CORD Network

CORD is a purpose-built decentralised infrastructure designed from the ground up to be a global public utility and enable a trust framework. CORD creates new possibilities in addressing trust gaps, managing the authenticity of transactions, and exchanging value at scale. CORD provides a stable, trustworthy network for enterprises and developers to explore new business models related to trust relationships and data sovereignty.

The core protocol enables data availability, discovery, consent receipts, integration, security, and compliance to ensure the right data is delivered to the right resource at the right time — and to ensure the data is being used for the right reason. This would enable businesses and governments to rely on a standards-driven value exchange protocol that is owned by everyone participating and not the monopoly of a single company.

Developers and enterprises can use the CORD network services to create applications that run on top of the network. The network supports the potential to catalyse exceptional levels of innovation in both existing and emerging industries-from conducting transactions and maintaining records, across many sectors of the economy such as finance, trade, health, energy, water, resources, agriculture and credentials.

Token

The purpose of CORD is to provide a stable, trustworthy network for a wide variety of decentralized, enterprise-grade applications, not to provide a cryptocurrency. However, like all public DLT networks, CORD needs a token to function. DHI is the native token of the CORD network. DHIs serve as the *fuel* to power decentralized applications, build peer-to-peer data exchange models, and protect the network from malicious actors.

The DHI token creates signalling for two key functions in CORD, namely

(i) Governance - DHIs are used as voting power, to let DHI holders participate and express their choice in governance decisions. Included in this function is determining the fees of the network, and exceptional events such as upgrades and fixes to the CORD network. These functions are not formally granted to token holders, but rather the underlying code of CORD will enable token holders to participate in governance.

(ii) Economics - DHI facilitates the consensus mechanism that underpins CORD. DHIs are used to reward the nodes that run the consensus protocol, fund the treasury, control the inflation rate, etc. In order for the network to function and allow for valid transactions to be carried out, CORD will rely on token holders to play active roles. Participants will put their tokens at risk (referred to as "staking") to perform these functions. This acts as a deterrent for malicious participation in the network. The total number of DHI required to participate in the network will vary according to the activity undertaken, the duration DHI is staked for, and the total amount of DHI staked.

In summary, DHI holders will have certain functions within the CORD network including:

- The ability to pay for on-chain transactions.
- The ability to act as a validator, or nominator.
- The ability to participate in the governance of the CORD network.
- The ability to participate in the decision-making process in relation to global upgrades and/or changes to the CORD Network.

Consensus

CORD adopts the Web3 foundation variant of PoS called Nominated Proof-of-Stake (NPoS), with design choices based on first principles and having security, fair representation and satisfaction of users, and efficiency as driving goals.

CORD uses a Hybrid consensus mechanism that consists of Blind Assignment for Blockchain Extension protocol (BABE): a block production mechanism of the chain that provides probabilistic finality and GHOST-based Recursive Ancestor Deriving Prefix Agreement (GRANDPA) which provides provable, deterministic finality and works independently from BABE.

NPoS allows all DHI holders to continuously participate, to become validator candidates, or become nominators. Nominators approve of candidates that they trust and back them with their tokens, and once per era a committee of validators is elected according to the current nominators' preferences. In CORD, the number k of validators elected is in the order of tens during the permissioned phase and maybe hundreds in the permissionless future.

Both validators and nominators lock their tokens as collateral and receive staking rewards on a pro-rata basis. However, negligent or adversarial behavior from a validator may also result in tokens being slashed as part of the governance rules in the network. Nominators thus participate indirectly in the consensus protocol with an economic incentive to pay close attention to the evolving set of candidates and make sure that only the most capable and trustworthy among them get elected.

Being a nominator is a way of investing one's DHIs, and of helping in the security of the system. Indeed, the larger the total number of DHIs staked by nominators and validators, the higher the system security, because an adversary needs that much more stake – or nominators' trust – before it gets any nodes elected as validators.

This nominator-validator arrangement gives strong security guarantees. It allows for the system to select validators with massive amounts of aggregate stake — much higher than any single party's DHI holdings — and eliminate candidates with low stake. In fact, at any given moment we expect there to be a considerable fraction of all the DHIs supply be staked in NPoS. This makes it very difficult for an adversarial entity to get validators elected (as they need to build a fair amount of reputation to get the required backing) and very costly to attack the system (because any attack will result in large amounts of DHIs being slashed).

Networks using the Proof-of-Stake consensus protocol include Polkadot, Cardano, EOS, Tezos, and Cosmos, among many others. While similar in spirit, the approaches in these networks and CORD vary in terms of design choices such as the incentive structure, the number of validators elected, and the election rule used to select them.

Transactions

Several resources in a decentralised network are limited, for example, storage and computation. Transaction fees prevent individual users from consuming too many resources. CORD uses a weight-based fee model. The fees are charged prior to transaction execution; once the fee is paid, nodes will execute the transaction.

Some of the properties we want to achieve relative to chain transactions are as follows:

- Each block should be processed efficiently, *even on less powerful nodes*, to avoid delays in block production,
- Each block has *guaranteed availability* for a certain amount of operational, high-priority txs.
- Blocks are typically far from full, so that peaks of activity can be dealt with effectively and long inclusion times are rare.

- Fees evolve slowly enough, so that the *fee of a particular tx can be predicted accurately* within a frame of a few minutes.
- For any transaction (tx) the fee level is strictly larger than the reward perceived by the block producer for processing it. Otherwise, the block producer is incentivized to stuff blocks with fake txs.

The amount of transactions that are processed in a block can be regulated in two ways: by imposing limits, and by adjusting the level of tx fees. We ensure properties 1 and 2 above by imposing hard limits on resource usage, while properties 3 through 5 are achieved via fee adjustments.

Limits

Limits are set based on the the four resources mentioned below, which can be consumed when processing a tx:

- Length: data size of the tx in bytes within the block,
- Time: time it takes to import it (i/o and cpu),
- Memory: amount of memory it takes when processing,
- State: amount of state storage increase it induces.

Notice that unlike the first three resources which are consumed only once, state storage has a permanent cost over the network. Hence for state storage we could have rent or other Runtime mechanisms, to better match fees with the true cost of a *tx*, and ensure the state size remains bounded. This needs further consideration.

In principle, a tx consumes some amount of the last three resources depending on its length, type, input arguments, and current state. However, for simplicity, we decided to consider, for each transaction type, only the worst-case state, and only the byte length of its input arguments. Consequently, we classify transactions based on length, type and argument length, and run tests (based on worst-case state) to examine their typical resource usage.

To simplify the model, we define a *tx weight* as a parameter that captures the time usage and state increase of a *tx*. Specifically, we define a *tx* weight as the *max* of its typical time and state usage, each measured as a fraction of the corresponding block limit. Then, given a collection of *tx*s, we will sum up their lengths on one hand, and their weights on the other hand, and we will allow them within the same block only if both limits are respected. This is a hard constraint on resource usage which must be respected in each block.

Fees

CORD transaction fees are set in fiat currency but paid in DHI. The CORD Network Governing Council sets the transaction pricing, and approves any changes to the pricing schedule. This model helps to offer low and predictable transaction fees on the CORD network.

We use the resource usage model described above to set the fee level of a *tx* based on three parameters: the *tx* type, its length, and its weight. This fee differentiation is used to reflect the different costs in resources incurred per transaction, and to encourage/discourage certain *tx* market behaviours.

A transaction fee *tx* is computed as follows:

$$fee(tx) = base\_fee + type(tx) . length(tx) + c_{traffic} . [weight(tx)]$$

where $c_{traffic}$ is a parameter independent from the transaction, that evolves over time depending on the network traffic; Parameter $type(tx)$ depends on the transaction type only; in particular for operational transactions, we currently set $type(tx)$ to zero. The term $weight(tx)$ covers the processing cost of the block producer, while the term $type(tx) . length(tx)$ covers the opportunity cost of processing one transaction instead of another one in a block.

As mentioned earlier, part of the *tx* fee needs to go to the block producer, to incentivize inclusion, but not all of it, so the block producer is discouraged from stuffing blocks with bogus *tx*s. For simplicity, we propose that 20% of each *tx* fee goes to the block producer, 5% of each *tx* fee goes to the protocol development council, with the remaining 75% going to the treasury. This ratio may be adjusted before the MainNet launch and could be made dependent on the *tx* type, to encourage the block producers to include certain *tx* types without necessarily adjusting the fee.

Fee Adjustment

Transaction volume on blockchains is highly irregular, and therefore transaction fees need a mechanism to adjust. However, users should be able to predict transaction fees.

CORD uses a slow-adjusting fee mechanism with tips to balance these two considerations. In addition to block *limits*, CORD also has a block fullness *target.* Fees increase or decrease for the next block based on the fullness of the current block relative to the target. The per-weight fee can change up to 30% in a 24 hour period. This rate captures long-term trends in demand, but not short-term spikes. To consider short-term spikes, CORD uses tips on top of the length and weight fees. Users can optionally add a tip to the fee to give the transaction a higher priority.

Governance

The Governance Model of the CORD network is based on a tricameral approach. It is designed to enable majority stakeholders to determine the direction of development and sustainability of the network. This goal is brought to fruition through the creation of a defined set of roles and responsibilities; on-chain voting mechanisms and the presence of an incentive structure that is fair, transparent and establishes accountability. The stated goal is to ensure that the majority of the stake can always command the network.

CORD uses a sophisticated governance mechanism that allows it to evolve gracefully over time at the ultimate behest of its assembled stakeholders. To do this, we use various novel mechanisms based on Web3 foundation specification, including an amorphous state-transition function stored on-chain and defined in a platform-neutral intermediate language (i.e. WebAssembly) and several on-chain voting mechanisms such as referenda with adaptive super-majority thresholds and batch approval voting. All changes to the protocol must be agreed upon by stake-weighted referenda.

To make any changes to the network, the idea is to compose active token holders and the council together to administer a network upgrade decision. No matter whether the proposal is proposed by the public (token holders) or the council, it finally will have to go through a referendum to let all holders, weighted by stake, make the decision.

Summary

We believe CORD will be an essential building block of Web 3.0 with its ability to reimagine real-world interactions that best fit a particular purpose, balancing security and control with the convenience and opportunity of sharing data between institutions and individuals. The technology will continue to evolve over the coming years, and for that reason, this overview should be considered as the start of the conversation between stakeholders on how we can all work together to move forward. Together, we can drive the long-term development and adoption of the technology, and capitalise on the tremendous economic and social opportunities it offers.