attention, causes customer refusing of service
4	Major - long term effect on service, external environment, critical financial losses, reputation damage, negative public attention, may lead to customers opting out of the service
3	Moderate – may cause interruption, have some impact on reputation, negative attention, possible money loss
2	Minor – limited negative attention, no significant money, time or performance loss
1	Irrelevant – does not cause significant obstacles, negative attention expressed by individual, no disruptions

5.3.3 Risk Matrix

To get an overview of critical risk, the value of risk classes is calculated in Risk Matrix. The Risk Matrix describing the values is presented in Table 5 (page 46). The scope of Risk Matrix is reduced and tailored to be suitable for current research.

Calculation method for Risk Matrix:

Risk = Probability * Impact

Table 5: Description of Risk values. [10]

Colour	**Risk value**	**Description**
🟥	**Critical (Risk value > 15)**	Unacceptable risk. If the risk is assessed as very high, it requires immediate action and the planning and implementation of preventive and mitigating measures. Further operation of the systems is not allowed without reducing the level of risk to at least the "high risk" level.
🟧	**High (Risk value 8-15)**	Significant risk. Risk mitigation is needed as soon as possible. A plan for risk mitigation must be already implemented.
🟨	**Medium (Risk value 4-8)**	Unwanted risk. If plan measures to reduce the risk, it needs to be implemented within reasonable time. Risk has to be monitored.
🟩	**Low (Risk value < 4)**	Tolerable or negligible risk. The risk is recognized, but no further action may be taken to reduce it. Risk has to be monitored.

5.3.4 Risk acceptance criteria

Acceptance criteria defined as following:

- It is obligatory to implement security measures for classes Critical or High. Critical and High risks need immediate reduction to the level at least "Medium".
- Risks that can paralyze service or cause reputation damage are prioritized even if the Risk Matrix score is below “High”.
- If risk is below High, then evaluate the cost vs security measure needed. Not in scope of Risk Mitigation Plan.
- If a security risk is “Medium” or below and it does not paralyze systems and business processes can continue without complications, then the company accepts the risk.

6 Results

The results of Threat Modeling presented in Appendix 6 demonstrate that while typical cyber incidents are not applicable for the decentralised systems the blockchain will create a way for totally new attack vectors. The analysis shows that the most popular attack vectors are directed towards users and systems, but also the amount of threats related to human error is significant. As presented in the Threat Catalogue the blockchain technology is not secure by the design. To achieve the compliance with the Security and Privacy requirements Supplain needs to think of how to add more tailored security controls. Due to the need of having a node on client's side that enables data read and write into the blockchain Supplain module becomes vulnerable to threats that are not under Supplain's controls but have significant impact on confidentiality, integrity and availability of the whole Supplain framework. This may lead to consequences where the product will lose the trust of its users and the Supplain may experience reputation damage and financial loss. Here is needed to work on a plan how to add security controls or security requests to the perimeter opened on client side to intentional or accidental activities of inside users.

It is important to note that while many treats are rather rare or unlikely to happen then due to the immutable nature of the blockchain functionality the impact is often major or catastrophic that may lead to serious consequences like data leak, financial loss or reputation damage. The recovery process takes a lot of time and incidents have long term effects on the service. Including negative media attention. That means the threat is immediately evaluated as high or critical and actions needed to reduce the risk level at least to medium stage.

The positive aspect is, that due to the decentralised model the attacker's movement across the entire system is not that easy as in well-known centrally managed environments.

The goal of the analysis is to show if the desired Security and Privacy Requirements defined in Appendix 2 are met or not. Below result will show the conformities and non-conformities to the requirements.

SEC-1

There are findings about possible threats to Data Privacy. Threat identifies as THR20 and 21 will demonstrate direct threats to data privacy although all consequences that reflect data leak or loss (THR1; THR2; THR9; THR10; THR12; THR15-19; THR23-27) are also appliable for his requirement. Data does not remain private in the whole supply chain.

SEC-2

There are findings proving the lack of privacy controls. Data tampering and spoofing is possible due to the accidental errors or consequence of intentional malicious activity of Insider or Supplier. For more detailed info please look at THR1; THR3-8; THR10-13; THR16-25; THR26 and THR27.

SEC-3

Verification is enabled thru W3C Decentralised Identifiers module built in Digital Twin process. Digital Twin will determine the access rights and provide users authorization from the client side. Digital Twin itself is installed on Linux supported machines and the maintenance of the node on client side is left on the hands of admins from client side and verified by the blockchain if required updates. Previously there are documented findings of threats and vulnerabilities defined for Digital Twin service. That shows the need for extensive security preventive actions from the client side. Not verifying if the node on client side is kept up to date and preventative actions are in place may lead to security incidents and data loss. For more detailed info please see all Threat Types marked as Spoofing or Elevation of Privileges.

SEC-4

There are many studies that show the possible malicious behaviour or causing unintentional error by the Validator. Relying on analysis based on Polkadot Parachain there is a possibility the Validator behaves in unexpected way without the system detecting the flaws. Due to the lack of information of the possibilities to add more controls or secure the protocol in sufficient ways and the fact that the Fishermen module is still not yet designed throughout it is not possible to evaluate if this requirement is met or not. More information needed to collect in future stages of developing Supplain protocol.

SEC-5

The desirable swarm size and the minimum swarm size needed to assure the operability of the Suppain Relay Chain will be inherited from the Polkadot design. Threats that may have an impact on Supplain Relay Chain operability causing the service being unavailable is defined by Denial or Service type of threats and evaluated accordingly. Please see THR1; THR5-7; THR10; THR12; THR14 and THR16-18 for more details.

SEC-6

Even if the technology of blockchain enables to transfer data securely and guarantees immutability then the data entries enable data spoofing, tampering and fraud. Applicable Threat ID-s: THR1-5; THR8-13; THR15-17; THR22-27.

SEC-7

There are security controls configured to prevent unauthorized users being able to access nodes on client premises. Since there exists possible threats that may be used for baypassing security controls are taking advantage of weak controls and configuration errors, then it is not 100% assured the requirement is met. Please see THR1; THR11; THR12; THR25.

SEC-8

Threats applicable to systems and software have been evaluated. Results show that there are ways to compromise the service. Possible threats presented in subsections "Attack towards systems and users" and "Attacks against source code". All findings are presented in Threat Catalogue in Appendix 6.

SEC-9

There are findings that show if the service gets hit by the targeted cyber attack then the results may be financial loss, reputation damage or data loss. Known blockchain oriented cyber attacks are defined in section "Attack towards systems and users". There are findings about possible software related errors and design flaws that are exploitable and may lead to successful cyber attack. For more info see subsections "Attack towards systems and users" and "Attacks against source code".

SEC-10

The cryptographic measures chosen for Supplain protocol are strong and well thought of. The possibility of accidental error like losing or exposing the cryptographic keys is the realistic threat in this scenario. It can be stated this requirement is met but is vulnerable to human errors.

7 Conclusion

The launch of Supplain protocol further advances the current state of blockchain significantly, bringing it closer to mainstream adoption. There won't be one platform to rule them all however, with some use cases better suited to one platform over another. The more projects researching and delivering breakthrough technology the better, each learning from each other and pushing each other to reach that goal earlier.

The idea to start using Blockchain technology in wider areas and in different use cases, not only crypto currencies, is quite new. First research papers are found from 2019 that show the benefits of using decentralised data exchange models in parcel service as defined in use cases for current work. Supply chains are one of those areas where the trust problems of communication chains and data exchange are actual. Thanks to Supplain.io's great project and talented team it is possible to get a closer look at how exactly blockchain is used to solve these problems and perform the security assessment of the service.

The process of the threat assessment and treatment of critical flaws is fundamental while developing new systems. Only by fully understanding the sources and consequences the developers will be able to provide an appropriate level of protection against cyber security threats and avoid major design flaws. For the interested stakeholders this work will help to understand the applicable threats and mitigation techniques to lower the probability of the threats to become live in the Supplain.io-s technology.

Threat model created based on the hybrid model in combination of STRIDE and PASTA methods demonstrates how attackers might influence the quality and integrity of the Supplain service. With the inherited design of Polkadot, the security of the relay chain is paramount. Meaning if some parachain is compromised then all connected chains will also be compromised. The findings of non-conformities to Security and Privacy Requirements prove the desired security level cannot be achieved by the default design of blockchain and more tailored cyber security controls are needed to implement. Hopefully mitigation proposals for reducing the probability of the threats to become real will help the Supplain Team make deliberate decision where restrictions and security controls are needed to design and what kind of security requirements are needed to adapt on the client side.

Proposal for future work is to assess different use cases built on similar platforms like Polkadot to keep an eye on the development of the blockchain applications and one day hopefully perform the threat model analyse in real time being able to continue the research by Mubashar Iqbal and Raimundas Matulevicius [14] building a comprehensive reference model for security risk management to systematically evaluate the security needs that helps such companies as Supplain to evaluate the security and privacy of the blockchain based product.

References

[1] IBM Corporation: IBM Blockchain for Supply Chain solution brief. Technical report (2020, USA). 3-8

[2] Gjorgji Shemov, Borja Garcia de Soto, Hoda Alkhzaimi: Blockchain applied to the construction supply chain: A case study with threat model. (2020) 564-577

[3] Esteban Ramirez: Preserving Information's Integrity and Confidentiality with Blockchain in the service in Supply Chain. Taltech master thesis. (2021)

[4] Lukas Marx: Storing Data on the Blockchain: The Developers Guide. (2018)

[5] Beth Owens: Blockchain in logistics: What it is and how it's changing the industry. Technical article by Whiplash. (2021)

[6] David Bailay-Lauring: Supplain Whitepaper. Source: homepage https://supplain.io (2022)

[7] Dylan Raffety, Kevin Curran: The Role of Blockchain in Cyber Security. (2021) 4-8

[8] Teelika Šutov (Taltech, 163350EALM): Reckoning Supply Chain Human Errors in Blockchian Technology Development. (2018)

[9] OWASP Blog: Advanced Threat Models https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf . Last visited: 14.05.2022

[10] ISO/IEC 27005:2018 Information Security Risk Management Standard.

[11] Bayramova,A.; Edwards, D.J.; Roberts, C. : The Role of Blockchain Technology in Augmenting Supply Chain Resilience to Cybercrime. 2021

[12] Rami Alkhudary, Xavier Brusset, and Pierre Fenies: Blockchain and Risk in Supply Chain Management.. 2020

[13] Mubashar Iqbal and Raimundas Matulevicius: Blockchain-based Application Security Risks: A Systematic Literature Review. (2019)

[14] Mubashar Iqbal and Raimundas Matulevicius: Comparison of Blockchain-Based Solutions to Mitigate Data Tampering Security Risk. (2019)

[15] Polkadot wiki. https://wiki.polkadot.network/docs/learn-launch. (2020) Last visited: 14.05.2022

[16] Dr. Gavin Wood: Polkadot: Vision for a Heterogeneous Multi-Chain Framework Draft 1 (2018)

[17] Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kılın ̧c Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart, Gavin Wood, Web3 Foundation, Parity Technologies: Overview of Polkadot and its Design Considerations. (2020)

[18] Pavel Horbonos: How to build a parachain on Polkadot. (2019)

[19] Trustnodes.com: Polkadot, The Ethereum 2.0 or The Mighty Race: Vitalik Buterin v Gavin Wood. (2019)

[20] Cryptosec.medium.com: Polkadot — An Early In-Depth Analysis — Part One — Overview and Benefits. (2020) Last visited: 14.05.2022

[21] Ben Lomax Thorpe: Risk mitigation in digital twins. 2021.

[22] Cryptosec.medium.com: Polkadot — An Early In-Depth Analysis — Part Two — How consensus works. (2020) Last visited: 14.05.2022

[23] Exbeam Blog: Top 8 Methodologies and Techniques. Infromation Security (2021) Last visited: 14.05.2022

[24] Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, Carol Woody: Threat Modeling: A Summart of Available Methods (2018)

[25] Adam Shostack: Fast, Cheap and Good – An Unusual Tradeoff Available in Threat Modeling. (2021)

[26] Dr. Abhijeet Ghadge, Maximillian Weib, Nigel Caldwell, Richard Wilding: Managing cyber risk in supply chains: A review and research agenda. (2019)

[27] Nataliya Shevchenko: Threat Modeling: 12 Available Methods (2018)

[28] Secure Software blog post by TustedConsultant: PASTA Process for Attack Simulation and threat analysis (PASTA) Risk-centric Threat Modeling (2012) Last visited: 14.05.2022

[29] Nancy R. Mead, Forrest Shull, Krishnamurthy Vemuru, Ole Villadsen: A Hybrid Threat Modeling Method. (2018)

[30] Larry Conklin, Victoria Drake: Threat Modeling Process. (2020)

[31] OWASP Blog: Testing Against OWASP. OWASP BLOG (2022) Last visited: 14.05.2022

[32] Visual Paradigm Online: DFD Using Yourdon and DeMarco Notation. (2022) Last visited: 14.05.2022

[33] European Commission Study: Legal, governance and interoperability aspects. (2018-2020) Last visited: 14.05.2022

[34] CVE details: CVE catalogue of vulnerabilities. Updated 2022. Last visited: 14.05.2022

[35] FBI: Flash report of known indicators of compromise (IOC). 19th April 2022. Last visited: 11.05.2022

[36] Cryptosec.medium.com: Polkadot — An Early In-Depth Analysis — Part Three — Limitations and Issues. (2020). Last visited: 14.05.2022

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Marje Salumets,

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Threat Modeling of the Supplain.io Blockchain Protocol: Preserving Data Trust, Privacy and Security in Physical Supply Chains”, supervised by Kaido Kikkas, PhD.
    1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
    1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

12.05.2022

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Security and Privacy Requirements

Requirement ID	Name	Description	How to verify?
SEC-1	Privacy Preserving	Data is and remains private in the whole supply chain	Evaluate data security in rest and in transit; Analyse data flow use cases;
SEC-2	Privacy Controls	Supplain has to constantly balance between its open nature and privacy controls, ensuring that the network remains thrustless	Evaluate the threats that might be imposed by the members of Supplain Relay Chain, Private Parachain (Supplier; Insider)
SEC-3	Identity verification	All new companies must be verified; All users accessing the systems from client side must be recognized	Evaluate the threats categorized as Spoofing; Privileged escalation;
SEC-4	Validators duties	Ensuring validators fulfil their duties and being reachable.	Evaluate against provably and previously defined known malicious actions or threats
SEC-5	Operability of the Relay Chain	Providing immutability, timestamping, and cross-chain services. This enables smaller chains with fewer participants to pool their security together, with built-in cross-chain capabilities	Evaluate the swarm size of validators and efficiency of Fishermen; Define and evaluate the threats that might lead to service being unavailable
SEC-6	immutability and non-repudiation	Data is valid and verified, it cannot be changed	Evaluate threats that might use means for data spoofing, tampering and plain old fraud.
SEC-7	Authorization of users	Strong user authentication and	All users must be authorized and

		authorization principles are implemented on client side.	assure it will not be possible to manipulate with the data and permissions
SEC-8	Functionality and operational architecture and implementation of secure coding practises	Follow and documents principles of secure code development. Define testing goals and criteria of acceptance.	Evaluate threats applicable to systems and software. System creator shall guarantee the final product is tested (black box, white box), is secure for the users and code bugs are eliminated. The final product shall be secure by the design for users with technical skills and non-technical users.
SEC-9	Backend, API communication and nodes	Assure the availability and functionality of the systems while under cyber attack. Assure the nodes are secure for downloading and distribution.	Evaluate the cyber resilience of the systems under different pressure. Make available system hashes and functionality description to allow users to verify if the connections and functionality of the downloaded version is accurate and safe.
SEC-10	Cryptographic measures	The strength of cryptographic measures.	Evaluate the threats applicable to cryptographic controls in Supplain Relay chain and Private parachain

Appendix 3 – Attack Surface

ID	Resources of same type	System/Process	Description	System dependency; communication chain
USR-1	USER	Non-technical end-user; Customer	Customer, makes an order from E-shop	OWN-1; DS-1; COD-7;
USR-2	USER	Non-technical end-user; E-shop admin	E-shop owner or administrative personnel. Processing the order, inserting new products, sends invoice, send the delivery data to shared file server	COD-1; DS-1; COD-4
USR-3	USER	Technical end-user; Developer/ Sys admin	Personnel with technical IT skills and programming	COD-3; DS-1; DS-2; DS-5;
USR-4	USER	Technical end-user; Sys admin/ Network admin/ hosting admin	Personnel with technical IT skills, mainly infrastructure and networking	COD-2; DS-1; DS-2; DS-5
USR-4	USER	Technical end-user; Sys admin	Personnel with technical IT skills like system administrator and network administrator	COD-6; DS-3; DS-5
USR-5	USER	Non-technical end-user; Warehouse admin	Warehouse is responsible for stored products, keeping records up to date, making sure all products in E-shop are available	COD-4; COD-1; DS-2; DS-1
USR-6	USER	Non-technical end-user; Courier	Courier gets notification with data needed for delivery and takes the order to the Customer	COD-7; DS-3; USR-1

USR-7	USER	Non-technical end-user; Logistics admin	Logistics admin receives limited data from shared file systems, that is already verified by Supplain relay chain and only data needed for delivery is revealed, is responsible for order delivery	COD-5; DS-3
USR-8	USER	Technical end-user; Supplain admins	Personnel with technical IT skills like programming and system administrator	COD-8; DS-5
PRIV-1-6	USER	Validators, Collators for Private Parachain	Supplain token holders working on Proof-of-Stake principle to make sure data is trusted, accurate and verified for Smart Contracts creating Private parachain	DS2; DS-3; DS-4
SUP-1-5	USER	Validators, Fishermen, Collators for the Relay Chain	Supplain token holders working on proof-of stake consensus in Supplain Relay Chain	CRY-1; CRY-2; DS-4
VAL-1	USER	Validator	Supplain token holder accessing Supplain Relay Chain	OWN-2; CRY-1
COL-1	USER	Collator	Supplain token holder accessing Supplain Relay Chain	OWN-3; CRY-2
FIS-1	USER	Fishermen	Supplain token holder accessing Supplain Relay Chain	OWN-4; CRY-2
NOM-1	USER	Nominator	Supplain token holder accessing Supplain Relay Chain	OWN-5; CRY-2

OWN-1-5	PERSONAL DEVICE	Personal device - not company owned, can be computer or mobile devices	No centralized cyber security related preventive or protective means	USR-1; VAL-1; COL-1; FIS-1; NOM-1; CRY-1; CRY-2; DS1-5;
COD-1-4; COD-5-6; COD-7	COMPANY OWNED COMPUTER	Company owned computer	Under monitoring of E-shop IT, centralized cyber security related preventive or protective means implemented, only authorized software allowed	USR-2-8; DS-1-5;
COD-8	COMPANY OWNED DEVICE OR PRIVATE DEVICE	Company owned or private computer	No centralized cyber security related preventive or protective means	USR-8; DS-5
DS-1	DATASTORE	Web service system for hosting, maintaining, and developing	Under monitoring of E-shop IT, centralized cyber security related preventive or protective means implemented, only authorized software allowed	USR-1; USR-3; USR-4; USR-2; DS-2; COD-1; OWN-1
DS-2	DATASTORE	Web services system provided by Supplain, but hosted, maintained and further developments by E-Shop IT admins	Under monitoring of E-shop IT, centralized cyber security related preventive or protective means implemented, only authorized software allowed	DS-1; DS-3; DS-4; DS-5
DS-3	DATASTORE	Web services system provided by Supplain, but hosted, maintained and further developments by Logistics provider IT admins	Under monitoring of Logistics IT, centralized cyber security related preventive or protective means implemented, only authorized software allowed	USR-6; COD-7; USR-7; COD-5; DS-2; DS-4; DS-5

DS-4	DATASTORE	A smart contract is a code that exists at an address on a chain and is callable by external actor	No centralized cyber security related preventive or protective means	DS-2; DS-3; SUP-1-5;
DS-5	DATASTORE	GitHub public cloud service; Supplain interface	No centralized cyber security related preventive or protective means	DS-2; DS-3; COD-8; USR-8; COD-2; COD-3; COD-6; USR-4; USR-3; USR5
CRY-1; CRY-2	DATASTORE	Crypto Wallet	Public service; Any wallet supporting Supplain tokens	OWN-2-5; VAL-1; COL-1; FIS-1; NOM-1;SUP-1-5;
DF1	DATAFLOW	User Authorizes access to the device	No matter if it is private device or company owned device, every device needs authorization	USR-1-8; COD-1-8; OWN-1-5
DF2	DATAFLOW	Order from E-shop	Customer accesses front end of E-shop to choose products and to place an order	USR-1; OWN-1; DS-1
DF3	DATAFLOW	LOGIN	Customer needs to login	USR-1; OWN-1; DS-1
DF4	DATAFLOW	Registrate	In case customer does not have user account to confirm order	USR-1; OWN-1; DS-1
DF5	DATAFLOW	Place order	After user profile is created and successful login customer places an order.	USR-1; OWN-1; DS-1
DF6	DATAFLOW	DS1	New user created and verified; order is registered in the E-shop web system	OWN-1; DS-1
DF7	DATAFLOW	Process order	Order processing started, info about new order sent to USR-2 who will be responsible for delivery	USR-2; COD-1; DS-1

DF8	DATAFLOW	COD-1	info about new order sent to USR-2 who will be responsible for delivery	USR-2; COD-1; DS-1
DF9	DATAFLOW	Check available product	USR-2 checks if ordered product is available	USR-2; COD-1; DS-1
DF10	DATAFLOW	COD-4	USR-5 verifies availability of products to USR-2	USR-2; COD-1; DS-1; USR-5; COD-4
DF11	DATAFLOW	Send Invoice	USR-2 sends invoice thru DS-1 to Customer	USR-2; COD-1; DS-1; USR-1; OWN-1
DF12	DATAFLOW	Make payment	Customer makes the payment	DS-1; USR-1; OWN-1
DF13	DATAFLOW	DS1	Payment registered in E-shop system and confirmation sent to USR-2	USR-2; COD-1; DS-1;
DF14	DATAFLOW	Confirm order	USR-2 confirms order in the E-shop system	USR-2; COD-1; DS-1;
DF15	DATAFLOW	Reveal shipping details	Shipping details stored into DS-2	DS-1; DS-2
DF16	DATA FLOW	Assembly request	From DS-2 Assembly request is sent to USR-5	DS2; COD-4; USR-5;
DF17	DATA FLOW	Assemble order	USR-5 assembles the order	DS2; COD-4; USR-5;
DF18	DATAFLOW	Add Shipping info	USR-5 adds shipping details	DS2; COD-4; USR-5;
DF19	DATA FLOW	Order ready for delivery	USR-5 send confirmation about order ready for delivery into DS-2	DS2; COD-4; USR-5;
DF20	DATA FLOW	Digital Twin	Digital Twin picks up the order information, adds encryption and transfers the data to private parachain	DS-2; DS-3; PRIV-4;5;6
DF21	DATA FLOW	PRIV-4;5;6	Data is shared between all Collators.	PRIV-4;5;6

DF22	DATA FLOW	DS-4	Collators make a request to write the data into Smart Contracts	PRIV-4;5;6; DS-4
DF23	DATA FLOW	PRIV-1;2;3	Request from Collators forwarder to Validators	PRIV-1;2;3; DS-4
DF24	DATA FLOW	Inbound	New data request sent by validators to Supplain Realy Chain Inbound	PRIV-1;2;3; SUP-1; CRY-2
DF25	DATA FLOW	SUP-1	A collator picks up a new request and forwards it to first group of validators SUP-4	SUP-1; SUP-4; CRY-2
DF26	DATA FLOW	SUP-4	SUP-4 verifies request and forwards it to the next group of Validators SUP-5	SUP-1; SUP-4; CRY-1; SUP-5
DF27	DATA FLOW	SUP-5	SUP-5 receives data, verifies, and presents the info to SUP-3 to confirm.	SUP-4; SUP-2; SUP-3; VAL-1; OWN-2; CRY-1;
DF28	DATAFLOW	SUP-3	Nominators validate the presented data and confirm back to validators	SUP-5; CRY-2
DF29	DATA FLOW	SUP-2	Fishermen check constantly the actions legality of SUP-4 and SUP-5.	SUP-4; SUP-5; CRY-2
DF30	DATA FLOW	Outbound	After mutual agreement achieved by SUP-4, SUP-5 and SUP-3 + legality approved by SUP-2, the SUP-5 forwards the data to Outbound	SUP-5
DF31	DATA FLOW	PRIV-1, PRIV-2, PRIV-3	Verified info forwarded to group of	SUP-5; PRIV-1;2;3

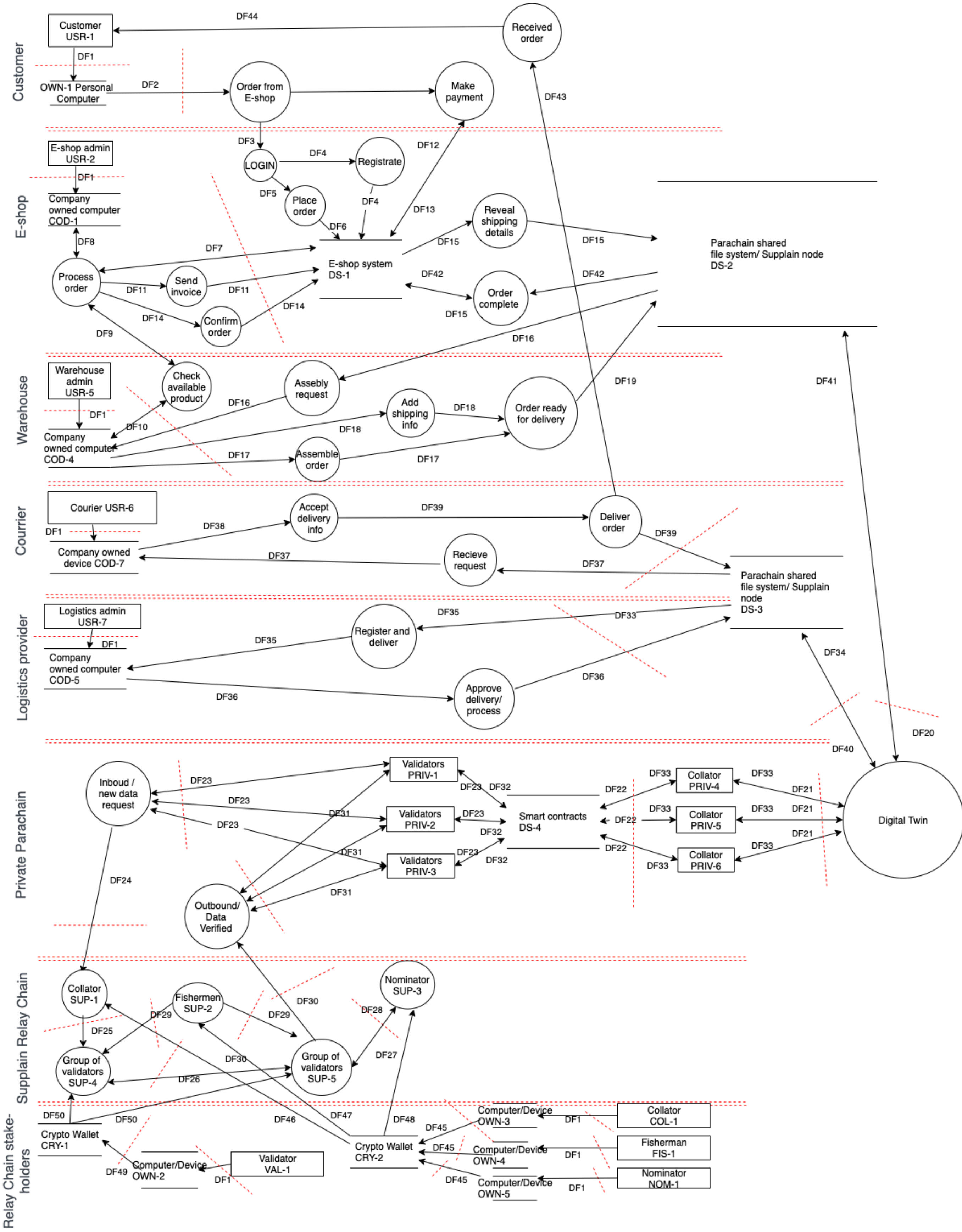
			Validators in Private parachain.	
DF32	DATA FLOW	DS-4	Group of Validators will accept the info from Relay Chain and write it into Smart Contracts.	PRIV-1;2;3; DS4; SUP-5
DF33	DATA FLOW	PRIV-4, PRIV-5, PRIV-6	Collators will pick up the info written into Smart Contracts and forward to Digital Twins	DS-4; PRIV-4, PRIV-5, PRIV-6; DS-2; DS-3
DF34	DATA FLOW	Data transfer to DS-3	Digital Twin delivers the encrypted data back Logistics provider	DS-4; PRIV-4, PRIV-5, PRIV-6; DS-3
DF35	DATA FLOW	Register delivery request	USR-7 receives delivery request from DS-3	USR-7; DS-3; COD-5
DF36	DATA FLOW	Approve delivery/process	USR-7 approves the delivery and is sent back to DS-3	USR-7; DS-3; COD-5
DF37	DATA FLOW	Receive request	From DS-3 delivery request is sent to COD-7 where USR-6 gets info about the delivery	USR-6; DS-3; COD-7
DF38	DATA FLOW	Accept delivery info	USR-6 accepts Delivery info and starts process	USR-6; DS-3; COD-7
DF39	DATA FLOW	Deliver order	USR-6 starts to deliver order. Data shared back to DS-3	USR-6; DS-3; COD-7
DF40	DATA FLOW	Digital Twin	Data about USR-6 delivery process shared to Digital Twin which makes the transfer from DS-3 to DS2 and shares it out to Private parachain; Dataflow repeated from DF21 to DF33	DS-3; DS-4; PRIV-4, PRIV-5, PRIV-6; DS-2

DF41	DATA FLOW	DS-2	DS-2 receives data from Digital twin	DS-3; DS-4; PRIV-4, PRIV-5, PRIV-6; DS-2
DF42	DATA FLOW	Order complete	DS-2 sends info to DS-1 to confirm delivery and marks order complete	DS-2; DS-1
DF43	DATA FLOW	Received order	USR-6 makes the delivery to USR-1	USR-6; USR-1
DF44	DATA FLOW	USR-1	Customer receives the order	USR-6; USR-1
DF45	DATA FLOW	CRY-2	Collators, Fishermen and Nominators need to own Crypto Wallet to access Supplain Relay Chain. User creates own personal crypto wallet account.	COL-1; FIS-1; NOM-1; OWN-3; OWN-4; OWN-5; CRY-2
DF46	DATA FLOW	SUP-1	After authorization COL-1 can perform activities in Relay Chain	COL-1; OWN-3; CRY-2; SUP-1
DF47	DATA FLOW	SUP-2	After authorization FIS-1 can perform activities in Relay Chain	FIS-1; OWN-4; CRY-2; SUP-2
DF48	DATA FLOW	SUP-3	After authorization NOM-1 can perform activities in Relay Chain	NOM-1; OWN-5; CRY-2; SUP-3
DF49	DATA FLOW	CRY-1	Validators need to own Crypto Wallet to access Supplain Relay Chain. User creates own personal crypto	VAL-1; OWN-2; CRY-1; SUP-4
DF50	DATA FLOW	SUP-4	After authorization VAL-1 can become a member of SUP-4 or SUP-5.	VAL-1; OWN-2; CRY-1; SUP-4; SUP-5

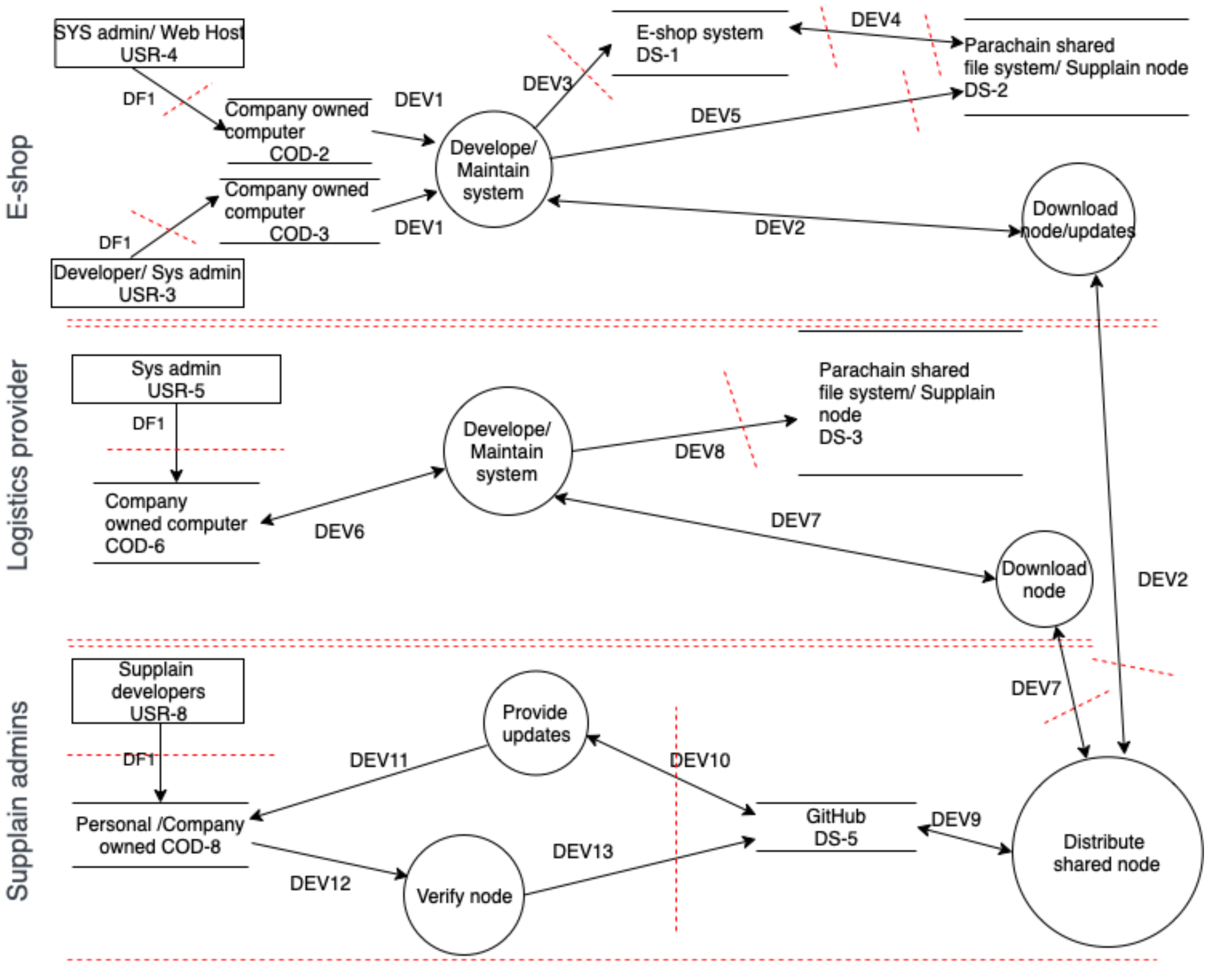
DEV-1	DATA FLOW	Develop/Maintain system	USR-3 and USR-4 work on the system maintenance together to verify cooperation of DS-2 and DS-1.	USR-3; USR-4; COD-2; COD-3; DS-1; DS-2
DEV2	DATA FLOW	Download node/updates	USR-3 downloads updates from DS-5	USR-3; USR-4; COD-2; COD-3; DS-2; DS-5
DEV3	DATA FLOW	DS-1	DS-1 receives updates and configuration to connect to DS-2	USR-3; USR-4; COD-2; COD-3; DS-1; DS-2
DEV4	DATA FLOW	DS-2	Established connectivity between DS-1 and DS-2	DS-1; DS-2
DEV5	DATA FLOW	DS-2	DS-2 is provided by the Supplain admins, but the maintenance and hosting are responsibility of E-shop admins	USR-3; USR-4; COD-2; COD-3; DS-2
DEV6	DATA FLOW	Develop/maintain system	USR-5 develops and maintains the system keeping it up to date DS-3	USR-5; COD-6; DS-3
DEV7	DATA FLOW	Downloaded node	USR-5 downloads the Supplain node form DS-5 to receive updates	USR-5; COD-6; DS-3; DS-5
DEV8	DATA FLOW	DS-3	Keeping the system up to date and maintained	USR-5; COD-6; DS-3
DEV9	DATA FLOW	DS-5	Supplain admins use GitHub for distributing latest and verified version of Supplain nodes. DS-5 used to receive feedback from node users.	USR-3; USR-4; COD-2; COD-3; DS-2; USR-5; COD-6; DS-3; USR-8; COD-8
DEV10	DATA FLOW	Provides updates	All proposed updates are reviewed, and statistical data collected	USR-8; COD-8; DS-5

DEV11	DATA FLOW	COD-8	Supplain developers decide based on the statistics and the criticality of need for new updates and accept proposals when needed	USR-8; COD-8; DS-5
DEV12	DATA FLOW	Verify node	All updates or if new node released are tested throughout before release	USR-8; COD-8; DS-5
DEV13	DATA FLOW	DS-5	New node or updates published on DS-5	USR-8; COD-8; DS-5

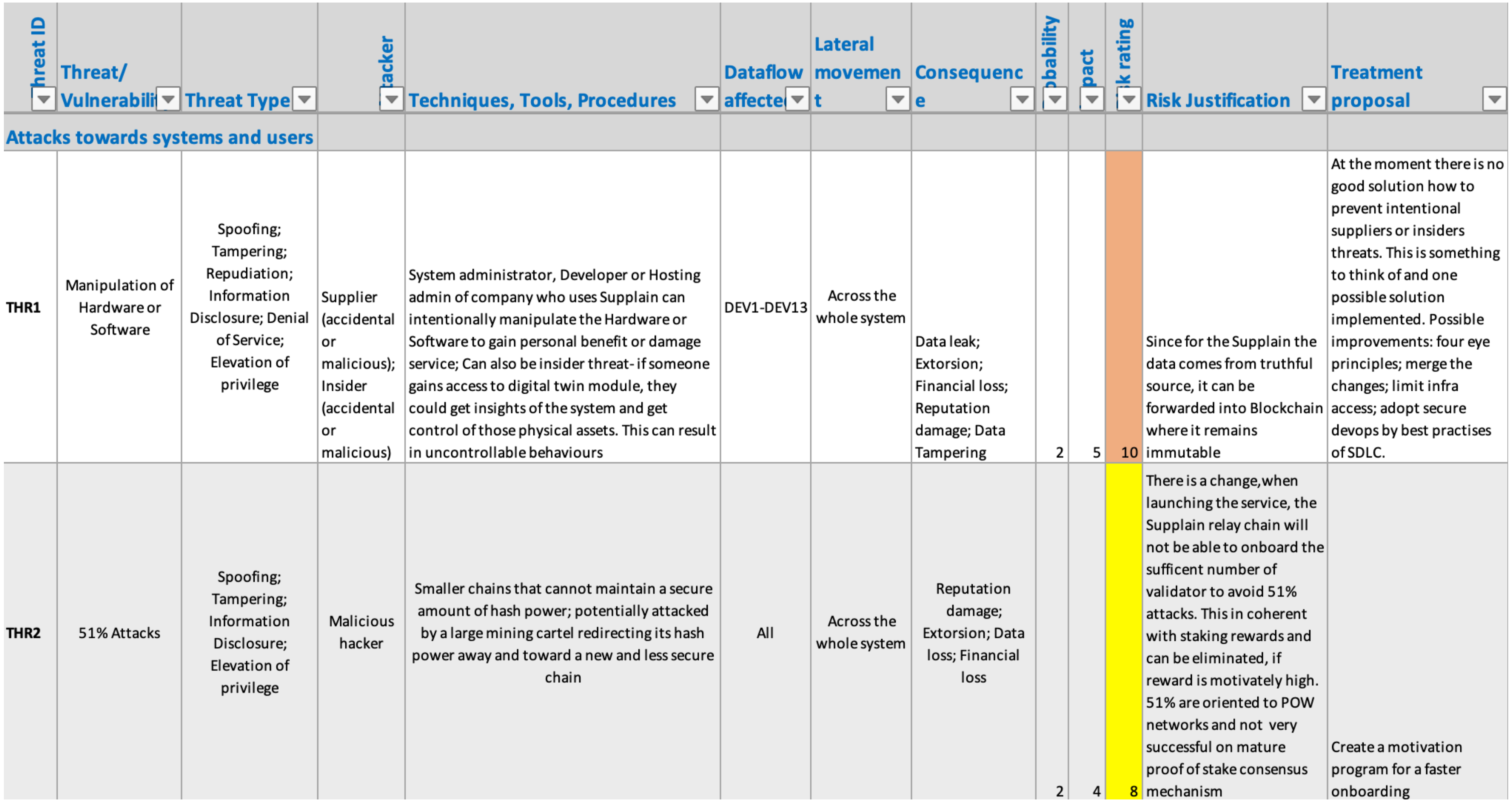
Appendix 4 – Data Flow Diagram for use case 1



Appendix 5 – Data Flow Diagram for use case 2



Appendix 6 – Threat Catalogue and Risk Treatment proposal



hreat ID	Threat/ Vulnerabili	Threat Type	acker	Techniques, Tools, Procedures	Dataflow affecte	Lateral movement	Consequence	obability	pact	k rating	Risk Justification	Treatment proposal
Attacks towards systems and users												
THR1	Manipulation of Hardware or Software	Spoofing; Tampering; Repudiation; Information Disclosure; Denial of Service; Elevation of privilege	Supplier (accidental or malicious); Insider (accidental or malicious)	System administrator, Developer or Hosting admin of company who uses Supplain can intentionally manipulate the Hardware or Software to gain personal benefit or damage service; Can also be insider threat- if someone gains access to digital twin module, they could get insights of the system and get control of those physical assets. This can result in uncontrollable behaviours	DEV1-DEV13	Across the whole system	Data leak; Extorsion; Financial loss; Reputation damage; Data Tampering	2	5	10	Since for the Supplain the data comes from truthful source, it can be forwarded into Blockchain where it remains immutable	At the moment there is no good solution how to prevent intentional suppliers or insiders threats. This is something to think of and one possible solution implemented. Possible improvements: four eye principles; merge the changes; limit infra access; adopt secure devops by best practises of SDLC.
THR2	51% Attacks	Spoofing; Tampering; Information Disclosure; Elevation of privilege	Malicious hacker	Smaller chains that cannot maintain a secure amount of hash power; potentially attacked by a large mining cartel redirecting its hash power away and toward a new and less secure chain	All	Across the whole system	Reputation damage; Extorsion; Data loss; Financial loss	2	4	8	There is a change,when launching the service, the Supplain relay chain will not be able to onboard the sufficent number of validator to avoid 51% attacks. This in coherent with staking rewards and can be eliminated, if reward is motivately high. 51% are oriented to POW networks and not very successful on mature proof of stake consensus mechanism	Create a motivation program for a faster onboarding

THR3	Sybil attack	Spoofing; Tampering; Information Disclosure; Repudiation;	Insider (malicious)	One person tries to take over the network by creating multiple accounts, nodes or computers [32] Attackers may be able to vote against honest nodes; Manage to gain control over network	All	Across the whole system	Reputation damage; Extorsion; Data tampering; Financial loss	3	4	12	Polkadot has not yet finalized the model how Sybil attacks will be prevented. Will it be the responsibility of Collators or Fishermen, it's not clear yet. It poses a risk to other organization who wish to adopt Polkadots functionality like Supplain does	At the moment there are only limited possibilities to implement - extra layer of authentication; onboard fishermen already in early stages while launching the service
THR4	Double Signing	Spoofing; Tampering; Repudiation;	Insider (accidental or malicious)	High availability setups (HA) for validators can be dangerous. The session keys used by a validator should always be isolated to just a single node. Replicating session keys across multiple nodes could lead to equivocation slashes or parachain validity slashes which can make you lose 100% of your staked funds. Double-signing or conspiring to provide an invalid block	DF20-DF40; DF45- DF50	None	Reputation damage; Extorsion; Data tampering; Financial loss	1	3	3	Given that HA setups would always be at risk of double-signing and there's currently no built-in mechanism to prevent it. Even if your validator goes offline for some time, the offline slash is much more forgiving than the equivocation or parachain validity slashing	
THR5	Byzantine fault	Denial of Service; Tampering; Spoofing;	System Failure; Insider (accidental)	A component of Byzantine agreement like a server can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers. It is difficult for the other components to declare it failed and shut it out of the network, because they need to first reach a consensus regarding which component has failed in the first place.	DF20-DF40; DF45- DF50	None	Service unavailable for a shot period; Reputation damage;	2	2	4	Since for the integrity of the service is guaranteed by the 33% of active validators, then it will not have long time affect, but only if enough validators are on-boarded. Maybe serious risk at during the start period.	
THR6	The Post-Bomb attack.	Denial of Service	Insider (accidental or malicious)	A standard transaction DoS attack. This is where all parachains send the maximum amount of posts possible to a particular parachain.	DF20-DF40; DF45- DF50	None	Slows down the service, perhaps unavailable for a while	1	2	2	While this ties up the target's ingress queue at once, no damage is done	

THR7	One chain of Relay Chain spamms other	Denial of Service	Insider (malicious)	One chain intentionally spams others with transaction data; Parachain and relay chain can not make adequet decisions,	DF20-DF40; DF45- DF50	None	Reputation damage; Extorsion; Data tampering; Financial loss	3	3	9	There is no equivalent mechanism provided by the protocol to prevent the spamming of transaction processing.	At the moment Polkadot is looking for solution for the specific threat. Keep an eye on the research.
THR8	Cost to attack	Spoofing; Tampering; Repudiation;	Insider (malicious)	It is possible, that stakeholders like Zug Capital in Polkadot, who are covering 10% or more of the validators selection, could take a small bribe to get invalid node verified. It is the nominators which take the vast majority of risk; Checking the security of setups used by validators is difficult, and whilst there are registrars to confirm identities, these can also succumb to bribes/false information provided;	DF20-DF40; DF45- DF50	None	Reputation damage; Extorsion; Data tampering; Financial loss	4	4	16	In the example of Polkadot using Zug Capital they have verified their identity on-chain using their website, which you can see from polkadot.js UI. zugcapital.com website redirects to the nomination UI. They are anonymous.[31]	Add extra layer for authentication. Every user needs to be properly verified.
THR9	DAO attack	Spoofing; Tampering; Information disclosure; Elevation of privilege	Malicious hacker	The hacker is sending repeated transaction request to transfer funds to a DAO clone and due programming error, the system did not immediately update the balance, allowing the attacker to drain the account; Programming error; code vulnerability; Zero-day	DF20-DF40; DF45- DF50	None	Financial loss; Data loss; Reputation damage	3	4	12	Supplain plans to keep the code public and anyone can explore and audit. At this state there is not planned an secure feedback channel. Neither managed responsibility to keep the code safe. This risk is possible to occure	The vulnerability in code, where DAO was possible, was detected long time before it was exploited by malicious attacker. The responsibility needs to be defined and secure feedback channels established
THR10	Insufficient maintenance/faulty installation of node	Tampering; Denial of Service	Insider (accidental)	Blockchain integration with existing supply chain technological solutions and ERP tools built with conventional technology stack can generate additional or new risks and cost when introduced in the Supply Chain operations; Digital Twin module configuration	DEV1-DEV13	None	High maintenance cost; Reputation damage; Data loss; Financial loss	3	3	9	Since the access node to private parachain is installed and maintained on clients side, then incorrect configuration, administrative mistakes or lack of cyber security knowledge may lead to information disclosure or paralyze the service and harm its integrity	Trainings and workshops; Well defined cyber security requirements and controls

THR11	Data Fraud	Spoofing; Tampering; Elevation of privilege	Insider (malicious or accidental)	Malicious employee may intentionally enter false data. Since it stays immutable in blockchain it affects data integrity across the chain	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Reputation damage; Extorsion; Data tampering; Financial loss	2	5	10	Due to the nature of blockchain technology data is immutable. Blockchain components dont see all the info entered nor dont have the capability to judge if data inserted from the client side is done maliciously or accidental.	It is very hard to avoid such threats, but one possibility may be evaluating the information security maturity level of the client.
THR12	Lack of identification and authentication of sender and receiver	Spoofing; Tampering; Repudiation; Information Disclosure; Denial of Service; Elevation of privilege	Insider (accidental)	Without any properate security authorization techniques in place the attacker is able to steal data or abuse integrity, if identification measures between system communication is not verified; Lack of cryptographic measures for data in transit and data in rest; Ledgers may be susceptible to DoS or transaction spamming if proper identity management is not set for private blockchain; Component/information traceability throughout the entire life cycle of the system to assure efficient and secure processes	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Data leak; Financial loss; Reputation damage	2	4	8	Information can lose its integrity when unauthorised changes are possible	To ensure informations integrity cryptographic, authentication and security measures have to be in the correct place to prevent unwanted modifications
THR13	Attacks against crypto wallets	Spoofing; Tampering; Information Disclosure; Elevation of privilege	Insider (malicious or accidental); Malicious hacker	Reverse proxy phishing; Cryptojacking; Dusting; Clipping; Spear phishing	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Data leak; Extorsion; Financial loss; Reputation damage	2	5	10	Crypto wallet security is becoming a major priority as hackers tactics evolve, it is best to take all standard wallet protection measures when dealing in crypto.	Follow best practises for crypto wallet protection: 2FA; no clipping; avoid reusing and simple passwords etc.
THR14	Governmental and legal changes/ unexpected regulations	Denial of Service	Force majeure	Stricter regulations regarding privacy, like GDPR, have placed more pressure on blockchain apps to ensure data compliance. Due to the fast changing regulations and at the moment it is not clear how the blockchain will be regulated at the end, the Supplain Team may not and can not be aware of all applicable laws and regulation, the change in regulations or new regulation that may paralyze the service	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Financial loss; Service not available; End of business	3	5	15	Due its volatile nature the cyprotmarket is very risky way to invest money. More regulated and lawful environment can give the investors confidence to make larger investments but at the same time can seriously damage the service of exicting blockchain apps.	Build a compliance program. This enables the possibility being up to date with all laws and regulations.

THR15	Fraudulent web sites pretending to distribute Supplain protocol	Spoofing; Tampering; Information Disclosure; Elevation of privilege	Malicious hacker; ATP	Malicious software is distributed via fraudulent; websites pretending to be Supplain.io; Gain access rights and user data; attempt credit card fraud; Users in use case 2 can download the false version of Supplain node compromising the whole organisation and give access for malicious actor	DF20-DF40; DF45- DF50; DEV1- DEV13	Client-Private Chain- Relay Chain	Financial loss; Reputation damage; Data leak;	2	5	10	If no actions are taken to limit the distribution of fraudulent and false information under Supplain name, the reputation of the service may suffer and may lead to the end of business	Create a motivation program so people will be interested to search for fraudulent info and inform
Attacks against source code												
THR16	Rust programming language vulnerabilities	Spoofing; Tampering; Repudiation;I Information Disclosure; Denial of Service; Elevation of privilege	Supplier (accidental)	Source code vulnerabilities makes possible remote code execution, ransomware, overflow and bypassing	DF20-DF40; DF45- DF50; DEV1- DEV13	It is possible to bypass fraudulent data to end users	Service interruptions; Financial loss; Reputation damage; Data leak;	3	5	15	Supplain aims to produce scalable open source framework where developers themselves can make adjustments according to business need. While passing the code audits and multiple test before launching the service can prevent malicious activities, but it can not protect it against vulnerabilities detecting on later stages and Zero-Trust. For Rust there are found 22 vulnerabilities since 2018 [29] and successful ransomware distribution in 2022 [30]	To avoid serious damage to reputation Supplain needs to keep maintaining the source code and assuring the initial node needed to access Relay Chain is secure and verified
THR17	Software Vulnerabilities or Errors / bugs	Spoofing; Tampering; Information Disclosure; Denial of Service	Supplier (accidental) ; Insider (accidental) ; Malicious hacker	Every developer makes errors, some of them may lead to result of unexpected outcome, when the algorithm does not turn out the expected value. The programmers dont have sufficient training or knowledge to follow secure programming principles. No or insufficient software testing	DF20-DF40; DF45- DF50; DEV1- DEV13	Bypassing security controls and remote execution; move on to client side	Losing of trust; Service interruptions; Financial loss; Reputation damage; Data leak;	3	5	15	Keeping the product desirable for the market requires constant improvement like updating the current system or adding new features.	Activate bug bounty program or adopt Polkadot's practise to organize hackathons

THR18	Protocol updates	Denial of Service	System Failure; Insider (accidental)	Often the protocol updates cannot roll seamlessly due to the presence of a software bug, or inconsistencies in the blocks of a particular user that may compel the entire blockchain to split unnecessarily	DEV1-DEV13	None	Service interruptions; Financial loss; Reputation damage; Data leak;	2	5	10	Since the roll back activities are very heavy weighted in the blockchain any update has to be tested throughout	Have a team who is responsible for continuous test and collect data for statistics to make right decisions
THR19	No secure feedback channel by design	Information disclosure; Elevation of privilege	Insider (accidental)	Evaluate threats applicable for data spoofing and tampering in secure feedback communication channelHow users can give feedback about usage, design flaws, code bugs or security and privacy issues. Lack of established monitooring mechanisms for security breaches; Lack of procedures for reporting security weaknesses	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Service interruptions; Financial loss; Reputation damage; Data leak;	2	5	10	As identified previously in many successful attacks towards blockchain protocols continuous development is needed to keep the service secure and assure it remains that way. All stakeholders connected to private parachain are interested to use a secure service.	Establish secure feedback channel; Evaluate feedback; Collect data for statistics
Attacks against privacy												
THR20	Abuse of Personal Data	Information disclosure;	Insider (accid. or malicious); Supplier (accid. or malicious)	Hashed personal data is still personal data; it is not possible to erase, destruct or anonymize the data as defined by GDPR. Data retrieval is a mentioned problem due to inefficiency. Both retrieval by full node or lightweight mode present issues with efficient data retrieval and privacy, respectively	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Financial loss; Reputation damage;	3	3	9	Once a transaction is written to the blockchain, it cannot be deleted or cancelled, the blockchain can only be appended to, and existing data remains unaltered.	Have the PII stored on client side. Digital Twin protocol will transmit the personal data. NB! The client has to be GDPR compliant
THR21	Disclosure of Sensitive Information or privacy loss	Information disclosure;	Insider (accidental or malicious); Supplier (accidental or malicious)	Supply chain users might not want the total transparency provided by a blockchain assuring the business secret remains secret. Privacy leakage is a known issue due to its nature attackers can link the transactions back to a common user.	DF20-DF40; DF45- DF50; DEV1-DEV13	None	Financial loss; Reputation damage;	2	3	6	The identification component and the functionality of Digital Twin may be the solutions to assure keeping the information secret, but due to possible attacks vectors to these service an the immaturity of blockchain services there is still a risk that the confidentiality and privacy can not be 100% guaranteed	

Human error												
THR22	Malicious collators bribe validators	Spoofing; Tampering; Repudiation;	Insider (malicious)	Validators assigned to each parachain will wait until nodes the attacker controls are assigned to the parachain or easier method malicious collators bribe validators so that they validate an invalid blob [9]	DF20-DF40; DF45- DF50; DEV1- DEV13	None	Losing of trust; Service interruptions; Financial loss; Reputation damage; Data leak;	2	4	8	The security argument says here that validator need to wait around 50 years for the attacker controlled node, so the attack is not possible. In the real life Polkadot example- since the attack does not have any risk, the collators can bribe parachain validators with their stake and parachain validators validate an invalid blob[31]	
THR23	No incentive for Fishermen to keep continuously checking	Spoofing; Tampering; Repudiation;	Insider (accidental or malicious)	If there was no compromised block for a long time, then fishermen would stop to pursue their work since they do not receive any rewards which makes their business unprofitable. At the moment there is no incentive block for Fishermen, it is considering it as future work by Polkadot. This may lead to invalid block. [9]	DF20-DF40; DF45- DF50; DEV1- DEV13	None	Losing of trust; Service interruptions; Financial loss; Reputation damage; Data leak;	2	3	6	Reverting back invalid requires to roll back the state of ALL parachains and all transactions. This poses tremendous uncertainty and insecurity to the network. The alternative is to do not roll back the state and the invalid block from one of the parachains could then corrupt the other connected parachains.[31]	It can be combined with Nominators activity, but this problem will need solution before the community grows very large
THR24	Lack of effective change control / change management	Tampering; Repudiation	Insider (accidental)	Supplain admins need to assure the node available in Github is kept up to date and verified without any possibility to somehow damage or harm clients systems.	DEV1- DEV13	None	Data leak; Extorsion; Financial loss; Reputation damage	2	3	6	Due to the human error it is possible for the risk to occur, but it can be prevented by automated controls and tests.	

THR25	Identity theft	Spoofing; Tampering	Malicious hacker	Gaining access or authorization thru phishing techniques. Possible attack vectors: user accounts; administrative accounts; poor network set up; poor security of crypto wallets	DF1-DF50; DEV1-13	None	Reputation damage; Extorsion; Data tampering; Financial loss	2	5	10	Due to the immutable nature anyone who has access to supply chain can maliciously take advantage of the system	Follow best practises for access management: enforce 2FA; no plaintext password storing or sharing; avoid reusing and simple passwords etc.
THR26	Loss of cyptographic keys	Tampering; Information Disclosure; Elevation of Priviledges	Insider (accidental)	If any user loses the set of public/private keys, they are stolen, or the user expires, then those blocks cannot be retrieved; private blockchains' security depends on cryptographic keys for encryption of the information to ensure maximum security, however, if these keys are not handled properly, the security can get compromised	DF45- DF50	None	Data leak; Financial Loss; Reputation damage	2	4	8	This private key is the digital identity to the cryptocurrency market and anyone who gets hold of this can perform fraudulent transactions, steal crypto coins or pretend to be validator/nominator/fishermen for the relay chain. Thats why the risk is managed as high	Raise public awareness how to securely store set of public/private keys
THR27	The validator may act maliciously	Spoofing; Tampering; Information Disclosure; Elevation of privilege	Insider (accidental or malicious)	If a validator set is compromised, they may create and propose a block which though valid, takes an inordinate amount of time to execute and validate. It may be also the case for validators unintentional failures. Cases where blame cannot be precisely allotted (being part of an ineffective group).	DF45- DF50	None	Data leak; Financial Loss; Reputation damage	2	4	8	It may become a problem is the rewards are set as to be too high. Due the long time it takes to find out the reason or who to blame this risk is managed as high	The validators reward has to be sufficiently large to make verification worthwhile for the network, yet not so large as to offset the costs of fronting a well-financed, well-orchestrated industrial-level” criminal hacking attack on some unlucky validator to force misbehaviour. [9]