Concordium White Paper

An introduction to the features of the Concordium Platform

Concordium is a privacy-focused, public and permissionless blockchain architecture. This paper describes the Concordium Platform along with a range of novel features that allow individuals, businesses and public institutions to use permissionless blockchain technology in a way that is private, trusted, scalable and compliant with regulations.

The Concordium Platform is designed to be fast, secure and cost-effective. Concordium's innovative identity layer provides on-chain identity, compliance-centric transactions and enhanced privacy for users, while also allowing for the identity of network participants to be disclosed to authorities. Concordium's state-of-the-art BFT-style consensus protocol finalizes blocks shortly after they are produced, providing fast confirmation of transactions. Concordium has a standards-based smart contract core with multi-language support. Additionally, multiple different tokens are supported at the protocol level, which are minted and managed by independent token issuers. Concordium enables interoperability and communication between Concordium and other blockchains. The Concordium Platform also features a transparent incentive structure with cost-effective transactions and predictable fees.

An Introduction to Concordium
Version 1.13, February 2026

Table of Contents

Concordium: An Overview

Regulatory Compliance by Design

Concordium is designed to integrate with current financial and business systems that require knowledge of a user's identity. Through the development of unique protocol-level identity primitives, Concordium helps application developers, individuals and businesses build products that comply with local regulations, while retaining the benefits of a privacy-focused, public and permissionless blockchain.

By user, we mean any entity that holds an account on the Concordium Platform. These can be individuals or legal entities, such as businesses, and they require a valid form of identification to facilitate the off-chain identification process.

Both Privacy and Verification of the Identity of Users

Concordium's innovative identity layer provides a compliance-centric balance between privacy and accountability. A user's identity is private on-chain, however, this privacy can be revoked and their real-world identity disclosed in response to a valid request from a government authority via established legal channels. In a nutshell, selected *privacy guardians*—entities holding secret keys that can decrypt identifiers associated with every account—examine legal requests from authorities, and if approved, they work together with the identity providers to link user accounts with user identity information. From the user's perspective, privacy towards the general public is maintained and Concordium's identity layer can accommodate identity providers and privacy guardians based in different jurisdictions around the world. As such, the Concordium Platform offers a global, multi-jurisdictional solution to the adoption of blockchain technologies across regulatory regimes.

Fast Transactions at Scale

The Concordium Platform is designed to be fast enough, in terms of transactions per second and the time it takes to finalize a transaction, to meet the needs of business applications on a global scale. This is a major development compared to previous generations of blockchain technology.

Provable and Fast Finality

Concordium has developed its own Byzantine fault tolerance (BFT) style consensus protocol, which finalizes a block once the following block is validated. This means that a transaction on the Concordium Platform is confirmed and immutable within a short period of time. This is a major advantage over Nakamoto-style blockchains, where the finality of a block is only assumed after a large number of subsequent blocks have been produced.

Reliable Uptime

Concordium is designed for demanding business use cases with strict uptime requirements. Our consensus design ensures that the platform remains available and secure in the most adverse conditions. Blocks are correctly added and validated when less than 33% of all stake is controlled by malicious parties. And the safety of our consensus layer holds even under catastrophic failures to the network that causes messages to be delayed much longer than under normal conditions or to disappear. In such a situation, block production stops until communication is restored, then automatically picks up where it left off when the network conditions are restored.

High Throughput for Global Scale

Many real-world business applications of blockchain technology have high throughput requirements. To meet these needs, Concordium is developing novel scalability mechanisms that operate in tandem with our consensus layer and help enhance the growth of the entire ecosystem without sacrificing security or decentralization.

A Standards-based Smart Contract Core with Multi-Language Support

Concordium's core on-chain language is WebAssembly (Wasm), a portable, well-defined assembly-like language. Wasm is an internet standard that is gaining a lot of traction in recent years and is already supported in the major web browsers. Many programming languages can already be compiled to Wasm, which potentially allows us to support a large range of smart contract languages. Concordium uses Rust as our first high-level smart contract language, a safe language that also allows for low-level resource control.

A Single Native Token That Is Easy to Model

The native utility token of the Concordium Platform is called CCD (short for ConCorDium) and has the symbol Ͼ. It is the medium of incentivization that ensures network participants are rewarded for their efforts. CCD can be used for a variety of purposes, including for smart contract execution fees and for transactions between users.

Protocol-Level Tokens

Tokens may be minted and managed at the protocol level by independent token issuers—so-called protocol-level tokens (PLTs). PLT balances are managed natively and PLTs therefore benefit from the increased security and lower costs provided at the protocol level compared to the more common smart contract tokens. Issuing PLTs is currently gated—the Concordium Governance Committee approves PLT issuers individually—adding further security to PLTs.

Cost-Effective Transactions

To accommodate businesses that operate at scale, transactions on the Concordium Platform are designed to be cost-effective as well as fast. Low costs are a function of our proof-of-stake and finalization along with incentive mechanisms that prevent excessive charging.

Know Transaction Costs Ahead of Time

Transaction costs need to be understood ahead of time in order to build sustainable business models. Concordium uses an innovative price stability mechanism to ensure that transaction costs are fixed in real-world fiat terms despite potential volatility in the price of CCD on the open market.

Transparent Token Economics and Incentives

The economy and incentive structure within the Concordium Platform is transparent and easy to understand. All parameters that control the distribution of rewards, the CCD growth rate, and the pricing of transactions are publicly available. The Concordium Foundation will actively monitor and manage the health of the Concordium economy.

Responsible Governance on the Road to Decentralization

While the Concordium Foundation will act as a guarantor that the central principles of the Concordium Platform are adhered to, including privacy with accountability, key functions will be delegated to the Governance Committee. Over time the Governance Committee will evolve to have more responsibilities and governance will be decentralized across network participants.

Open Source

The Concordium Platform has been developed in a closed environment, but before the launch of Mainnet, the codebase for all central components of the Concordium Platform has been made open-source at https://github.com/Concordium.

Design Overview

The Concordium protocols can be divided into the following layers:

The **network layer** consists of a **peer-to-peer layer** and a **catchup layer.** The peer-to-peer layer consists of a public, permissionless, high-speed protocol for broadcasting messages to all available nodes. The catchup layer sits between the peer-to-peer layer and the consensus layer and ensures that nodes receive all relevant messages.

The **consensus layer** ensures agreement on all transactions and their order in the ledger. The consensus layer consists of a novel **proof-of-stake Byzantine fault tolerance (BFT) consensus protocol**, ConcordiumBFT. In future updates, Concordium's consensus layer will be augmented to another layer that improves scalability even further.

The **identity layer** defines how users' identities are processed and used during the creation of new accounts. It specifies how identity providers and privacy guardians interact with users to create identity objects and disclose the identity of users if validly ordered by a qualified authority.

The **execution layer** allows users to interact with the platform. Using the **API**, users can submit transactions, including, for example, transfers between user accounts and deployment and execution of smart contracts.

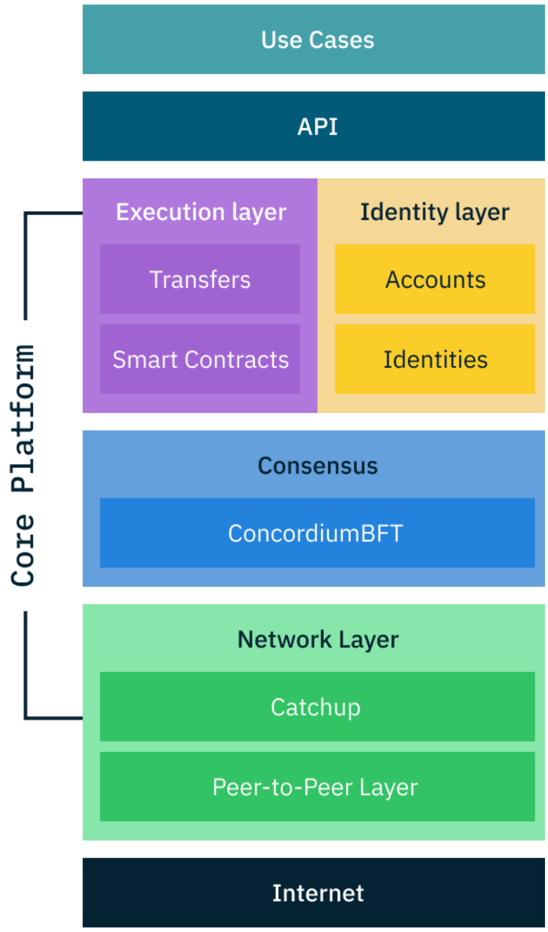

Figure 1: Overview of the Concordium stack.

Network Layer

The Concordium Platform is a distributed system. It consists of multiple nodes which maintain the blockchain by creating and validating blocks. The network layer establishes and manages the communication between nodes.

The network layer provides an abstract interface for communication such that protocols sitting on top of it do not have to know details of the actual communication protocol. For example, the interface for the consensus layer is a broadcast channel that allows parties to send messages to all other parties.

The network layer consists of the peer-to-peer layer that manages communication and the catchup layer that ensures all nodes, including those having been temporarily offline, receive all necessary messages.

Peer-to-Peer Layer

The peer-to-peer layer establishes a node's connection with peers and manages bi-directional communication between them. Its role can be divided into 3 parts:

1. To set up and maintain a node's presence on the network. This includes finding and managing peer nodes and collecting information about the network to ensure optimal peer-lists.
2. To manage one-to-one communication with each peer.
3. To broadcast messages, including transactions, blocks and validation messages, to all nodes in the network.

When a node starts up, the peer-to-peer layer is the first module that boots up. The node resolves a DNS record, decodes the list of bootstrap servers, connects and receives a list of peers. Initially, the bootstrap servers will be managed by the Concordium Foundation.

All communication on the peer-to-peer layer is done through network messages. For efficiency, network messages are serialized using FlatBuffer which enables fast implementation in various programming languages.

The peer-to-peer layer protocol is heavily secured against wiretapping by making use of the Verifiable Noise Protocol [Per16] and using formally verified encryption implementations. This enables a very robust guarantee against wiretapping and replay attacks on the peer-to-peer layer.

Any node can initiate a broadcast of a message, *m*, by sending *m* to its peers. When a peer receives *m* for the first time, it forwards *m* to all its peers. This ensures that the message propagates through the whole network. To avoid resending the same message multiple times, nodes buffer hashes of previously broadcast messages. A received message is then only forwarded to all peers if it is not already in the buffer.

Catch-up

After a node connects to a peer, it sends a catch-up request to the peer. This catch-up request includes a summary of the node's consensus status, including the last finalized block hash and round, the hashes of any subsequent blocks, the current round number, and a summary of what validators have signed in the current round. Based on the request, the peer can determine any blocks and signatures it has that the node is missing. The peer then sends these to the node in the appropriate order, followed by a catch-up response message with similar information to the catch-up request, but from the perspective of the peer. If the node is very far behind, the peer will limit the number of blocks it sends in response to a request. The catch-up response message allows the node to determine if it is now fully up-to-date with the peer, or if it needs to make further catch-up requests. The node attempts to catch-up with each of its peers one at a time in round-robin fashion until it is up-to-date with each of them. This distributes the burden across the network, and ensures the node does not receive redundant information from multiple peers.

The node also supports an out-of-band catch-up mechanism that is useful when a node is far behind the rest of the network - for instance, if it is joining for the first time. In this mechanism, the node downloads blocks from a web server before it ever connects to peers. These blocks are processed and verified just as if they were received on the peer-to-peer network, so there is no requirement to trust the server.

In the future, Concordium plans to add support for fast catch-up, allowing a node to start from the state of a recent block without executing all of the historic blocks. The node would check a proof that the block is correctly finalized on the chain, witnessed by each set of validators signing off on the next set, and the last set of validators in the chain signing off on the block. The block itself contains a hash of the block state, so that the node can verify that the block state it received correctly matches the block. The node can thus be sure it has correctly caught up with the chain without having to trust the source of the catch-up data.

Consensus Layer

Overview

Concordium uses a proof-of-stake based consensus called **ConcordiumBFT**. Here, BFT stands for "Byzantine fault tolerance", meaning the protocol is secure in a setting with so-called Byzantine corruptions, i.e., security is guaranteed even if some participants actively try to cheat. ConcordiumBFT is based on Jolteon [GKSSX22], which is a state-of-the-art variant of the HotStuff consensus protocol [YMRGA19]. Compared to Jolteon, ConcordiumBFT adds a proof-of-stake based leader election, and involves several optimizations, among others reducing the required communication in case of timeouts.

Proof of Stake and Delegation

The Concordium Platform uses a proof of stake (PoS) mechanism to ensure resource-efficient operation of the network along with enhanced security among participants. Users that hold CCD in their account can either become a validator, i.e., stake some of their CCD and run their own node, or delegate their CCD to existing validators. A delegator has two options: 1) they choose a specific validator and add their stake to that validator's pool—thus increasing that validator's chance of winning the lottery to produce a block—and share some of the rewards; 2) they choose Concordium's novel passive delegation feature, which provides the delegator with the rewards from sharing their stake between all validator pools, thus reducing the risk of delegating to a single pool that performs poorly, but the reward rate is fixed, and might be lower than for individual staking pools. Details of how rewards are calculated for validators, delegators to staking pools and passive delegators are given in the Section Tokenomics and On-chain Incentivization.

Leader Election

ConcordiumBFT proceeds in **rounds**, where each round is assigned a unique validator, called the **leader** for that round, to produce a new block and extend the chain. For every **epoch**, corresponding to one hour real time, all validators are fixed and the probability that a given validator is selected for a given round is proportional to that validator's pool's relative stake. The randomness for the leader election is derived from the so-called **leader-election nonce** for the current epoch. To compute the leader-election nonce for a given epoch, the **block nonces** of blocks in the previous epoch are hashed together with the current set of validators and their relative stake. The block nonce of a block is computed by the validator evaluating a verifiable random function (VRF) on the current round and the current leader-election nonce. Every validator has a secret key for the VRF, which guarantees that other validators can verify that the VRF was evaluated correctly, but prevents them from predicting the outcome beforehand. This design further ensures that block nonces for blocks in a given round are unique, to prevent malicious validators from manipulating the leader election.

The leader election uses a fixed relative stake for each validator per **pay day**, which is set to be 24 hours. Rewards for validators are distributed at the end of the pay day. Under normal network conditions, the stake of a validator for a pay day is determined one hour (one epoch) before the end of the previous pay day.

Block Production and Validation

ConcordiumBFT proceeds as a series of rounds, in which blocks are produced and agreed upon. In every round, ConcordiumBFT proceeds as follows: the validator elected as leader for the current round produces a new block, appends it to the chain, and distributes it over the network to the other validators. These then verify the validity of the block and sign it. Signatures from validators together holding at least ⅔ relative stake are aggregated into a quorum certificate, which certifies that block. Once such a quorum certificate is formed, the leader for the next round can produce the next block extending the certified block and so on. This process is summarized in Figure 2.

Note that the relative stake used to weigh the signatures is not taken relative to the total stake. Instead, a specific subset of the validators—those in the finalization committee—certify the validity of blocks. The relative stake of validators outside the committee is 0 and for those in the committee it is their pool stake relative to the total stake of the committee pools. The parameters are currently set so that the finalization committee is nearly equal to the entire set of validators, but for efficiency reasons the validators that do not have enough stake to open a pool—but run one nonetheless, because it was opened before the current threshold of 500’000 CCD was set—are not part of this committee. The current formula for determining the finalization committee is the top 40 validators (in terms of pool size) plus any validator in the top 1000 that has a pool with at least 0.005% of all stake in pools.

If the leader fails to produce a block (or produces an invalid block), the validators wait for 10 seconds (or more if there has been a sequence of timeouts) and then sign a timeout message for the current round. If validators with at least ⅔ relative stake sign such a timeout message, a timeout certificate is formed and the next leader can proceed, skipping the current round without a block.

Whenever there is a sequence of two certified blocks in two consecutive rounds and in the same epoch, the first of the two blocks is considered final. A final block is guaranteed to never be rolled back and always be part of the finalized chain. Hence, a transaction is confirmed once it is in a block followed by another certified block in the next round, so the average confirmation time roughly corresponds to 1.5 times the average block time (0.5 waiting for the next block to include the transaction plus waiting for the next block). Note that not all certified blocks are automatically finalized because during bad network conditions, the quorum certificate can be delayed beyond the timeout and there can be both a quorum certificate and a timeout certificate for the same round, allowing the next leader to skip a certified block using the timeout certificate. This cannot happen for finalized blocks.

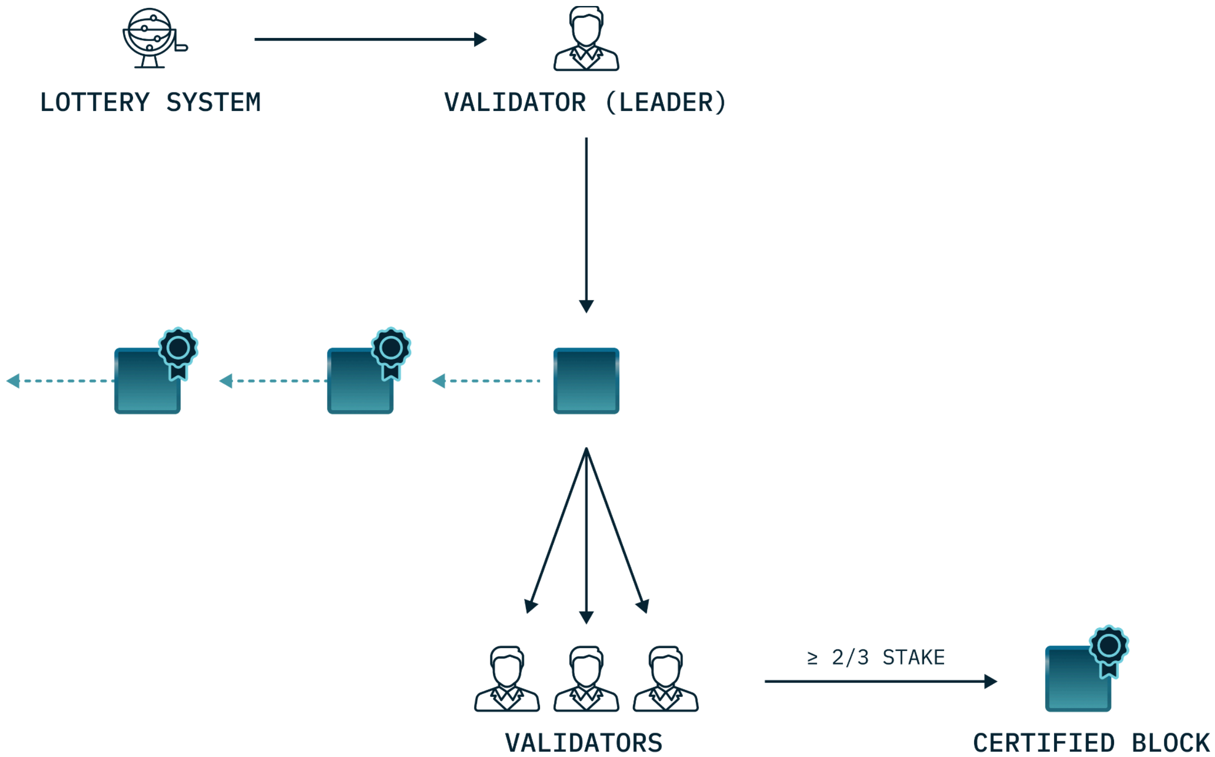

Figure 2: Overview of one ConcordiumBFT round.

Assumptions and Security Guarantees

ConcordiumBFT requires that less than ⅓ of the validators weighted by their relative stake are corrupted. Not being corrupted means being online and running the protocol as intended, without trying to cheat. Corrupted validators can behave arbitrarily without affecting the overall security—as long as the ⅓ threshold is not violated. However, they can slow down the protocol by sending invalid certificates or blocks, failing to produce valid blocks when it is their turn, or not including certain transactions in their blocks.

The protocol works in a so-called partially synchronous network, which means that security is guaranteed even if network messages among validators are arbitrarily delayed during certain periods of time. More precisely, this means that in all network conditions, finalized blocks are always guaranteed to be on a chain and forks can only occur among the unfinalized blocks. During sufficiently long periods of time with timely delivery of network messages, the protocol ensures that blocks keep being produced and finalized.

Scalability

Our state-of-the-art consensus protocol enables high transaction throughput and fast confirmations. To address scalability needs even further, an in-depth research phase is currently underway, investigating a number of different approaches. We discuss the most important ones below.

Parallelization

Rather significant speed-ups are achievable by concurrently running processes that do not conflict. We give three examples here below.

Block Preparation and Verification

In the version of ConcordiumBFT that is currently implemented, the leader for a round prepares a block and sends it around, after which the other validators verify it. When it is accepted, all validators move on to the next round, where a new leader is elected, prepares a new block, and sends it around, etc. This process can be optimized if the leader for the next round already prepares the next block while waiting for the block in the current round to be validated. In most cases the validation is successful, so the next block is already ready and can be immediately sent out when the validators progress to the next round.

Consensus and Block Execution

Currently, validators execute a block as part of the verification process of the consensus mechanism. But it is possible to decouple the consensus from the block execution. For example, one thread runs the consensus protocol to agree on the next set of transactions that are added to the chain, while another thread executes the transactions that have already been finalized. In this way, consensus and block execution are run concurrently.

Transaction Execution

Transactions are totally ordered by the chain, and the outcome depends on this order. However, in practice most transactions in the same block do not conflict and could be executed in parallel. A lot of research exists on how to do this, and how to resolve conflicts if they arise, which can be applied to the Concordium blockchain.

Sharding

The main goal of sharding is to overcome scalability issues. Without sharding, every node in the network has to process all transactions and execute all smart contracts. The basic idea of sharding is to parallelize execution by dividing the network into smaller components, called shards. Nodes are then assigned to different shards with separate account balances. Each shard essentially corresponds to a separate blockchain that is running almost independently of the other shards. This means that transactions on one shard are only processed by the nodes on that shard and, consequently, more transactions can be processed overall.

Full Sharding

One could consider a two-level sharded design with a very robust control chain and light weight shards, as described by David et al. [DMMNT22]. With this architecture, the control chain manages shards, provides a finalization service to the shards and gives a vehicle for cross-shard transactions. Each shard runs an individual blockchain and uses the control chain to coordinate the individual shards.

As shards allow for efficient reading of only the parts of this global ledger needed for a given application, this architecture makes it possible to create shards for specific purposes including private shards.

Lightweight Sharding

One can also consider lighter versions. For example, the Concordium blockchain currently has a lot of *data register* transactions, which do not require full consensus, so they can be split off into a shard that runs a weaker form of consensus—but much faster—protocol, e.g., the protocol by Sliwinski and

Wattenhofer [SW21]. The specialized shard would have a much higher throughput than the main chain, which has full consensus. At the same time, the number of transactions on the main chain would diminish as a lot of them are run on the specialized shard, freeing up capacity for more transactions.

Layer 2 Scaling

Layer 2 scaling techniques propose another approach to help scale the blockchain. These techniques—commonly referred to as “off-chain” scaling solutions—serve as a separate blockchain built on top of a base network like Concordium. A layer 2 protocol increases transaction speed by processing transactions off the chain while still ensuring similar security and decentralization guarantees as the base network.

The main layer 2 solutions are zero-knowledge (zk-) rollups and optimistic rollups. Zk-rollups are smart contracts that condense hundreds of transactions executed off-chain into one on-chain transaction and submit a short cryptographic proof on-chain that ensures the validity of the executed transactions. By storing only a small fraction of total data on-chain rather than all transaction data, zk-rollups make the base network cheaper and faster. As opposed to ZK-Rollups, optimistic rollups do not rely on cryptographic proofs. Instead, they are “optimistic” and assume transactions are valid. Only if the result of a rollup transaction gets challenged via a fraud-proof does the protocol correctly update the rollup’s state and penalizes the responsible rollup sender who included the invalid transactions. Concordium is investigating rollup scaling solutions as a support for the main chain.

Identity Layer

This section describes Concordium’s innovative identity layer that allows users to create a verifiable identity off-chain to ease compliance with relevant regulations, while also allowing that identity to be represented on-chain in a way that protects the user’s privacy. Concordium’s identity layer has been proven secure in [DGKOS21].

Previous blockchains have chosen extreme balances between user privacy and accountability. Some blockchains allow fully anonymous transactions without any accountability, making them vulnerable to illegal activity. Equally troubling is that while some blockchains do not provide true anonymity for transactions, allowing for transactions and accounts to be tracked, they offer no systematic way to discover the real-world identity of suspicious users.

Concordium offers a workable solution by providing transactional privacy for users, along with a mechanism that allows accountability to local regulations. This means that transactions are processed without exposing the identity of the sender or receiver. But when a suspicious transaction or set of transactions have been detected, the real-world identity of the user can be obtained by qualified authorities with the help of privacy guardians and identity providers. Moreover, if a specific real-world identity is the subject of an authorized investigation, privacy guardians and identity providers can help trace all accounts and transactions of that user.

Entities in the Identity Layer

This section provides an overview of the entities involved in the identity layer.

Account Holders

Account holders are individuals or companies who hold accounts on the blockchain. Before opening accounts on chain, account holders need to register with an identity provider.

Identity Providers

An **identity provider** is a person or organization that performs off-chain identification of users. For each identity issued for a user, the identity provider stores a record off-chain called an **identity object**, and the user gets a corresponding private part of the identity object, called **identity credential**, which is known only to the user.

The primary functions of an identity provider are to:

- Verify the identity of users;
- Issue user identity certificates to users;
- Create and store identity objects and relevant attributes for record-keeping purposes; and
- Participate in the identity disclosure process.

Information about the organizations that act as identity providers, such as their name, location or public key, is found in an on-chain registry. Initially, the registration of identity providers will be managed by the Concordium Foundation. Users must go through the identification process with a registered identity provider in order to open and operate an account on the Concordium Platform.

Privacy Guardians

A **privacy guardian** is a person or organization that is trusted by the Concordium Platform to help identify a user that owns an account should the need arise. Initially, privacy guardians will be appointed by the Concordium Foundation.

All accounts on the Concordium Platform are associated with a real-world identity, which is linked to an identity object stored by an identity provider. Identity objects are also linked to a set of privacy guardians. Privacy guardians play a critical role in revealing the real-world identity of a suspicious user by decrypting[1] the **unique user identifier** that is stored on-chain for each account. When a unique user identifier has been decrypted following service of an official order (as described below), it can be combined with information stored by the relevant identity provider to allow the qualified authorities to obtain the real-world identity of the user.

Processes

In this section we describe the processes related to the identity layer.

Account Holder Registration

Before an individual or entity can use the Concordium Platform, their real-world identity must be verified and recorded by an identity provider. To that end, the user—with the help of a government-issued identity document (e.g., passport)—must complete the process of creating user identity information via a purpose-built wallet or app.

[1] No PG can decrypt the user identifier on their own. The information is “secret shared”, and each PG returns their share to the authority, who combines them to get the identifier.

The identity provider verifies as part of this process that the attributes in the user identity information are valid for the user. If the verification is successful, the identity provider stores a record and provides the user with an identity certificate that can be used for creating accounts on the Concordium Platform. These certificates are valid for a given period and users can obtain new certificates in connection with updated identity verification by an identity provider.

Creating Accounts on the Concordium Platform

Once a user has acquired a user identity certificate from an identity provider, they can create accounts on the Concordium Platform. This is typically done using an app or wallet that guides users through the account creation process.

The private account keys are stored by the user, whereas public **account creation information** is published on the blockchain. The latter contains public account keys, and information about the identity provider and privacy guardians. While this allows the relevant privacy guardians and the identity provider, when working together, to link the account to the user, the account creation information does not allow other parties or any single party to identify the user. Further, accounts created with the same user identity certificate cannot be publicly linked.

Multi-user Accounts on the Concordium Platform

The Concordium Platform also allows users to create jointly owned accounts. For example, three users can have a joint account where two of them are needed to authorize a transaction. The total number of users and the authorization threshold can be configured freely by the users. To create a multi-user account, one user creates a normal account and the other users generate account credentials that can then be added to the account by the initial owner. All added credentials contain identity information on the users, which, similar to a normal account, allows the relevant privacy guardians and the identity provider, when working together, to link the account to the users.

Identity Disclosure

The identity of a user can only be revealed to a qualified authority as part of a valid legal process. A **qualified authority** is a governmental body that has the authority to act in a relevant jurisdiction. For example, a local police force, a local court or an investigatory division of a local authority that regulates financial conduct may have authority to act in their relevant jurisdictions. These authorities are qualified to begin the process of disclosing the identity of a user when they proceed through established legal channels and make a formal request. The outcome of such a request is likely to be that a qualified authority obtains an **official order**, which may be in the form of a warrant, court order, or similar instrument. Only after a qualified authority validly serves an official order upon the relevant privacy guardians and identity provider, can the real-world identity of a user be revealed and only to the extent set out in the order.

Concordium's identity layer is flexible and sensitive to the evolving nature of financial regulation and its impact on the blockchain space. Where new legislation or rules emerge, for instance the application of the so-called "travel rule" to blockchain transactions, the Concordium identity framework offers a compliance-centric solution that can be tailored to specific business needs.

After the authorities have identified an on-chain transaction or account they would like to investigate in order to reveal the real-world identity of a user, the following process must be followed.

- The qualified authority must identify the privacy guardians and identity provider associated with the account under investigation and present them with an official order. This information is available on-chain as part of the account creation data.
- Per the terms of the official order, the privacy guardians will extract parts of[2] the unique user identifier for the user by inspecting and decrypting the available on-chain data.
- The qualified authority can now combine the parts received from the privacy guardians to reconstruct the unique user identifier.
- With this unique user identifier, the qualified authority can work with the relevant identity provider to retrieve the real-world identity of the user.

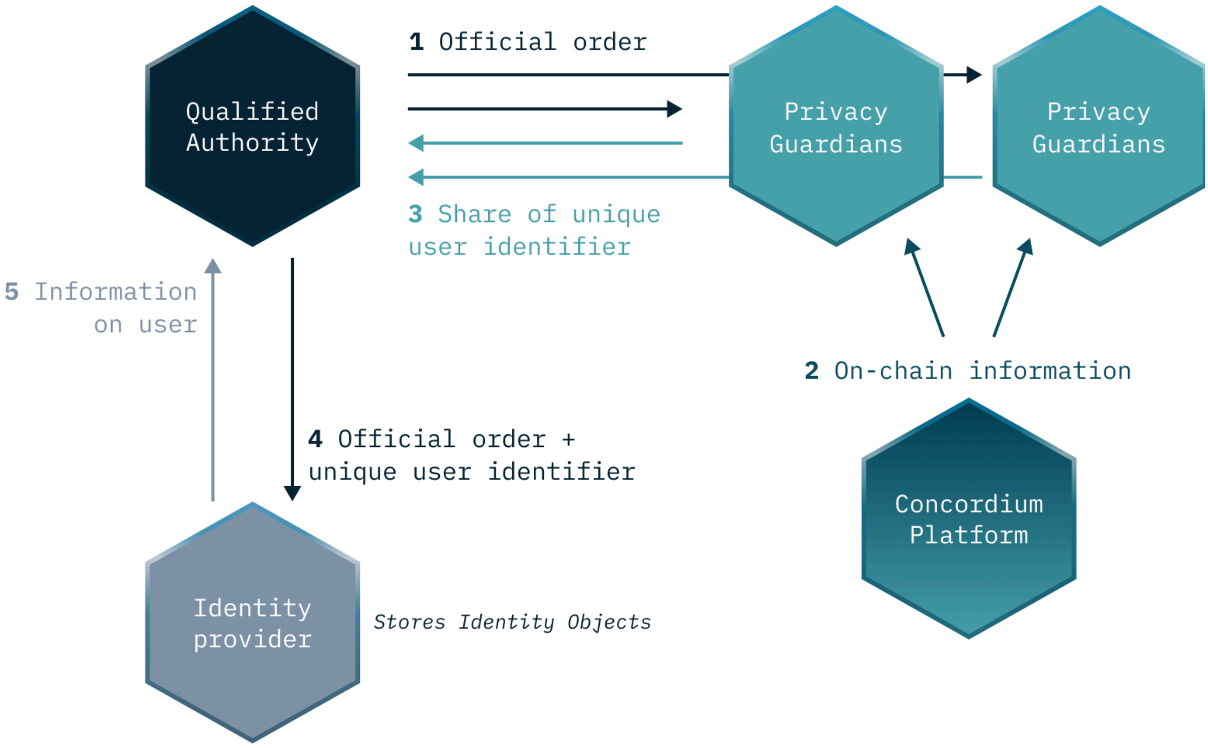

Figure 3: The identity disclosure process.

If required and per an official order, all accounts and transactions related to a specific user can be uncovered in a similar process.

It is important to note that this process intends to dovetail into contemporary legal systems that have established checks, balances and controls to prevent overreach by qualified authorities. It also provides that a user can create accounts for which neither identity providers nor privacy guardians acting alone can reveal an on-chain user's real-world identity on their own.

Proving Statements On Identity Attributes

Concordium wallet allows account holders to store and manage their attributes that have been issued by identity providers. An account holder by being in control of their wallet can decide in a self-sovereign manner how and when to provide their attribute information to applications. When an application needs to verify some statements of attributes, the account holder can generate a zero-knowledge proof that attests to the truth of the requested statement. This allows account holders

[2] More precisely the unique user identifier is "secret shared" and after decryption each privacy guardian can return its share of the identifier.

to convince the application that they meet verification requirements without their personal data, apart from the statement, ever being collected.

The proof system provides the following functionality:

- (in)equality of attribute with a public value
- Set (non-)membership of attributes in a public set
- Range proofs, e.g., attribute <= public value
- AND combination of the above

For example, one can prove that “I am older than 18 and I am resident within the EU”.

All proofs are created and verified off-chain. Moreover, in a future release, Concordium plans to add support for non-transferable proofs by which a prover can generate a proof to an intended receiver in a way that only the specified receiver can be convinced about the validity of the prover's claim. Such proofs can provide plausible deniability for the prover and ensure that the verifier cannot forward the proof to a third party.

Verifiable Credentials

Concordium now offers a self-sovereign identity infrastructure called Web3 ID that comes with support for Verificable Credentials. A verifiable credential system includes three roles: Issuer, Holder, and Verifier. An issuer attests some facts about holders in the form of verifiable credentials. For example, a book club can attest memberships or an organization can attest the completion of a professional program by issuing a diploma. To ensure decentralization, anyone—under some requirement—has the authority to become an issuer.

When needed, a holder can use the credential to prove arbitrary statements about their attested claims to the verifier in zero-knowledge, and a verifier will verify the claim by checking the validity of the credential proof provided by the holder. The trust level of the statement depends on the trust level of the issuer. Anyone with an account on the Concordium platform can become a holder. To verify a credential proof, one only needs read access to the Concordium blockchain.

Execution Layer

Users interact with the Concordium Platform via different types of transactions. Once transactions are submitted, they are added to the transaction pool. Validators check the validity of transactions and include valid transactions into the next block. Transaction validity and the manner in which transactions are handled is dependent on the type of transaction. We discuss the most important types below.

All transactions have timeouts. The **timeout** is set by the creator of the transaction and a transaction cannot be executed after its timeout time has expired. This prevents the situation where an old transfer can suddenly execute days later.

Transaction Types

Account opening

A user opens a new account by publishing an **account-opening transaction**. This transaction contains account creation information (see the above section, *Identity Layer*). It does not cost the user anything, so no CCDs are required to perform this transaction.

Plain Transfers

Once a user has an account, they can execute a **plain transfer** of *x* CCD from *Account A* to *Account B*. Such a transaction is valid if the public balance of *Account A* is at least *x* + *transaction fee*. The effect of the transaction is that the public balance of *Account A* is reduced by *x* + *transaction fee* and the public balance of *Account B* is increased by *x*. Both accounts and the value *x* are publicly visible for this type of transaction. A memo of up to 255 bytes may also be sent along with the transfer of CCD.

Register Data

Concordium also allows small strings to be put on the blockchain, e.g., to register the hash of a document. This protects the integrity of the document (since changes can be detected, as the hash will not match any more) and also serves as a timestamp.

Protocol-Level Token Transactions

User Transactions

Similarly to CCD, a **token transfer** transaction sends protocol-level tokens (PLTs) from the sender's account to the receiver's account. The fees for transactions on the Concordium blockchain are paid in CCD, so the sender account also needs enough CCD to cover the fee to perform such a token transfer. Like for CCD transfers, a memo of up to 255 bytes may also be sent along with the transfer.

Token-Governance Transactions

If the token issuer selected options for the PLT to be mintable, burnable, or have an allow list or a deny list, then the issuer can perform the corresponding transactions from their account. More specifically, they can submit **mint** and **burn** transactions to mint and burn new tokens, respectively. Moreover, they can manage the allow and deny lists by adding and removing accounts from these lists with **addAllowList**, **removeAllowList**, **addDenyList**, and **removeDenyList** transactions.

Finally, token issuers also have **pause** and **unpause** transactions, which globally pause and unpause all token transfers, minting and burning for the PLT.

Smart Contract-Related Transactions

The life of a smart contract starts with the deployment of the smart contract code. Any user can deploy smart contract code using a special transaction and can get an instance of a deployed smart contract using an **initialization transaction**. Each initialized smart contract is associated with an account. An instance of a smart contract can receive inputs in the form of **input transactions**. These transactions specify an amount of ENERGY that is allowed for the execution of the input. The order in which different inputs are executed depends on the order in which the input transactions are added to blocks.

Consensus-Related Transactions

Users can become validators by publishing a special transaction. The newly created validator is associated with one of the user’s accounts, which is used for holding the staked amount of CCD and for receiving rewards. Furthermore, there are transactions to change the stake of the validator, to open or close the pool to new delegators or any delegators, to change whether the rewards are restaked, and to deregister as a validator.

Users can also delegate stake to validators, either to a specific staking pool or using the passive delegation feature. Transactions for changing the stake, changing the delegation target and changing whether the rewards are restaked are also available.

Smart Contract Languages

WebAssembly Low-Level Language

Concordium’s core on-chain language is WebAssembly (Wasm), a portable, well-defined assembly-like language. Wasm is an internet standard that is gaining a lot of traction in recent years and is already supported in the major web browsers.

Many programming languages can already be compiled to Wasm, which potentially enables support of a large range of smart contract languages. Wasm allows for low-level control of the on-chain code, which helps with optimizations when adding support for cryptography in smart contracts.

Among permissionless blockchain platforms, there are very few common standards for smart contracts, however, Wasm is one of the few that is seeing adoption by multiple platforms.

Rust High-Level Language

Concordium plans to support a number of smart contract languages and has chosen Rust as the first high-level smart contract language. The Rust ecosystem is quite friendly, with good documentation and good support for WebAssembly.

Rust is a safe language, but it also allows for low-level resource control. This can help reduce the cost of contracts and makes it very well-suited for development of cryptographic primitives and protocols. Many high-quality libraries exist that can be used off-the-shelf and compiled to WebAssembly.

Concordium also provides additional validation of Rust code so that generated modules conform to on-chain requirements: for instance, that smart contract entrypoints have appropriate types.

Ultimately, however, any language that is able to compile to WebAssembly will be able to target the Concordium chain.

Protocol-Level Tokens

Any user can create and manage their own token in smart contracts on concordium—e.g., following Concordium’s CIS-2 standard [Con22]. While the simplicity of access to smart contracts has its advantages, they do not provide any assurance on the quality of the code nor are there any guardrails to prevent untrustworthy actors creating tokens.

For increased security and reliability, third-party tokens can be issued on the Concordium blockchain at protocol-level—so-called protocol-level tokens (PLTs). Issuance of new PLTs currently requires the approval of the Governance Committee, adding a further layer of assurance for end users.

PLT Initialization

When initializing a PLT, the issuer must choose a token name and a token-governance account. They can also choose which features their token should have. The current options that need to be specified upon initialization are:

- **Initial supply**: how many tokens are minted upon token initialization.
- **Mintable**: whether new tokens can be created by the token issuer after token initialization.
- **Burnable**: whether tokens can be destroyed by the token issuer.
- **Allow-list**: whether the token has an allow-list of accounts that can transact with the token.
- **Deny-list**: whether the token has a deny-list of accounts that cannot transact with the token.

The options are fixed at token initialization, and cannot be changed at a later point.

PLT Governance

The options set during PLT initialization define the governance features available to the token issuer. If the token is mintable or burnable, the token-governance account can submit mint and burn transactions. If a token has an allow or a deny list, the token-governance account can submit transactions to add and remove accounts from these lists.

Furthermore, any PLT can be globally paused by the token-governance account, which prevents any transactions with that PLT from taking place. A paused PLT cannot be minted or burnt either, but the allow and deny lists can still be managed as usual. Once an unpause transaction has been submitted, normal operations can resume.

PLT Use

Users can own and transfer PLTs. If the PLT has an allow list, both sender and receiver need to be on the list for the transfer to succeed. If the PLT has a deny list, neither sender nor receiver can be on the list for the transfer to succeed. If the PLT is paused, the transfer will also fail.

Transferring a PLT requires the sender to have CCD to pay for the transaction fee.

Sponsored Transactions

Sponsored transactions are transactions where the transaction fees are paid by an account other than the sender account, i.e., a sponsor account. This includes CCD transfer and staking operations, but most significantly PLT transactions. Accounts can thus hold and transact with PLTs without holding CCDs, which are required for payment of transaction fees.

In addition to a sender account, a sponsored transaction has a sponsor account that co-signs the transaction. For a sponsored transaction, the transaction fee is charged to the sponsor account instead of the sender account. In all other respects, a sponsored transaction behaves the same as a (non-sponsored) transaction from the sender. In particular, the transaction is authorized to act on behalf of the sender account, but not on behalf of the sponsor account.

Interoperability

Blockchain interoperability can be considered at different levels such as:

- Inter-blockchain ordering of events
- Interfacing to external applications. This could be for retrieving external information to be used in the blockchain ("oracles") or for emitting verifiable information from the blockchain
- Interoperability at smart contract level making it easier to develop decentralized applications based on smart contracts for different blockchain platforms

Ordering of events across different blockchains can be handled by submitting transactions to the blockchains. However, in practice, such synchronization between blockchains is only as precise as the latency on the different blockchains. The design of the Concordium Consensus layer with almost immediate finalization and thereby protection against roll-back is well suited for such inter blockchain ordering.

Regarding interfacing to other applications, the finalization committee in the Concordium Platform is, in principle, able to create messages authenticated by the blockchain. The format of such outgoing messages is independent of the block structure on the chain and will follow a standardized format. The main hurdle is to create these authenticated messages in such a way that the recipient does not have to travel through the complete chain in order to reach a point of trust in the form of the Genesis Block. Concordium is working on solutions to this.

Another aspect of the external interface is providing external data to the blockchain (decentralized oracles). Concordium implemented one such oracle as it is needed to dynamically update exchange rates in our tokenomics model.

With respect to smart contracts, Concordium has a strategy to use existing programming languages with a strong community of developers in order to lower the threshold for many developers to start working with smart contracts. Furthermore, we expect that the choices of Rust as the initial smart contract languages and Wasm as on-chain languages will make it easier to port smart contracts between different blockchains.

Tokenomics and On-chain Incentivization

The Concordium Platform comprises a set of transactions and economic roles that interact within the economy. An economic role, such as a validator or identity provider, exists either off-chain or is represented by an account on the Concordium Platform.

The flow of CCD between accounts via transactions creates an economy that is designed to incentivize participation in the network and counter dishonest behavior. It is the objective of the Concordium Foundation to guide the creation of a sustainable economy that rewards participants for their efforts in developing the network.

Overview of the Concordium Platform Economy

The Concordium Governance Committee (GC) is responsible for maintaining the health of the economy through monitoring of internal dynamics and scrutiny of the impact of external market conditions. The GC will adopt a flexible approach to nurturing the Concordium Platform economy as it evolves to include more complex dynamics and transactions.

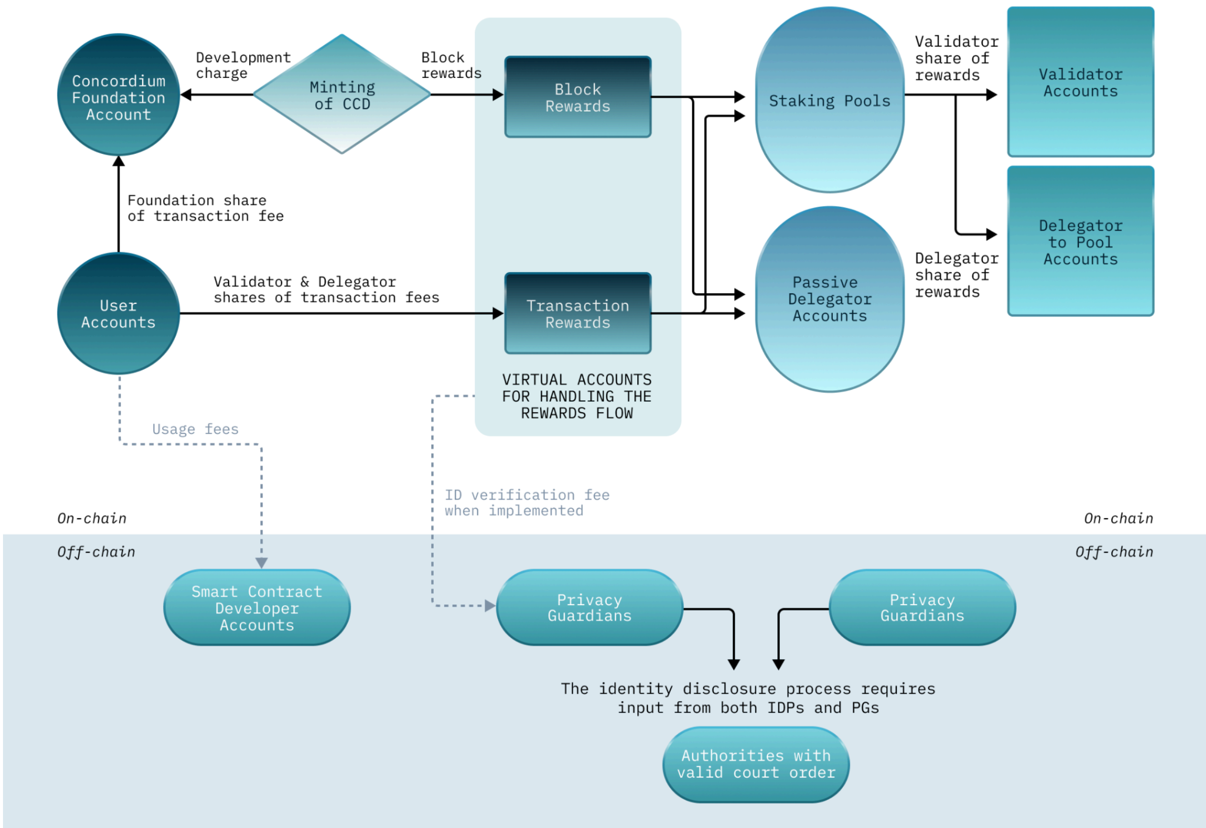

Figure 4: The Concordium Platform economy and roles.

See Figure 4 above for a visualization of the various roles, accounts and transactions in the Concordium economy, both on-chain and off-chain. In this figure, the blue lines indicate the core flow supported at the moment, while the dotted lines indicate flows planned for future updates.

CCD - Concordium's Native Token

CCD is the native token on Concordium Platform. CCD can be used for a variety of purposes, including for smart contract execution fees, for transfers between users, and for commercial transactions. A specific number of CCD is created in the genesis block. After this, the only mechanism to create more CCD is the minting process. The number of CCD that exists on the platform at any time is defined and publicly known.

Roles and Participation in the Economy

There are a number of transactions that allow users and other entities to interact with the economy and each other within the Concordium Platform. Many of these transactions are discussed at length in the section *Execution Layer* above. Specific roles within the Concordium Platform are:

Users can be individuals, businesses, and other identifiable legal entities that create and control accounts within the Concordium Platform.

Users participate in the Concordium Platform economy as follows:

<u>Creating an Account:</u>
1. Account-opening and account-update transactions allow a user to create an account on the Concordium Platform.
2. Initially, there will be no payment required from the user to the identity provider for the creation of a user's identity object, the costs being covered by the Concordium Foundation to stimulate the ecosystem. However, in the future, users may have to pay a fee to identity providers, or the identity providers may get a fee as part of the overall tokenomics flow as indicated in Figure 4.

<u>Making transactions:</u>
1. Users, via an associated account, can initiate transactions, including plain transfers of CCD to other accounts, registering information on the chain, or transferring other tokens that exist on the Concordium Platform. In addition to the transactions enabled on the blockchain, smart contracts provide powerful programming functionality to handle specific applications.
2. Users can receive CCD into their account when their address has been specified as the recipient in the transaction.

<u>Staking:</u>
1. A user can stake part of the CCD on the user's account. This is required if the user wants to operate as a validator.
2. Rewards associated with a user's stake will be automatically transferred to the user's account, and either automatically restaked or made available in the account.

<u>Delegation:</u>
1. In the Concordium Platform, a user can initiate a delegation transaction to delegate an amount of CCD to a staking pool or as passive delegation. Likewise, a user can initiate a similar transaction to un-delegate CCD, i.e., withdraw CCD from the pool or passive delegation.
2. Rewards associated with a user's delegated CCD will be automatically transferred to the user's account, and either automatically re-delegated or made available in the account.

Similar to other users, **the Concordium Foundation** has a number of accounts and runs a number of nodes as validators. Furthermore, the Concordium Foundation plays a central role in the governance of the chain, including oversight over the Governance Committee that manages the tokenomics parameters as described in the section on Governance. The Concordium Foundation is the recipient of the Platform Development Charge that comprises part of newly minted CCD and part of the transaction fees, which are used for developing the Concordium blockchain and the ecosystem around it.

Validators are created when users issue special transactions to register as a validator. To register as a validator, a user must stake a certain amount of CCD which is locked (i.e., cannot be spent) while the validator is registered. This stake must exceed a minimum threshold determined by the Governance Committee (currently 500’000 CCD). The user also determines whether the validator has a staking pool, allowing other accounts to delegate to the validator.

Delegators are users who either delegate some CCD to a staking pool or to passive delegation. They receive rewards similar to validators, but their rewards are lower. Validators that run pools receive a commission from the delegators to their pool. This commission is set by the validator, and may be changed at any time.

Smart Contract Developers: Any user can write, deploy, or use a smart contract on the Concordium Platform. Users that publish a smart contract may also be rewarded for the use of that smart contract by other users. In the future, this process could entail an *App Store*-like library of certified smart contracts. This will allow users to use high-quality code without having to develop it themselves.

Identity Providers perform off-chain identification and create identity objects. Identity providers do not need an account. Identity providers are initially paid in fiat money off-chain but in the future may be incentivized with CCD on-chain for the process of creating identity objects.

Privacy Guardians perform decryption of encrypted user identifiers related to accounts and disclose such numbers to relevant authorities if presented with a valid court order. Privacy guardians do not need an account.

Transaction Costs for Users

Users of the blockchain pay a Transaction Fee (also referred to as a payment of GAS) for each transaction they make. The fee is paid in CCD, and for that purpose, users will need to acquire and hold CCD.

Transaction costs are designed to be relatively stable in EUR terms, thereby enabling businesses and other users to predict and plan with fixed predictable EUR costs.

With the ENERGY principle described below (sometimes denoted NRG), Concordium combines the freely fluctuating value of the CCD with a transaction cost that remains stable versus EUR. This is achieved by making the number of CCD to be paid for transactions vary inversely with the price of the CCD when measured against EUR. So if the value of the CCD goes up, a user needs fewer CCD to pay for transactions, thereby maintaining a stable cost in EUR terms. The technical implementation of the above principle is discussed below.

ENERGY, which is an internal measure of transaction cost per transaction, comprises three elements:

   Transaction Base Cost (same amount for all transaction)
\+ Complexity Premium (dependent on the computational complexity in relation to verification of the transaction and the amount of time it takes to execute)
\+ Size Premium for transactions that contain a large amount of data
= Total Transaction Cost expressed as a number of ENERGY

The calculated ENERGY is converted into a CCD cost by applying a fixed EUR/ENERGY conversion rate and a variable CCD/EUR exchange rate which is adjusted dynamically to ensure that the cost remains stable when measured in EUR.

The EUR cost of transactions may be changed by the Governance Committee (see the section on Governance) in response to significant changes in market conditions or changes in the costs related to processing transactions. It is envisaged that over time, the transaction costs will decrease considerably, ultimately approaching zero. Any changes to the EUR cost of transactions will be announced to users and the public with a notice period of no less than 1 month, unless exceptional circumstances occur, thereby enabling users to make necessary adjustments to their use of the blockchain.

The GAS payment in CCD terms is calculated by applying the following calculation:

GAS (CCD) = ENERGY x (EUR/ENERGY conversion) x (CCD/EUR exchange rate)

The CCD/EUR conversion rate required to perform the conversion is supplied using an Oracle that aggregates data from different sources and takes the median of the obtained values. This ensures that if one of the sources provides incorrect data significantly deviating from the other sources, the conversion rate is not affected. Currently, we are using data from CoinMarketCap, CoinGecko, and Live Coin Watch.

Staking Rewards

The Concordium Governance Committee is tasked with overseeing and adapting the tokenomics described in this section. They have the possibility of changing the parameters to ensure the long term viability of the economic model.

Sources and Types of Rewards

Validators and delegators receive rewards for their involvement in the blockchain. There are two sources for these rewards: the transaction fees paid by the users, which are described in the section above, and newly minted CCD.

These sources of CCD fuel two types of rewards:

- **Block rewards**, which are distributed to a staking pool for every block added to the chain.
- **Transaction rewards**, which are distributed to staking pools for all the transactions included in the blocks that they make.

Minting of CCD

The process of minting new CCD is an automatic feature of the Concordium Platform whereby newly minted tokens are transferred partly to reward accounts for distribution as incentives and partly to Concordium Foundation. Minting is the only source of growth in the number of CCD in existence inside the Concordium Platform. The growth rate is controlled by the Governance Committee.

Minting is governed by a parameter which controls how many CCD are created per day. This ensures that the CCD growth rate is linked to time and does not depend on fluctuations in the rate by which blocks are created. The CCD/day parameter is currently set to have a yearly growth of 4%, and the impact of the CCD growth on the overall tokenomics is monitored to ensure the sustainability of the economy.

A Platform Development Charge of 10% of newly minted CCD is transferred to Concordium Foundation. The remaining 90% of the minted CCD is distributed as block rewards.

Transaction Fees

A Platform Development Charge of 10% is also levied by the Concordium Foundation. The rest of the transaction fees are transferred to the validators and delegators as transaction rewards. This is described in the next section.

Distribution to Staking Pools and Passive Delegation

Delegation Mechanism

Concordium's delegation mechanism allows a CCD holder to delegate some of their CCD to a validator of their choice. This amount of CCD is added to the validator's pool, which increases the probability of this validator being selected to create a block—since this is proportional to the stake in their pool—and thus increases the pool's rewards. Some of the extra rewards obtained by the pool are then distributed to the delegators; the rest goes to the validator.

Concordium has introduced a novel delegation mechanism called *passive delegation*. The delegator who chooses this model does not select a specific validator to whom to delegate, but instead receives rewards as if they had delegated to all staking pools proportionally to each pool's stake. This has less risk than delegating to a single pool since the rewards are not affected by a single validator performing poorly, but the commissions are fixed at 25%, which can be substantially higher than the commissions for individual pools.

Pay Days

Rewards are accrued over a period of 24 hours, and then distributed to accounts. This currently takes place at approximately 9:00 UTC on Mainnet. Changes to validator and delegator stake are also effective at this point (if they were entered at least 1 hour before the end of the pay day).

Block Rewards

Block Rewards are distributed to staking pools for every block that they produce. The amount available for block rewards is currently 90% of the CCD minted in a day, and is divided equally for every block produced. Let this total amount be denoted R_B.

Delegators who choose the passive delegation model get a share which corresponds to the expected reward for delegating to all staking pools proportionally to each pool's stake, minus a passive delegation commission which is currently 25%. This means that an account with passive delegation of s_L CCD will receive

$$R_{B,L} = R_B \cdot s_L / totalStake \cdot 75/100\,,$$

where $totalStake$ is the sum of the stake of all pools and passive delegators.

Let R'_B denote the block rewards left after removing the share of passive delegators. And let the number of blocks produced in a day by pool P on the current chain be n_P. Then that pool will receive

$$R_{B,P} = R'_B \cdot n_P / totalBlocks\,,$$

where $totalBlocks$ denotes the total number of blocks added to the current chain in the day.

Transaction Rewards

The transaction rewards are distributed to staking pools when they produce a block. As said above, 90% of the transaction fee is available as reward, since the Foundation levies the 10% Platform Development Charge. Let R_T the transaction rewards available from a specific block and let the staking pool P be the one that made this block.

Like for the block reward, passive delegators receive a share of the transaction reward corresponding to the expected reward for delegating to all pools proportionally to each pool's stake, minus a passive delegation commission which is currently 25%. This means that an account with passive delegation of s_L CCD will receive

$$R_{T,L} = R_T \cdot s_L / totalStake \cdot 75/100\,,$$

where $totalStake$ is the sum of the stake of all pools and passive delegators.

Let R'_T denote what remains after removing the passive delegators' shares. This is, however, not all distributed to the pool that produced the corresponding block: Concordium has introduced a smoothing mechanism, so that blocks with high transaction fees profit the following validators as well. More specifically, the remaining transaction rewards are shared between the pool that produced the block and a virtual account called the **GAS account**. The current share is 50% for each. Furthermore, the pool that made the block does not only get 50% of R'_T, they also get 25% of what is currently in the GAS account. We thus have

$$R_{T,P} = R'_T \cdot 1/2 \ + \ GAS_{old} \cdot 1/4\,,$$
$$GAS_{new} = GAS_{old} \cdot 3/4 \ + \ R'_T \cdot 1/2\,.$$

Furthermore, if the block includes account creation and protocol update transactions, the staking pool receives a small percentage of the GAS account for these transactions.

Distribution from Pools to Validators and Delegators

The section above covered the distribution of rewards to staking pools and to passive delegators. This section explains how the pool rewards are shared between the validator and their delegators. In a first step, every member of a pool receives a share of the pool rewards proportional to their own stake. Then, delegators return a part of the rewards to the validator. This part is called the commission, and is set by the validator for their pool. They can choose different values for block and transaction rewards if they want.

More specifically, let R_P be the rewards received by a pool in a certain category, and let c be the commission of that category. Let s_P denote the total stake of the pool, let s_B denote the stake of the validator and let s_D denote the stake of a specific delegator D. Then the rewards received by D are

$$R_D = R_P \cdot s_D / s_P \cdot (1 - c),$$

And the rewards received by the validator are

$$R_B = R_P \cdot s_B / s_P + \ R_P \cdot (s_P - s_B)/s_P \cdot c.$$

Relationship between Staking, CCD Growth, and Return on Staking

Validators receive rewards from transaction fees and newly minted CCD. In this section, we explain the relation between the rewards from minted CCD and the amount of CCD staked in the simplified setting with no delegators.

Because the number of minted CCD per block (and thus the rewards) are linked to the CCD growth while the amount of staked CCD is the result of each individual validator's staking decisions, the Return on Staking (RoS) for validators will fluctuate over time.

As described above, rewards being paid out to validators will be 90% of new minting. If the CCD growth rate is 2%, and 50% of all CCD are staked, then the RoS will be:

$$2\% \times 90\% / 50\% = 3.6\%$$

If the number of staked CCD drops to 25%, the RoS will be:

$$2\% \times 90\% / 25\% = 7.2\%$$

The current CCD growth rate is set to 4%. With this rate and if 50% of all CCD are staked, then the RoS will be:

$$4\% \times 90\% / 50\% = 7.2\%$$

If the number of staked CCD drops to 25%, the RoS will be:

$$4\% \times 90\% / 25\% = 14.4\%$$

When the amount of staked CCD goes up, the Return on Staking goes down, and vice versa. This relationship is seen as having a stabilizing effect as it makes it financially more attractive to stake when there is a low amount of CCD being staked and vice versa.

Suspending Inactive Validators

Concordium has a mechanism to automatically suspend validators that consistently fail to participate in the protocol. Suspended validators are excluded from the committee of validators, and will therefore not be selected to propose blocks nor be required to sign off on rounds. Consequently, suspended validators do not earn rewards for themselves or their pool.

The account associated with a suspended validator can lift the suspension by sending a transaction to do so. The validator will then be included in the committee the next time it is determined. (The committee is determined one epoch before each pay day.)

The procedure for automatically suspending a validator is as follows:

- For each current validator, continuously track the number of missed rounds since the validator last successfully produced a block. A missed round is a round in which the validator was the round leader, but no block was produced.
- At each payday, if the number of missed rounds for a validator exceeds a threshold (determined by the "maximum missed rounds" chain parameter, currently set to 10) then mark the validator as "primed for suspension".
- At each snapshot (that is, the start of an epoch prior to a payday), if a validator is primed for suspension, then it is marked as suspended. Suspended validators are not included in the calculation of the validator committee.

- Whenever a validator produces a block, or is a signatory of a quorum certificate that is in a block, its missed rounds counter is reset and it is no longer marked as primed for suspension.

Managing Staking

Validator Status

If a user wants to validate on a certain day, they must register as a validator at least an hour before the start of that pay day—currently, pay days start around 9:00 UTC on Mainnet.

The validator registration includes the following information:

- An account address. This account is associated with the validator, and only the owner of the account can make changes to the validator. The validator's rewards are paid to this account, and the capital staked by the validator comes from this account.
- Equity capital. This is the amount staked by the validator. This amount must be less than the balance on the account at that point in time. The balance of the account cannot fall below the equity capital while the account is a validator, meaning that the validator's stake is locked and cannot be spent or transferred by the account holder.
- Whether rewards are to be automatically added to the equity capital.
- Whether the staking pool associated with the validator is open to all delegators, closed to new delegators or closed to all delegators.
- An optional boolean for suspending a validator or resuming validation after a suspension.

The size of a staking pool is currently capped at 5% of all stake in pools. If this amount is exceeded (e.g., via automatically re-staking rewards), the excess is not counted towards the lottery power of the pool and does not result in extra rewards. We note that the intention is to decrease this cap in the future.

As long as the validator is active, the equity capital CCD amount is locked in the account and cannot be moved. Any amount above the equity capital can freely be transferred to another account or used for paying transaction fees.

If a validator wishes to change their stake it can be done by updating their validator registration with a higher or lower equity capital. The equity capital CCD amount has to be available on the account for the transaction to succeed, otherwise, the update will fail and the equity capital will not be updated.

If the validator decreases the stake, the change in stake is effective at the next pay day, given that it was entered at least an hour before the end of the pay day. The stake is then moved from active stake (counting towards the lottery power and rewards of the validator) to inactive stake, where it remains in cool-down for 7 days. Inactive stake does not earn any rewards. Once the cool down has expired, the inactive stake is unlocked. A new reduction of the stake while some stake is already in cool-down will add the new inactive stake to the cool-down queue, and be unlocked in the wallet 7 days later. The same applies to stopping validating altogether, where all of the stake becomes inactive and is put in cool-down.

If the validator increases their stake for a given pay day, the transaction must be submitted at least an hour before that pay day starts, just like for the stake decrease. To increase the stake, CCD is first taken from the back of the cool-down queue, and only if nothing is in cool-down are unlocked CCD taken from the wallet and locked as stake

A validator can also change whether rewards are automatically restaked, and the status of their validator pool, by updating their validator registration.

Delegator status

A delegator has the choice between delegating to a specific validator or to passive delegation, and can also choose if the rewards are automatically restaked or made available in their account.

Staking pools have two bounds. The first is the bound on the total stake which is currently 5% of all stake in pools and was mentioned above. The second is that the ratio between the stake in the pool and the stake of the validator running the pool can be at most 6. It is not possible to delegate to a pool if the new stake would violate one of these bounds. But if they are violated by re-staking rewards, then the excess does not count towards the lottery power of the pool and does not produce rewards.

Delegators may also change their stake. Increasing or decreasing the stake takes effect at the next pay day, if it was entered at least an hour before the end of the pay day. Any decrease is subject to a 7 day cool-down before it is unlocked in the wallet—during which time it does not earn rewards—just like for validators. However, changing staking pool or moving to passive delegation is effective on the next pay day without any cool-down. As with validators, an increase in stake is first taken from the back of the cool-down queue.

If a validator shuts down, the delegators are automatically moved to passive delegation.

Governance

Introduction

Three bodies share the governance on Concordium: the Concordium Foundation, the Governance Committee and CCD holders. At its launch, the Concordium Foundation was the sole governing entity. Through the decentralization process, which is seeing a mix of direct and representative democracy being introduced to the chain, governance is slowly shifting to the CCD holders via the Governance Committee.

The Concordium Foundation is a non-profit organization established in Switzerland. Its purpose is stipulated in its public deed. The foundation board is responsible for ensuring that the Concordium blockchain develops in accordance with the deed. It therefore has both an executive role and a supervisory role. To facilitate this, it has established guidelines for the development of the Concordium blockchain.

The governance committee (GC) is an advisory committee to the Concordium Foundation Board, which has been assigned certain tasks and responsibilities. In particular, it is involved in parameter and protocol updates, tokenomics and governance decentralization. The Governance Committee was set up with 5 members chosen by the Foundation. New members are added by the token holders through elections, until it reaches 9 members. Then seats are up for re-election.

The decentralization process will lead to CCD holders being able to nominate and elect GC members, vote on some GC decisions and propose their own changes. A roadmap for this decentralization process is given further down. The role and tasks of the GC are described in more detail in the next section.

The Concordium Governance Committee

The GC is an advisory committee to the Concordium Foundation Board and is a dialogue partner of Concordium's executive management group (EMG). It is tasked with providing input to the EMG and recommending changes to the Foundation board on the following areas of the Concordium blockchain:

- Parameter updates
- Protocol updates
- Tokenomics
- Managing CCD holder proposals and votes
- Preparation of the next phase of decentralization

The GC is expected to work with the EMG on the areas described above, with a particular focus on driving tokenomics changes and governance decentralization. In doing so, the GC will consider the following goals and priorities:

- Widespread adoption of the blockchain
- Value creation on the blockchain
- Prevent dominance by single parties
- Ensure a decentralized network of validators
- Stability of the protocol
- Inclusion of CCD holders in decision-making

A complete description of the GC tasks and rules can be found in the decentralized governance framework.

The Roadmap in a Nutshell

The decentralization of the Concordium blockchain's governance is divided in three phases. The initial preparatory phase, which ended with the election of two new GC members from the community in June 2024, was used to organize the first public election and plan the next phase of decentralization.

During the second phase of decentralization, from June 2024 to June 2027, while the Concordium Foundation Board has the responsibility for ensuring that the Concordium blockchain develops in accordance with the founding deed, certain tasks are assigned to the GC. At first, the governance model for the blockchain will be a form of representative democracy. CCD holders will elect members of the GC, first adding new members and then (re)electing members in the seats that were initially filled by the foundation. As part of the decentralization development, the GC will develop a framework and tools to allow CCD holders to vote on certain GC decisions and make proposals of their own.

When all members of the GC are elected by CCD holders—which will be June 2027 according to the current decentralization roadmap—the Concordium blockchain will start the next phase of decentralization, which will see forms of direct democracy being introduced. In this next phase, CCD holders will take an active role in voting on GC decisions and making proposals of their own.

First Phase: June 2021 to June 2024.

In this first phase, the Concordium Foundation Board appointed a Governance Committee with five members. The GC had two main tasks. First, it evaluated and implemented parameter changes and protocol updates, and oversaw and adjusted the tokenomics, including the CCD growth rate within the discretion granted by the Concordium Foundation. Second, the GC developed the details of the governance framework for the start of the first phase and submitted its proposal to the Foundation Board for approval. Besides legal and organizational aspects on how the GC itself should operate, the GC ensured that conceptual and technical solutions were available to elect members to the GC. In particular, the GC prepared the first elections of external members to that committee, which took place in June 2024. In this preparation phase, the Foundation Board oversaw the work of the GC.

Second Phase of Decentralization: June 2024 to June 2027

June 2024

CCD holders appointed two new members to the GC by on-chain voting, thereby expanding the committee from five to seven members. At this stage, two of seven members of the governance committee are appointed by the CCD holders.

June 2025

CCD holders appointed two further members of the GC by on-chain voting, expanding the GC from seven to nine members. At this stage, four of nine members of the GC are appointed by the CCD holders.

The GC has started preparing a governance framework to determine what proposals are put to a vote by CCD holders and what quorums are needed for them to be accepted. They also reviewed the passed elections, and made recommendations on possible changes in the procedures.

June 2026

The GC's number of members remains at nine members, with three seats up for (re)election every year. Thus, three of the initial five committee seats appointed by the Board of Concordium Foundation are up for election in 2026. At this stage, seven of nine members of the GC are appointed by the CCD holders.

During this year, the GC will finalize the rules and tools required for the next stage of decentralization, i.e., voting on GC decisions and community-driven proposals.

Third Phase of Decentralization: June 2027 and onward

June 2027

After the on-chain elections of June 2027, where three seats are up for (re)election, all members of the GC will be appointed by the CCD holders. This starts phase three of decentralization, where the elections will continue with three seats being up for (re)election every year.

During this phase voting will be introduced, allowing the community to vote on tokenomics parameters and possibly on protocol updates. They will also be able to propose changes of their own. Certain aspects of the governance framework may even be modified by CCD holders. The precise scope of the GC's mandate will be determined based on the experience gained during the preceding steps.

References

An up-to-date list of research papers from the Concordium Blockchain Research Center Aarhus (COBRA) can be found under https://cs.au.dk/research/centers/concordium/publications/.

[ANS19] Annenkov, D., Nielsen, J., Spitters, B. ConCert: A smart contract certification framework in Coq. Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, 2019. https://doi.org/10.1145/3372885.3373829.

[CM19] Chen, J., Micali, S. Algorand: A secure and efficient distributed ledger, Theoretical Computer Science, Volume 777, 2019. https://doi.org/10.1016/j.tcs.2019.02.001.

[Con22] Concordium Research ApS. (2022) CIS-2: Concordium Token Standard 2. https://proposals.concordium.com/CIS/cis-2.html

[DGKOS21] Damgård I., Ganesh C., Khoshakhlagh H., Orlandi C., Siniscalchi L. (2021) Balancing Privacy and Accountability in Blockchain Identity Management. Topics in Cryptology – CT-RSA 2021. Lecture Notes in Computer Science, vol 12704. Springer, Cham. https://doi.org/10.1007/978-3-030-75539-3_23

[DMMNT22] David, B., Magri, B., Matt, C., Nielsen, J.B., Tschudi, D. GearBox: Optimal-size Shard Committees by Leveraging the Safety-Liveness Dichotomy. 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). Association for Computing Machinery, New York, USA. https://doi.org/10.1145/3548606.3559375.

[GKSSX22] Gelashvili, R., Kokoris-Kogias, L., Sonnino, A., Spiegelman, A., Xiang, Z. (2022). Jolteon and Ditto: Network-Adaptive Efficient Consensus with Asynchronous Fallback. Financial Cryptography and Data Security. FC 2022. Lecture Notes in Computer Science, vol 13411. Springer, Cham. https://doi.org/10.1007/978-3-031-18283-9_14.

[GOT19] Ganesh C., Orlandi C., Tschudi D. (2019) Proof-of-stake protocols for privacy-aware blockchains. Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11476. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-17653-2_23.

[Kwo14] Kwon, J. Tendermint: Consensus without mining. Manuscript, 2014. https://tendermint.com/static/docs/tendermint.pdf.

[NS19] Nielsen, J., Spitters, B.: Smart contract interactions in Coq. CoRR abs/1911.04732, 2019. https://arxiv.org/abs/1911.04732.

[Per16] Perrin, T. The noise protocol framework, 2016. http://noiseprotocol.org/noise.pdf.

[SW21] Jakub Sliwinski and Roger Wattenhofer. 2021. Asynchronous Proof-of-Stake. In Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, November 17–20, 2021, Proceedings. Springer-Verlag, Berlin, Heidelberg, 194–208. https://doi.org/10.1007/978-3-030-91081-5_13.

[YMRGA19] Yin, M., Malkhi, D., Reiter, M., Gueta, G., and Abraham, I. HotStuff: BFT Consensus with Linearity and Responsiveness. ACM Symposium on Principles of Distributed Computing (PODC '19).

Association for Computing Machinery, New York, NY, USA, 347–356. https://doi.org/10.1145/3293611.3331591.

DISCLAIMER. This document reflects the Concordium Foundation's current plans regarding the functionality and specifications of the Concordium Platform, technology, blockchain and ecosystem (the 'platform'). Readers should be aware that: a) the actual and further development of the platform may deviate from what is described in this document; b) that the Concordium Foundation may change the specifications of the platform at any time; and c) that the Concordium Foundation accepts no liability for the reliance by third parties on the information in this document.