Supplain - A Vision For Distributed, Privacy-Preserving Data Exchange

1. Preface

This white paper is a technical summary of a new blockchain ecosystem and justifications for specific ideas proposed. It builds on the existing technologies, presenting new concepts that would make it possible to introduce them in industries traditionally resistant to blockchain technologies.

It is not intended to be a complete specification or the final design. It is not intended to cover non-core aspects of the framework such as APIs, bindings, languages, and usage. This is notably experimental, where the specific parameters are likely to change. It will evolve in collaboration with the community's ideas and critiques. There is scope to completely redevelop and pivot as necessary.

This document includes a core description of the protocol. We anticipate that this will be a starting point for the initial proof of concept. The final version will be refined according to the market's changing conditions.

2. Introduction

In this white paper, we analyse the requirements of a decentralised and open framework that would standardise the method of data exchange and enable autonomous business execution across any supply chain.

We believe that every piece of digital data has a rightful owner (or owners) who should have complete control over the management of this data in the most resource-efficient method.

However, the existing systems do not support explicit data ownership models, rather relying on copying data to disconnected servers that exchange information via custom integrations, APIs, or other methods. This model is flawed as it creates data security risks while being expensive to maintain. Moreover, it makes it challenging to trace, track and trust the counterparties, as there is no transparent control mechanism. We propose a framework for more clear data ownership and an open, interoperable ecosystem for trustless yet scalable data exchange within real-world commerce.

To achieve this, we propose a blockchain-based solution primarily derived from Polkadot's concept of parachains - multiple interoperable yet independent blockchains pooling their resources for security and consensus.

The major advancement for Supplain blockchain stems from significant improvements required for a privacy-preserving, regulatorily compliant solution suitable for handling sensitive personal and business information.

It seems clear, therefore, that one reasonable direction to explore as a route to a distributed, privacy-preserving compute platform is to seek a better method for mixing the concepts for public and private blockchains. This is the strategy that Supplain adopts to preserve both privacy and interoperability.

3. Summary

Supplain is a distributed, privacy-preserving blockchain. Unlike previous blockchain implementations, which have focused on staying thoroughly permissionless or have exchanged transparency for access control, Supplain is designed to revise the privacy-preserving aspects of blockchains.

Supplain does this through a consensus mechanism for multiple co-operating blockchains derived from Polkadot's heterogeneous multichain model. The primary difference in Supplain's model is that the involved parties can create both public and private parallel sub-chains (or parachains). As a result, those that want to utilise the blockchain technology while maintaining control over their data and the parties that have access to it can still reap the benefits of the Supplain network's interoperable nature through the cross-chain services.

While implementing such a model, we propose introducing two other fundamental concepts:

- 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.

Keeping the overall infrastructure equivalent to Polkadot's network, we consider Supplain to stay 'scalable.' 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.

4. Philosophy of Supplain

Supplain should provide an interoperable open network for data exchange that helps maintain data privacy, as long as no dispute resolution involving third parties is needed, to support real-world commerce needs. By providing high-level security and simple identity verification, Supplain can accelerate the adoption of blockchain technologies by industry users.

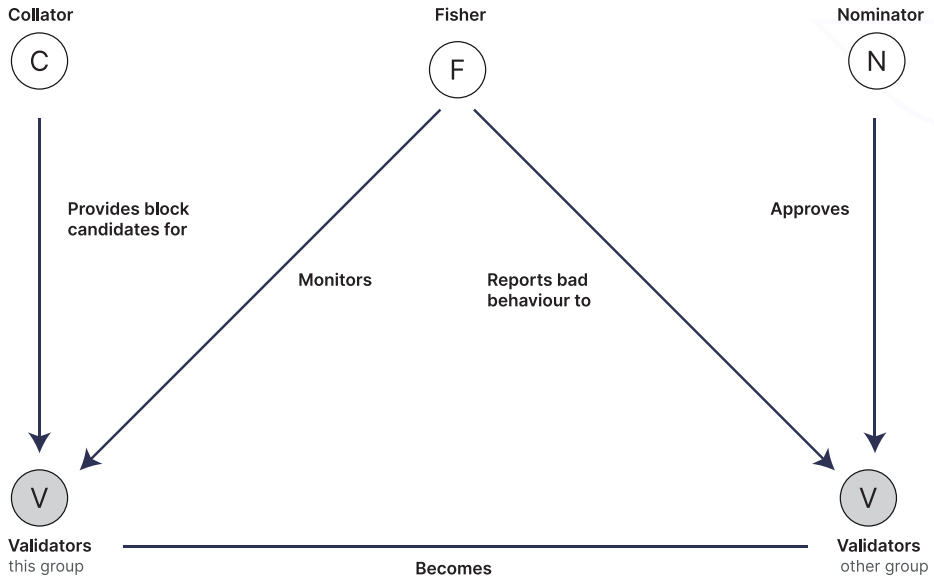
To manage chain upgrades, Supplain will support an on-chain governance structure to manage chain upgrades, mixed with an executive branch elected by the token holders. This executive branch would prepare votes and execute the results, while the token holders would set the primary direction.

Supplain's primary principles according to which all assessments are made, include:

- Minimalism: Supplain should have as little functionality as possible with additional complexity introduced through the parachains or applications built on Supplain.
- Longevity: Supplain should favour designs that support stability, interoperability, and decentralisation to create an everlasting ecosystem.
- Privacy-preserving: Supplain should constantly balance between its open nature and privacy controls, ensuring that the network remains trustless.

5. Participation in Supplain

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.



5.1. Validators

A validator is responsible for sealing new blocks on the Supplain network. Becoming a validator entails depositing a sufficiently high bond; however, other bonded parties may nominate one or more validators to act for them. Therefore the validator does not have to provide the entire value of the bond alone.

A validator must run a Relay Chain node with high availability and bandwidth. At each block, the node must be ready to ratify a new block on a nominated parachain. This process involves receiving, validating and republishing candidate blocks at an unpredictable rate. Since the validator cannot reasonably be expected to maintain a fully-synchronised database of all parachains, it is expected that the validator will nominate the task of devising a suggested new parachain block to a third party, known as a collator.

Once all new parachain blocks have adequately been ratified by their appointed validator subgroups, validators must then ratify the Relay Chain block itself. This involves updating the state of the transaction queues, processing the transactions of the ratified Relay Chain transaction set and ratifying the final block, including the final parachain changes.

A validator not fulfilling their duty by going offline without advanced notice or otherwise misbehaving in block validation is punished. For initial, unintentional failures, this is through withholding the validator's reward. Repeated failures result in the reduction of their security bond. Provably malicious actions such as double-signing or conspiring to provide an invalid block result in the loss of the entire bond.

5.2. Nominators

A nominator is a stake-holding party who contributes to the security bond of a validator.
Nominators participate in the block ratifying process without running their own validation node. Instead, they deposit their bond in support of a trusted validator, with whom they share the validation rewards and penalties.

5.3. Collators

A collator assists validators in producing valid parachain blocks by maintaining a "full-node" for a particular parachain. Thus, ensuring that validators would not have to maintain a fully-synchronised database of all parachains.

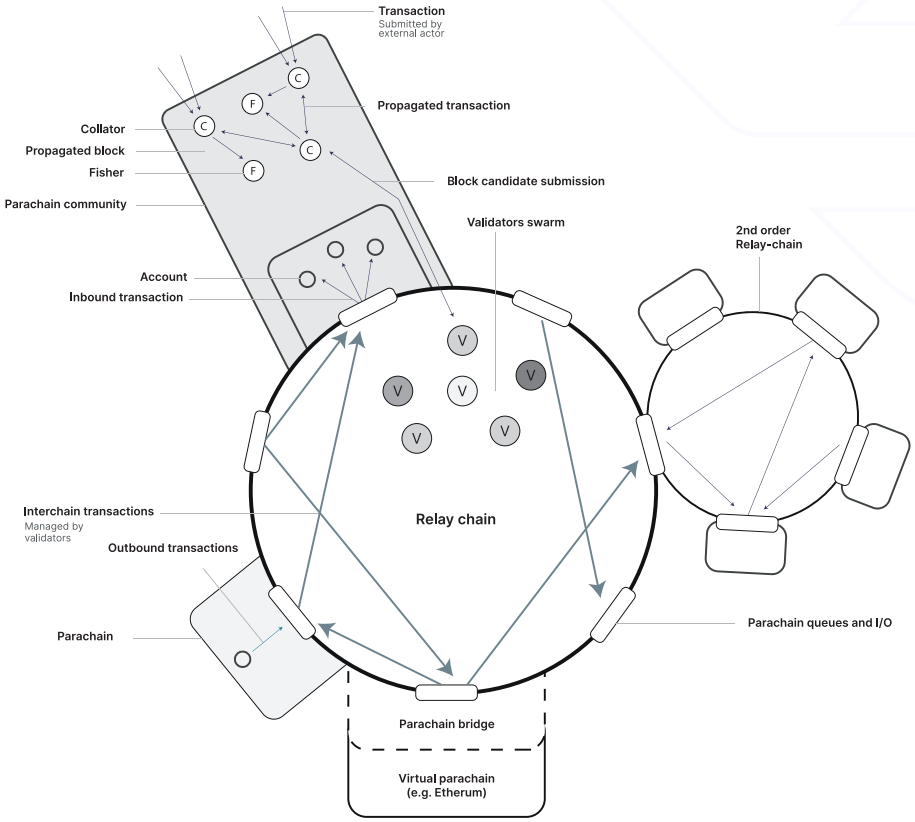
In the case of Supplain's private parachains, the majority (but possibly all), private parachain participants will become collators for their chains. Since all data within private parachains will remain secret, outside parties cannot fulfil this role.

5.4. Fishers

A fisher is responsible for cross-checking collators' work and providing an additional layer of security. They are independent "bounty hunters" motivated by a large one-off reward. Precisely due to the existence of fishers, we expect misbehaviour events to seldomly occur, and when they do, only due to the bonded party being careless with private key security rather than through malicious intent.

Fishers get their reward through timely proof that at least one bonded party acted illegally. Illegal actions include signing two blocks, each with the same ratified parent or, in the case of parachains, helping ratify an invalid block. The base reward for providing a single validator's illegally signed message is minimal to prevent over-rewarding or the compromise and illicit use of a session's secret key. This reward increases asymptotically as more corroborating illegal signatures from other validators are provided implying a genuine attack.

6. Design Overview



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. 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.

6.1. Consensus

Supplain will be designed as a fully open and public network that could operate without any particular organisation or trusted authority. Therefore, we will utilise a Proof-of-Stake mechanism to determine the network's validators and their incentive systems.

We expect that most parachains will use a Proof-of-Authority mechanism to reach consensus over a set of mutually agreed valid blocks. The private parachain authorities will also act as collators and fishers for their own private parachains. The final consensus would still be delegated to the main Relay Chains' validators.

6.2. Staking

Supplain will introduce its own token to measure how much "stake" any particular account has. These tokens will be used to elect the validators through a Nominated Proof-of-Stake (NPoS) scheme.

Incentivisation will primarily happen through sharing the transaction fees among the token holders that have taken a role in the consensus mechanism. The network could also introduce a token base

expansion mechanism (up to 100% per year, though more likely around 10%) to encourage more token holders to stake their tokens.

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.

6.3. Parachains

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.

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

6.3.1. Private Parachains

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 normal parachains except that private parachain authorities will act as Collators and Fishers for their own private parachain. Still, private parachain members need to be willing to publicise their dispute details should dispute resolution otherwise fail.

In case of agreement between the parties for their private parachains state transitions, they need not reveal any transaction details to the Relay Chain Validators. 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.

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.

6.4. Digital Twins

Supplain introduces the Digital Twin smart contract interface, a new form of digital ledger for record-keeping and data exchange within parachains.

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.

- Firstly, 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.
- Secondly, 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.

6.5. Interchain Communication

Like Polkadot, Supplain is a multi-chain that allows parachains to have varying levels of information channelled between them. In reality, this means that transactions executed in one parachain can initiate new transactions in a second parachain or the Relay Chain.

Interchain transactions are resolved using a simple queuing mechanism based around a Merkle tree to ensure fidelity. It is the task of the Relay Chain maintainers 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.

There will also be mechanisms to prevent a parachain from spamming another parachain with transactions.

6.6. Supplain and Other networks

There is an opportunity for Supplain to be interoperable with most other networks in a similar manner to Ethereum. In short, we expect validators to sign Supplain's transactions and feed them to other networks where they can be interpreted and enacted by a transaction-forwarding contract. In the other direction, we foresee the usage of specially formatted logs coming from a "break-out contract" to allow a swift verification that a specific message should be forwarded.

7. Protocol in Depth

This section describes additional concepts not used by Polkadot.

7.1. Relay Chain Requirements

Supplain's Relay Chain will likely be similar to Polkadot with contracts not deployable through transactions, a flat transaction fee applied in all cases and there is a unique functionality that supports listed contracts.

There are notable differences, though. Standardising the method of data exchange and enabling autonomous business execution across any supply chain comes with particular requirements, including the following:

7.1.1. Identity

For most use cases, the Supplain network will be used by real-world companies conducting real-world business with real-world regulatory, taxation, and compliance concerns. Therefore, participating parties will be legal entities who should be identified with the best certainty available given the market at hand, relying on legally binding identification such as the EU EIDAS scheme where possible.

We propose building support for the W3C Decentralised Identifiers (DIDs) at a core level for handling key

management, delegation, and other identity-related concerns. Where possible, the Supplain network, any services, and smart contracts running on it should rely on DID identifiers and their dynamic mappings to participants' accounts' cryptographic keys rather than fixed keys. This allows for key rotation, replacement, invalidation, and delegation as required.

Any real-world identities related to these DIDs, as attested to by either regulatory parties or a participating identification service, shall be represented as W3C Verifiable Credentials. These credentials shall be anchored along with the aforementioned DID identifiers to be presented to counterparties as required.

7.1.2. Programmability

The Supplain network users need flexibility in representing complex real-world processes and digital business relationships. For example, different executors can vary in pricing, conditions, and dispute settlement processes. The Supplain ecosystem should be flexible in expressing these relationships by companies with varying unique selling points.

Therefore, we propose that Supplain support a programming language agnostic Smart Contracts mode. In this regard, a WebAssembly (wasm) based execution environment like that supported by Polkadot's Substrate Blockchain Framework is the most appropriate for flexibility in choice for each party.

7.1.3. Proofs and attestations

Real-world companies and their private customers should be able to prove various facts required of them by third parties, regulatory or otherwise.

- Where possible, the system should allow parties to extract Zero-Knowledge Proofs of various facts from different parties' private parachains, which third parties can verify as relaying back to the public identity of the businesses in question.
- Where not possible, the system should provide a standardised smart contract interface for obtaining digitally signed attestations of said facts by the counterparty.

Since the underlying blockchain holding this data is private, such attestations must rely on the counterparty's publicly available identity and authority rather than being verified publicly.

7.1.4. Privacy

Privacy is crucial for most parties participating in the Supplain network.

Real-world companies do not want to expose their sales data, business relationships, or other sensitive business information to their competitors. In addition, private customer data must always be protected.

Therefore, in addition to public data and services, parties on the Supplain network must be able to keep details private between themselves, only revealing data to third parties as needed and with the owners' explicit consent. Only the counterparties of specific business transactions should ever be in possession of their data, and no trusted third parties should be required by the system's design.

While fully public distributed ledgers, where all transactions, smart contracts, and related data are visible to anyone on the network, are mature today, further integrations are required for privacy-preserving systems. Prior work in this field includes Splinter's private circuits, R3 Corda's shared facts, and privacy-preserving versions of Ethereum state channels and rollups.

A core challenge for Supplain is providing a unified open network where identities can be verified, services advertised, and money transacted between parties while keeping business details private as long as no dispute resolution involving third parties is needed.

7.1.5. Security

The Supplain network's goal is to guarantee data synchronisation, non-repudiation, and strict privacy controls between parties. This implies splitting the network's underlying state into public and numerous private partitions or shards, all of which should stay consistent and offer an equal level of security, or more specifically, immutability and non-repudiation.

7.1.6. Settlement

In addition to technical compatibility, the end goal of Supplain is to digitise and automate as much of the real-world business process as possible. This involves settlement for services provided as part of the smart contract business logic, where the smart contracts should determine the total amount to be paid, accounting for any irregularities, and settling the payment instantly once such determinations have been finalised.

Businesses cannot be expected to settle in a floating token; instead, they need access to and the ability to quickly withdraw from the network a widely supported stable coin. This means the system must provide allowances for easy cross-chain compatibility and provide a stable coin and bridges to standard public networks.

7.1.7. Snapshots

With Supplain's privacy goal in mind, while implementing private circuits for counterparties, we must still allow for the high availability of this private data exchange between parties. Bigger institutional participants can be expected to ensure their own data availability; however, smaller participants cannot be expected to be online permanently.

Third parties may be trusted with access to specific circuits to ensure long-term storage and availability, but only at the explicit consent of private parachain participants.

As one concept, we could introduce Digital Twin' Snapshots that enable end-users that do not operate network nodes to make copies of the Digital Twins and the data they have access to. Those Snapshots could keep their existence even after terminating the parachain.

7.2. Private Parachain Participants

The primary idea for private parachains is to create interoperable ecosystems for trustless yet scalable

data exchanges within real-world commerce transactions. There are three primary roles in any real-world commerce transaction in most such transactions: initiator, executor, and recipient.

- In particular circumstances, the intermediate role may be covered by either one of the other involved parties, or multiple executors can play a crucial role within individual transactions.

It is important to note that the roles of involved parties could change depending on the parachain. Once an initiator, the party could be a recipient in another parachain. However, there is always a clear distinction between the roles of the involved parties.

7.2.1. Initiators

An initiator is the original data owner that starts each private parachain and most transactions. The initiator's typical objective is to transfer particular data or physical goods to recipients, using the assistance of executors.

When using the services of executors, the initiator expects to only disclose the essential information to the executors. At the same time, the initiator requires a complete overview of the current state of the transaction throughout the process.

- The initiator may use a diverse pool of executors for different transactions depending on the terms and economic conditions. For the most part, an initiator has pre-existing agreements with executors, but sometimes they still need to contract an agreement.

Generally, the initiator utilises the Digital Twin smart contract interfaces to exchange data between the executors and recipients.

7.2.2. Executors

An executor is the one who conducts transactions.

- A single transaction may involve multiple executors responsible for different parts of the same transaction.

The executor's objective is to perform as many transactions as possible at the lowest possible cost. To do this, the executor is ready to collaborate with other executors and can outsource tasks to them.

During the handling of the transaction, the executor receives only the necessary information from the initiator. At the same time, they need to give the initiator a complete overview of the current state of any transaction.

The executor may request additional information from the initiator during the transaction.

7.2.3. Recipients

A recipient is at the end of each transaction the one to whom the data or the physical goods should reach.

The recipient wants to get updates on the current status of each transaction from the initiator. In some cases, the recipient must have the option to change the course of the transaction under certain conditions.

In addition, after a successful transaction, the recipient wants to have access to historical information related to the transaction, using Snapshots to capture Digital Twin copies.
Ideally, the recipient also wants to have complete control over the private data about itself and only share it with other parties on a short-term and needs-based basis.

8. Conclusion

In conclusion, Supplain will create a privacy-preserving yet interoperable framework that would standardise the method of data exchange and enable autonomous business execution across any supply chain.

As evident from the numerous references above, Supplain's vision for a distributed supply chain ecosystem shares many challenges with Polkadot and its parachains, such as providing security and immutability to partitioned smart contract enabled blockchain. However, they differ in Supplain's focus on privacy preservation and regulatory compliance, which lead to different areas of focus for further development.

8.1. The Road Ahead

We believe in improving Polkadot's concept of parachains and their Substrate Blockchain Framework as a starting point for the Supplain network. From there, we will focus on several areas of development to satisfy the requirements laid out in this document. The following is a summation of the critical areas identified by the development team requiring detailed design and development.

8.1.1. Privacy

The first and most fundamental challenge is defining and implementing a scheme for private parachains joining the Relay Chains' consensus and security. This entails work on the private parachains block production and consensus algorithm, a mechanism for creating said parachains between parties trivially and on-demand joining/leaving of the Relay Chain as necessary.

Different scaling characteristics for many private blockchains with few participants instead of public and highly distributed ones also present both challenges and opportunities.

8.1.2. Identity

To enable legal entities to trust their contractual obligations via automated execution and enable the easy establishment of those relationships and their corresponding parachains, they need to know who their counterparty is. While the W3C DID and Verifiable Credentials specifications provide a data model and general guidelines for some implementation aspects, work is required to define a standardised interface for Supplain, provide a global DID registry parachain and establish methods for verifying and onboarding businesses.

8.1.3. Services

Services offered by executors must be discoverable on a public parachain so that private parachains may be established to use those services. These services need standardised interfaces along with reference implementations. Attestations, proofs, and compliance need standardised mechanisms in place.

8.1.4. Recipient access

Recipients, be they private persons or businesses, will require access to parts of relevant Digital Twins due to the partitioned nature of private parachains where only such parachains participants ever have access to detailed data. Therefore an authenticated method for discovering customer-related data across parachains is required.

9. Glossary

Bonding: A key concept in PoS networks that can translate as building up a strong "binding" relationship with a PoS network. You express your commitment to the network by locking a defined amount of your network token for a specific period.

Collator: Collators maintain a full node. Their primary task is to aggregate transactions into a block (or block candidates) and provide proofs for validators on the relay chain.

Consensus Mechanism: A method of authenticating and validating a value or transaction on a blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any blockchain or distributed ledger.

Cryptographic key: A cryptographic key is a string of data used to lock or unlock cryptographic functions, including authentication, authorisation and encryption. Cryptographic keys are grouped into cryptographic key types according to their functions.

Cryptographic signature: Also known as a digital signature, it is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Decentralised application (dApp): Decentralised applications are digital applications or programs that exist and run on a blockchain or peer-to-peer (P2P) network of computers instead of a single computer. DApps are outside the purview and control of a single authority. DApps can be developed for various purposes, including gaming, finance, technology integration, and social media.

Digital Twin: A new form of a digital ledger for record-keeping and data exchange.

Ethereum state channel: State channels refer to the process in which users transact with one another directly outside of the blockchain, or 'off-chain,' and greatly minimise their use of 'on-chain' operations. EU EIDAS scheme: Electronic Identification, Authentication and Trust Services. The eIDAS Regulation established the framework to ensure that electronic interactions between businesses are safer, faster and more efficient, no matter the European country they take place in.

Executor: Executors are the ones who conduct transactions on Supplain parachains.

Fisher: Fishers are responsible for cross-checking collators' work and providing an additional layer of security. Given a proof of authority consensus for private parachains, the fisher's role may only be required for public parachains.

Floating token: The opposite of a stablecoin, a token with a value that is subject to outside forces and therefore susceptible to higher levels of volatility.

Immutability: The ability for a blockchain ledger to remain a permanent, indelible, and unalterable history of transactions.

Initiator: Initiators are the original data owners that start each private parachain and most transactions. The initiator's typical objective is to transfer particular data or physical goods to recipients, using the assistance of executors.

Merkle tree hash: In cryptography and computer science, a hash tree or Merkle tree is a tree in which every "leaf" (node) is labelled with the cryptographic hash of a data block, and every node that is not a leaf (called a branch, inner node, or inode) is labelled with the cryptographic hash of the labels of its child nodes. A hash tree allows efficient and secure verification of the contents of a large data structure. A hash tree is a hash list and a hash chain generalisation.

Metadata: Higher-level data that describes or annotates a data set, like tags in a programming code that describe the hierarchical structure and the relationships among discrete pieces of data.

Nominated Proof of Stake: The process of selecting validators to be allowed to participate in the consensus protocol. NPoS is a variation of Proof-of-Stake and is used in Substrate-based Blockchains such as Kusama, Edgeware or Polkadot.

Nominator: One of two main actors who are involved in a blockchain network that uses the nominated proof-of-stake (NPoS) consensus algorithm, the other being validators.

In regular proof-of-stake (PoS) networks, the power of an entity mining or validating network transactions is solely reliant on the number of network tokens they hold. The more tokens of that network are held by the miner or validator, the more mining power they have. This same power is also used in other types of decision-making scenarios. It is popularly used in governance functions, with validators voting on proposals for the future development of the network, for example.

Parachain: A parachain is an application-specific data structure that is globally coherent and validatable by the validators of the Relay Chain. They take their name from the concept of parallelised chains that run parallel to the Relay Chain.

Polkadot: A network protocol that allows arbitrary data—not just tokens—to be transferred across blockchains. Polkadot is a true multi-chain application environment where things like cross-chain registries and cross-chain computation are possible.

Private Blockchain: Private blockchain is developed and maintained by a private organisation with authority over the mining process and consensus algorithm. The private organisation decides who can join the network and download the nodes.

Proof of Authority: An algorithm used with blockchains that deliver comparatively fast transactions through a consensus mechanism based on identity as a stake.

Proof of Stake: A blockchain consensus mechanism for processing transactions and creating new blocks in a blockchain. A consensus mechanism is a method for validating entries into a distributed database and keeping the database secure. In the case of cryptocurrency, the database is called a blockchain—so the consensus mechanism secures the blockchain.

Protocol: A set of rules governing the format of messages that are exchanged between computers.

Public Blockchain: In a public blockchain, anyone is free to join and participate in the core activities of the blockchain network. Anyone can read, write, and audit the ongoing activities on the public blockchain network, which helps a public blockchain maintain its self-governed nature. The public network operates on an incentivising scheme that encourages new participants to join and keep the network agile. Public blockchains offer a precious solution from the point of view of a truly decentralised, democratised, and authority-free operation.

R3 Corda's shared fact: "To establish the architecture for an open, enterprise-grade, shared platform for the immutable recording of financial events and execution of logic"
See: https://www.corda.net/blog/r3-corda-what-makes-it-different/

Recipient: A recipient is at the end of each transaction the one to whom the data or the physical goods should reach.

Relay Chain: The Relay Chain is the central chain used by the Supplain network.

Settlement: The act or state of settling a transaction.

Smart contract: A self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralised blockchain network. The code controls the execution, and transactions are trackable and irreversible.

Splinter's private circuit: Splinter is a privacy-focused platform for distributed applications that provides a blockchain-inspired networking environment for private communication and transactions between organisations.

Stablecoin: Any cryptocurrency designed to have a relatively stable price, typically through being pegged to a commodity or currency or having its supply regulated by an algorithm.

Staking: The process of locking up crypto holdings to obtain rewards or earn interest.

Substrate Blockchain Framework: A framework for building customised blockchains. These blockchains can be run entirely autonomously.

Supply Chain: The entire process of making and selling commercial goods, including every stage from the supply of materials and the manufacture of the goods through to their distribution and sale.

Timestamping: A timestamp is a sequence of characters or encoded information identifying when a specific event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second.
Transaction fees: Fees charged by the transaction facilitator.

Validation Rewards and Penalties: The act of giving or slashing tokens to a validator based on their completion of a task.

Validator: Also called a "blockchain verifier," validators are computers that maintain the blockchain's integrity by constantly computing the linkage from the first block to the last.
Decentralised Identifiers (DIDs): DIDs are a new type of identifier that enables verifiable, decentralised digital identity.

Zero-Knowledge Proof: An encryption scheme whereby one party (the prover) can prove the truth of specific information to another party (the verifier) without disclosing any additional information.