Aventus Network

Technical whitepaper

Andrey Brozhko, C. Emmanuel Ngubo

Version 2. July 2022

Aventus Network belongs to the new generation of composable blockchain networks built for scalability and interoperability. It is capable of high transaction throughput, provides deterministic finality and low and predictable transaction costs. The network currently operates as a Layer 2 on Ethereum, and is used by several production applications. The mainnet has processed over 12 million transactions since its launch in 2021. This paper provides a technical overview of the fundamental architectural properties of the Aventus platform, the functioning of the network and the ecosystem. It further presents a high-level outline of the future roadmap for its evolution.

Table of Contents

1 Overview

Introduction

It has been 13 years since the introduction of blockchain technology to the world. The first generation of blockchains heralded a technology capable of not only disrupting the status quo in multiple sectors, but also challenging the thought process behind existing infrastructures. The handicap of this generation of blockchains was scale.

It was succeeded by blockchains that brought the ability to power arbitrary code on an immutable, decentralised ledger. And while it led to the creation of thousands of tokens, both fungible and non-fungible, it did not address the question of scalability, which was further exacerbated by the lack of composability. This technology 'upgrade' did not bring the means to extend the capabilities of the blockchain without causing irreparable damage to the chain history by way of hard forks.

Finally, we arrive at the current generation of blockchains designed to address these unanswered questions. Blockchains which are designed to be scalable, support the execution of code and be composable— ageneration to which Aventus proudly belongs. Its technology is built on Substrate for composability and interoperability, ensuring it can serve any and all business logic. Initially designed as a Layer 2, it plays well with legacy blockchains such as Ethereum, making it faster and cheaper to transact on Ethereum. And with modern cryptographic algorithms, consensus mechanisms and insignificant transaction fees, it's built to scale.

Aventus is a new benchmark for interoperable blockchains designed for modern businesses.

Aventus

Aventus's journey began in 2018, providing blockchain-powered solutions to the ticketing industry via a project called Aventus Classic [1]. The entertainment industry had been plagued with scalpers and fraudulent tickets, among other issues for which blockchain technology was more than apt for. So Aventus classic was an open-source, decentralised Ethereum-based ticketing protocol designed to alleviate fraud and touting in the long tail of the event ticketing industry. Its mission was tripartite: to improve oversight and control over tickets, to facilitate lasting communication between ticket owners and rights holders and to promote the standardisation of tickets and their life-cycle across the entire supply chain in order to reduce costs.

The Aventus team recognised from the start that the existing capabilities [2] in speed and scalability of Ethereum were not sufficient to power the solution for the ticketing market. However, in 2018, the Ethereum development community had ambitious immediate plans to address these limitations, and the Aventus team aligned the development of the company offering with the Ethereum roadmap as it was plotted at the time. While the evolution of Ethereum's capabilities in security, standards, and its independence from corporate interest have been excellent, delays and setbacks in the execution of scalability and speed roadmaps had become a blocking issue for Aventus.

With no out-of-the-box solution existing at the time, Aventus sought to build a scalable platform that would not only achieve the scalability required for the original vision, but could also be tuned to other business use cases. Aventus, therefore, began work on the Aventus Network, a solution designed to achieve the required levels of scale and privacy without compromising on native security and independence. The approach Aventus took here broadly puts the the Aventus Network solution into the Layer 2 (L2) 'bucket' in the sense that it enhances the scalability of the Layer 1 (L1) by offering a facility to securely bring over and process transactions on the Aventus Network (i.e. on L2 — off the L1 chain), while also providing the means for users to independently verify on L1 that L2 processed and validated their transactions. The team has further enhanced and adapted the original protocol ensuring that this L2 solution is also suitable for problems ingrained within other aspects of commerce including loyalty, vouchers, financial assets and virtual goods, i.e. any industry or supply chain focused on digital assets.

Aventus Network launch

The Aventus Network (AvN) launched in February 2021 with 10 validator nodes and a staking program which provided members of the community with the opportunity to stake their AVT and earn rewards. The AvN is built on Substrate —a next-generation blockchain technology developed by one of the co-founders of Ethereum. Substrate is the technology powering the Polkadot ecosystem, which established a new architectural paradigm delivering interoperability and scale.

The existence of multiple Ethereum competitors, as well as other private / permissioned networks, has created a situation where there are many disconnected silos of value. Aventus Network addresses this problem. It is interoperable with Ethereum in the sense that Ethereum assets can be seamlessly transferred to and from the AvN in a simple operation. At the same time, the Aventus platform is built using Substrate, which provides an open path to becoming a Polkadot parachain.

Scale, price, and interoperability

The AvN can currently scale to 2,000 transactions per second — 133 times more than Ethereum. The AvN will process a token transfer within 0.13 seconds — 100 times faster than the Ethereum blockchain.

The transaction costs on the Aventus Network are decided by the community. Currently average cost is $0.01 (paid in AVT). This is not only 99% cheaper than the average Ethereum transaction fee over the past year, but, most importantly, it is predictable. Aventus Network addresses transaction price volatility, and allows users of the network to plan for and allocate operational budgets for transaction processing. This is a matter of particular importance for businesses, where unexpected price spikes can result in the significant increase in the cost of business, or worse denial of service, and a loss of revenue.

The AvN has onboarded over 12 million transactions from multiple entities active on the network over the last year. We are expecting the flow of transactions to continue and the rate to accelerate as more and more businesses learn about the advantages of AvN. You can find full transparency of all Aventus Network traffic and fees at the Aventus Network Explorer.

Companies building on Aventus

Since the launch of the mainnet, there have been a growing list of companies from various sectors building on the Aventus network. The list below represents some of the highlights of the thriving Aventus ecosystem.

VereNFT

VereNFT is an enterprise-grade whitelabel NFT platform provider that enables and supports businesses in creating their own bespoke NFT marketplace, offering customisable bolt-ons including AML/KYC, crypto and fiat payment gateways and world-leading marketing services. Use cases including art, music, video games, film, sports, horse racing and data. VereNFT is powered by the Aventus Network.

Parity

Parity is a community for female athletes focused on closing the gender pay gap among athletes using NFTs, with 600+ athletes over 40+ sports and 20+ corporate partners. The Parity NFT platform is a whitelabel solution powered by VereNFT.

Aficionados

Aficionados is dedicated to supporting specialists in music, fine art, photography and sport, and helping to redistribute revenue more fairly in these industries. The Aficionados NFT marketplace is home to household names as well as unsigned, independent and breakthrough talent in music, photography, videography and art. Aficionados Marketplace is powered by Vere NFT.

Vow

VOW eliminates the cost of refunds and rewards for retailers by providing an innovative two-token model. The solution provides much more efficient loyalty schemes, restructuring how loyalty points are handled on the balance sheet of the issuing entity, and improving the user experience for customers via instant payout with no fees thanks to the power of the Aventus Network. Cashbackapp, a cashback provider using the VOW / vCurrency token system, is currently active across the UK, Denmark, India, USA, Southern Africa, Australia and Malta.

Fruitlab

Fruitlab is a social network for gamers which allows creators and community members to securely earn revenue by streaming clips of their gaming with the PIP token. With over 600,000 active users, fruitlab is an established platform on web and app for the world's gaming community. Aventus securely and cost-effectively executes all fruitlab token transactions.

Cavalieri

Cavalieri is a virtual racing platform that creates digital twins of real life horses in the form of NFTs and gives back to the industry. Users can collect, trade, breed and race horses. Using technology from Aventus, Cavalieri is able to produce life-like CGI and ensure that the probability of race success is dependent on real-world data. Via the platform, horse owners can generate an additional revenue stream from their real horse inventory, even after the real horse is no longer able to race or breed.

Symbiotix

Symbiotix is building the world's first medical data utilisation platform with the use of NFTs on a blockchain. It will use Aventus network and associated technology to create and trade NFTs at low cost. This will allow easy monetisation of structured medical data in a way that wasn't possible before. Symbiotix has acquired 100K patients' medical data in the UAE for the launch of the platform to demonstrate feasibility, scalability, governance and access control of sensitive data.

2 Architecture

The Aventus Network comprises both Layer 1 (L1) and Layer 2 (L2) technologies. These two layers communicate (between blockchains) important transaction information, state changes, etc. This chapter will discuss the architecture of the L2 as it is the engine that enables cheaper and faster transactions. The following chapter will be dedicated to L1 and the interoperation between the layers.

Aventus L2 is a general-purpose blockchain built on Substrate. Its function is to group transactions into blocks in such a way that the resulting cryptographic ID of the block is influenced by each transaction in the block; and the chronological order of the blocks is cryptographically verifiable.

Substrate

Substrate [1] is an open-source blockchain development framework written in Rust with the added functionality of being able to compile to WebAssembly (WASM). It provides robust tools to build blockchain networks designed and optimised for any use case.

Around the advent of blockchain technology, it was not uncommon to see "new" blockchain platforms with a codebase that was essentially a spin-off from already existing and established chains. Needless to say, the original designers of the code were not aware and could not accommodate the yet unknown activities and use-cases of these other chains. Moreover, there are multiple characteristics prevalent in those legacy chains that are not suitable for today's blockchain networks. These include forks, low transaction processing rate and incompatibility with other chains. Specifically, the need for forks has plagued the blockchain space for some time with notable mentions like the DAO hard fork [3] and the London hard fork on Ethereum. The slow rate of transaction processing on legacy chains such as Bitcoin and Ethereum led to the rise of L2 technologies [4][5] to offload transactions.

[1] https://docs.substrate.io/

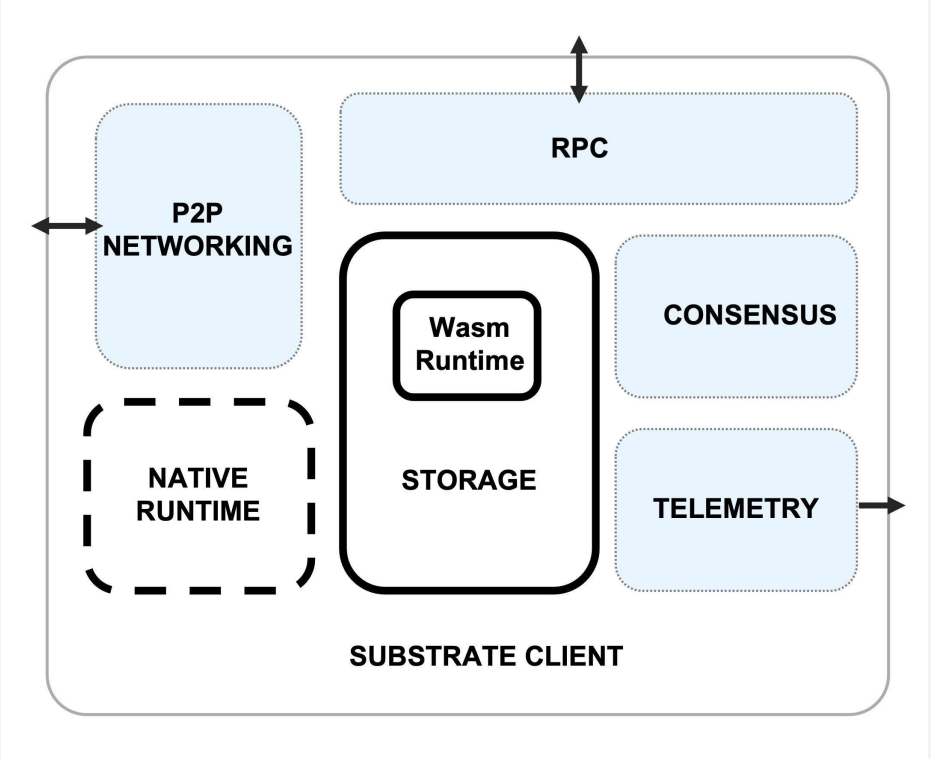

Figure 1: Substrate Client

With Substrate, major upgrades can be made to the Aventus mainnet without forking the blockchain; transaction processing is faster due to an optimised runtime, and the Aventus blockchain is compatible with relay chains like Polkadot[6] and Kusama. The Aventus blockchain is currently using version 3 of Substrate.

Substrate provides ample documentation on the generic framework and client build (figure 1) — therefore, the remaining part of this chapter will focus on the architecture of the specific Aventus build.

AvN accounts and nodes

An account can be referenced as a 32-byte address derived from a cryptographic public key but technically it is a key pair. Each account on the AvN can have two types of balances - an AVT balance and the balance of any ERC-20 token on the L2. AVT is the native token of the AvN (more on this in chapter 4). Similar to Bitcoin and Ethereum, we use an Elliptic-curve based public-key cryptography. The main difference lies in the curves used and the signature algorithms. Bitcoin and Ethereum use a curve called secp256k1 while we use Curve25519 as we are Substrate-based. For the signature algorithm, both Bitcoin and Ethereum use ECDSA (Elliptic Curve Digital Signature Algorithm). Substrate uses two algorithms, which also use the underlying curve in slightly different algebraic

ways. SR25519 is, at its core, a Schnorr signature on a variant of Curve25519 (the Ristretto group, hence the R in SR25519).

Ed25519 is a vanilla ECDSA signature (same as Ethereum) applied on the Curve25519. While an account can be created using either, accounts on the AvN are generally created using the SR25519 cryptographic curve as this is the standard cryptographic curve used by Polkadot and is regarded to be more secure and efficient than ED25519. All addresses on the AvN are related to their Public key. The account's address will then be the representation of this public key in the SS58 format. A user or node, using these keys, will be able to sign messages and transactions, and access funds on the AvN.

There are three types of nodes on the AvN: RPC, Archive and Validator nodes. A Remote Procedure Call (RPC) node is a node that allows network users to interact with the blockchain by sending transactions through it to the Validator nodes, or querying data on the state of the chain. The third type is an archive node, which is a node that keeps full history but does not participate in consensus, and is used to take backup snapshots. This is so that in the future, we can make validator nodes run without keeping a full history of the chain, which will be held solely in the archive nodes. Validator nodes are authorised nodes that can create blocks on the chain. These nodes maintain the blockchain by authoring blocks, verifying transactions submitted to them from both inside and outside the L2 or via gossip by other validators. RPC nodes do not have all these responsibilities and thus can be thought of as "light". The term "light" here means that they are not weighed down with the computationally intensive tasks required to validate transactions and author blocks. RPC nodes serve to answer queries and propagate requests to the validators as needed; relaying the answers back to the users, while the validators validate each transaction and process them into blocks.

There are currently 10 validator nodes on the main network. To promote decentralisation, the most prevalent network operation in most blockchain implementations is the Peer-to-Peer (P2P) exchange. The AvN uses the available Substrate pallet which is a Rust implementation of the *libp2p* network, and nodes communicate via the gossip protocol. Extrinsics submitted into the network are communicated to other nodes using the P2P network.

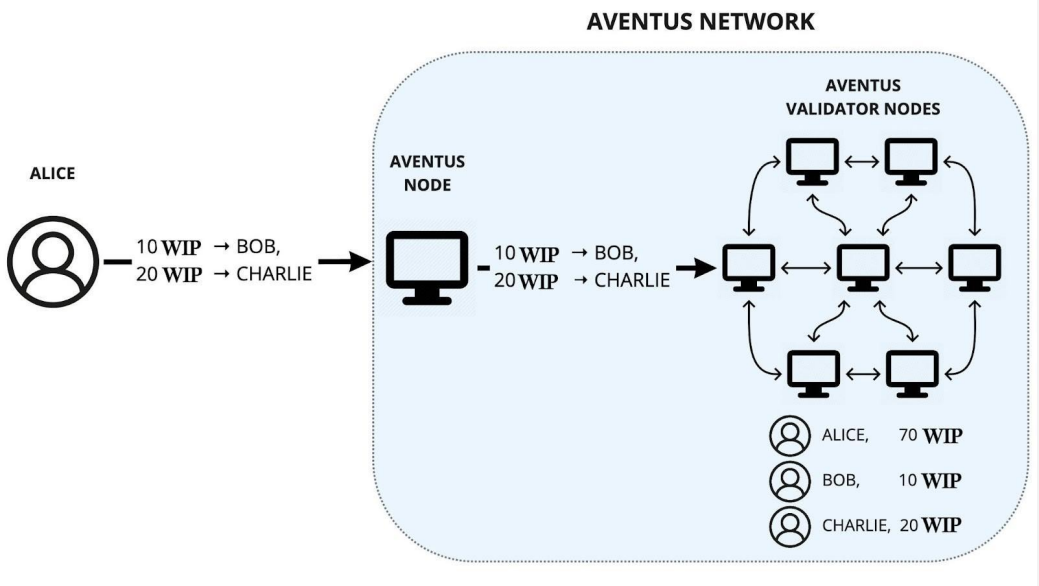

Figure 2: Executing an extrinsic on the AvN

Extrinsics

Extrinsics are the means by which we change the state of the blockchain. Extrinsics are transactions that originate from outside the blockchain network (for example, from users), yet are recognised by the blockchain. Every fee-paying extrinsic submitted to the chain has to be signed by the sender before this transaction is executed in the runtime by all the validator nodes. Given that all the validators must share the same state, each transaction is validated and the validators must reach a consensus on the acceptance of the transaction.

In figure 2, we see Alice sending two extrinsics for 10 and 20 WIP[2] to the Aventus network via an RPC node. These transactions are added to the RPC node's Memory Pool (mempool), which is a queue for incoming transactions waiting to be picked up, validated and sent to the validator nodes. All nodes run basic validation of transactions before accepting to send it to the rest of the nodes on the network. Assuming that at least 2/3 of the validators on the network are honest, the transactions should be processed correctly and Bob and Charlie should have a balance increase respective to the sent amount.

Alternatively, if more than 1/3 of the nodes disagree on the incoming transaction i.e., they can't agree on the validity of a signature, then the transaction is rejected

[2] WIP is a fictitious token created for this illustration.

and no WIP is sent from Alice's account and Bob and Charlie remain with their original balances.

Runtime and client

The AvN runtime and client are configured differently from the base Polkadot and Substrate configurations. The client is the code running on every validator that implements the communication logic, which receives network connections, handles all the requests from outside the network, and on occasion communicates with the other nodes.

The runtime is created by the client, it operates similarly to a virtual machine running inside the client. The runtime handles the low-level logic of the blockchain i.e. the state transitions and appending blocks to the chain, and is the environment where all extrinsics[3] are executed. Every client implements a runtime that operates the same way regardless of the underlying operating system. Therefore, it could be viewed as a shared workspace among all validators and members of the blockchain network.

The runtime has limited capabilities in order to ensure that every action it performs is deterministic. Runtimes also fulfil another major function of enabling forkless upgrades. New upgrades are compiled into WASM and stored on the chain, which therefore enables the chain to update its logic without nodes forking into alternative histories.

Consensus

The ability to implement consensus mechanisms is just one area in which Substrate excels. Consensus is at the heart of every blockchain network. Consensus provides the mechanics for determining if a submitted extrinsic should be appended to the immutable chain. Since the inception of the blockchain via the popular Bitcoin white paper by Satoshi Nakamoto, consensus mechanisms have been an ongoing conversation in the blockchain space. And although Proof of Work (PoW) has demonstrated its mathematical advantages, it is limited by its infamous energy expenditure and is not ideal for certain use cases and conditions.

[3] Also known as Transactions

Consensus and finality

Consensus is the process by which multiple parties agree about the subject of their deliberation. In the context of a blockchain, the consensus is the process by which nodes agree on the global view of the chain i.e. the canonical order of the chain. This process can be split into three: block authorship, finality and fork-resolution rules. There are multiple algorithms developed to achieve consensus such as PoW, PoS, PoA, NPoS, PBFT, etc.

Currently, the AvN runs on a Proof of Stake (PoS) consensus mechanism, where validator nodes take turns validating transaction sets, and it currently uses Blind Assignment of Blockchain Extension (BABE) for its consensus. BABE uses a Verifiable Random Function (VRF) method which introduces a degree of randomness and thus fairness into the block author selection process.

Substrate adopts a hybrid consensus model i.e. a model that consists of independent but connected mechanisms. While BABE handles the block production with an underpinning reality of a probabilistic finality, GHOST-based Recursive ANcestor Deriving Prefix Agreement (GRANDPA) ensures deterministic finality.

Block creation

Blocks are created on the L2 approximately every three seconds and can be viewed through the block explorer[4]. This means that, to enable timely resolution, the entire set of transactions in one block must execute in under one second. Each extrinsic has a weight that represents in somewhat abstract terms how much time it takes to run. There is a limit on how much weight can be included in a block. This limit should be adjusted such that the block's transactions do not go over one second.

Pallets

Pallets are a special kind of Rust modules consisting of a set of types, trait implementations and functions from which Substrate runtimes can be composed. Substrate provides numerous modules, and while we do re-use some of the Substrate code, the AvN currently has eight pallets in operation. A few of these pallets have already been open-sourced, others are to be open-sourced soon.

[4] https://explorer.aventus.io/

1. **AvN** This pallet provides functionality that is common for other avn pallets such as handling off-chain workers, validations, managing a list of validator accounts.

2. **AvN finality tracker** This pallet is responsible for tracking the latest finalised block and storing it on chain. All validators are expected to periodically send their opinion of what is the latest finalised block, and this pallet will select the highest finalised block seen by 2/3 or more of the validators.

3. **Ethereum-events** This pallet provides functionality to get ethereum events.

4. **Ethereum-transactions** This pallet handles Ethereum-related transactions.

5. **NFT-Manager** This pallet integrates NFTs into the Aventus blockchain on an infrastructure level allowing for the minting of both single and batch NFTs without smart contracts. The innovative work involved in the creation of this NFT standard resulted in our first and second Aventus Improvement Proposals.

6. **Summary** This pallet handles the checkpointing to the Ethereum blockchain. Periodically, a Merkle root summarising all AvN activity is calculated and submitted to the storage contract on Ethereum.

7. **Token-manager** The token-manager pallet handles how tokens are managed on the AvN. It keeps track of the account balance of the individual tokens, the nonce of the account for all tokens held by the account, etc. Because the AvN is designed to be a L2, all tokens must be *lifted*[5] from a compatible L1. The lifting process is described in the next chapter.

8. **Validators-manager** This pallet provides functionality to add/remove validators. The pallet is based on the Substrate session pallet and implements related traits for session management when validators are added or removed. *Staking* is now directly on the Aventus blockchain via the Substrate Staking pallet. Our implementation of this pallet, however, involves additional verification and checks not present in the generic Substrate v3. Most of this was achieved by embedding it within the validators-manager pallet.

Validators

A validator is an authorised node that processes transactions and is capable of creating blocks on the chain. Data must be validated before it is written to new

[5] Lifting is the process of migrating a specified amount of an asset existing on L1, to L2.

blocks and validators participating in this are rewarded for doing so with AVT. Each validator has an Ethereum and Aventus address as they sign transactions that get submitted on both L1 and L2. The validators hold five session keys for five different tasks. As mentioned before, each key can be of one of two types, indicated in brackets:

1. Grandpa (Ed25519): Finality gadget.
2. Babe (Sr25519): Block production protocol.
3. Authority discovery (Sr25519): When a validator joins the network, it first attempts to identify other validators on the network as well as identify itself to existing validators.
4. I'm online (Sr25519): Periodic messages sent between validator peers to notify them of their continued presence in the network. The absence of continued *I'm Online* messages from a validator node results in its peers assuming the validator is offline (a state which could have real-world implications attached to it).
5. AvN (Sr25519): A validator's main key, which is used to create unsigned transactions.

There is another type of transaction, which is *unsigned*. An unsigned transaction is not required to pay transaction fees and be signed. Due to these characteristics, validators use unsigned transactions to communicate; sending information to the runtime. They use them to send orders to the blockchain and pass messages to other validators, for example, the *I'm online* heartbeat message. However, our custom pallets mandate that every validator signs these transactions using their AvN key. This is done so the validators can verify that the transaction is from a known validator. This check is of increasing importance in the fully decentralised network architecture, when new validator nodes get added to the network. These transactions are also useful for creating the Merkle root hash. While signatures have been demanded in our implementation of unsigned transactions, the key signing these transactions is the validator's session key which does not manage funds and thus cannot be subjected to paying a fee.

Off-Chain Worker

Off-Chain Workers (OCW) are commonly used by AVN network nodes to process and offload tasks that take longer than the block creation period and to interact with the outside world from within the runtime. An OCW is an agent started by a validator to do specific tasks and these workers run on a schedule. Some of these

tasks include: producing summaries, checking that another validator did the required work when they were supposed to, checking that an Ethereum event exists, etc. An OCW runs on a single node, so it can read from the chain. As consensus is required for anything to be written to the chain, an OCW cannot independently change state on the chain.

The following AvN pallets use OCW:

1. Ethereum-events
2. Ethereum-transactions
3. Summary
4. Validators-Manager

Pre-setup

At the beginning of each OCW process is a setup step that ensures it is safe to run the OCW. This checks that the node is a validator, that it has a valid account and that no other OCW is already executing for the same task and block.

Registration

For a Network User to actively participate in the Aventus Network as a Validator and earn rewards in AVT, they must be nominated by the community of AVT holders and, after registration, put down a validator deposit. This deposit acts as a validator's stake in the system and can be used as collateral to ensure proper behaviour via challenges.

To register, a potential validator must stake a minimum of 5000 AVT on the Aventus mainnet. This Validator is then considered part of the Aventus Network Validator pool and will begin earning rewards in AVT based on incoming gas fees from standard Network Users. This user must then run the Aventus Node on their machine performing transaction validation and acting as a form of income.

Validators must 'lock' a deposit of AVT so they have a stake in the system and have an incentive to validate data correctly (Validators found to be behaving maliciously will have their deposit funds slashed).

De-registration

In the inverse of the registration process, a Validator can choose to leave the Aventus Network and recover their deposit of AVT. To deregister, a Validator must notify the network of their intention to leave and wait for a cooling period to

conclude before being able to leave the Validator pool and recover their AVT deposit. This cooling period ensures any challenges can be made for the retiring Validator to ensure they don't commit a bad act and try to leave before allowing time for them to be caught.

Penalty and deposit slashing

The Network is designed with checks in place to allow participants to call out other participants if they are found to be acting maliciously, attempting to defraud the Network of funds or not online when expected. When a validator is found to be acting maliciously, the other validators can raise an offence; the aim of the offence is to cause economic harm to the validator and incentivise the proper behaviour of these users to ensure they do not defraud the network.

External Validators

On the 30th of March 2022, six proposals passed with a minimum of 1.4 million votes each on our governance platform. These proposals were put to the community to approve or reject the introduction of six new validator nodes, managed by third-party companies, on the Aventus Network, in an effort to further decentralise the network. As stated in the previous section, though these nodes are managed by different external parties, they are subject to penalties and deposit slashing, if found by the rest of the network to be acting maliciously.

3 Aventus Network

The AvN L2 is a Substrate-based blockchain designed as a scaling solution for Ethereum and beyond, capable of supporting various types of blockchain assets. Building on the architecture of the L2 laid out in the previous chapter, this chapter focuses on the facilities in L1 that facilitate communication between Layer 1 and Layer 2.

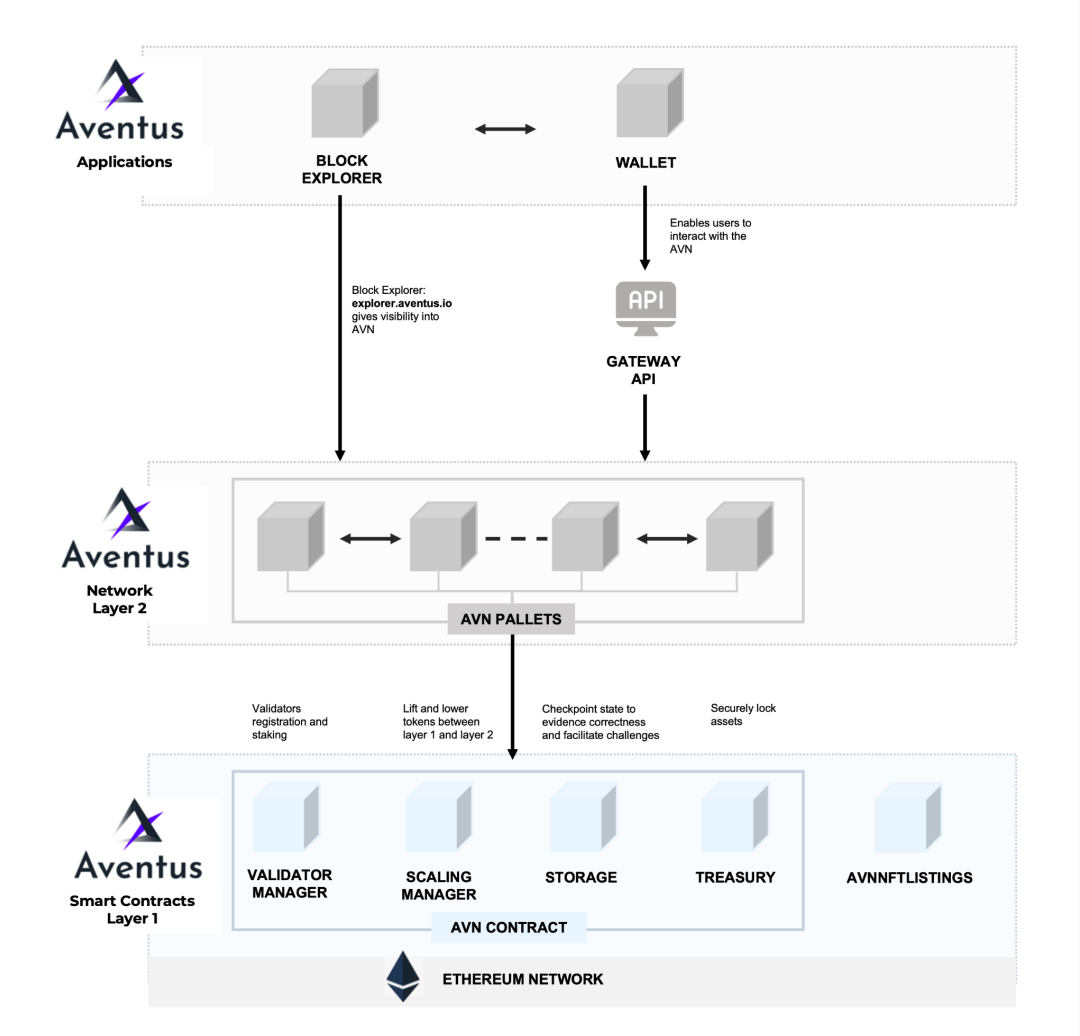

Figure 3: The Aventus Network

While the term *protocol*[6] might be justified here, L1 and L2 communicate based on a set of rules enforced by pallets and a smart contract on Ethereum. To achieve this on the Ethereum blockchain, *Solidity*[7] smart contracts have to be in

[6] A set of rules governing the exchange or transmission of data between devices or in this case, layers.
[7] The most popular and most frequently used language for Ethereum smart contracts.

place to act as our bridging interface with Ethereum itself. The current AvN architecture uses a single lightweight and gas-efficient smart contract.

This smart contract has three essential responsibilities: to verify and validate the Merkle tree roots calculated at specified intervals, securely move blockchain assets between chains, and ensure individual L2 transaction verification is possible by decoding the raw SCALE encoding transactions. Figure 4 shows how these smart contracts on Layer 1 achieve these three main tasks.

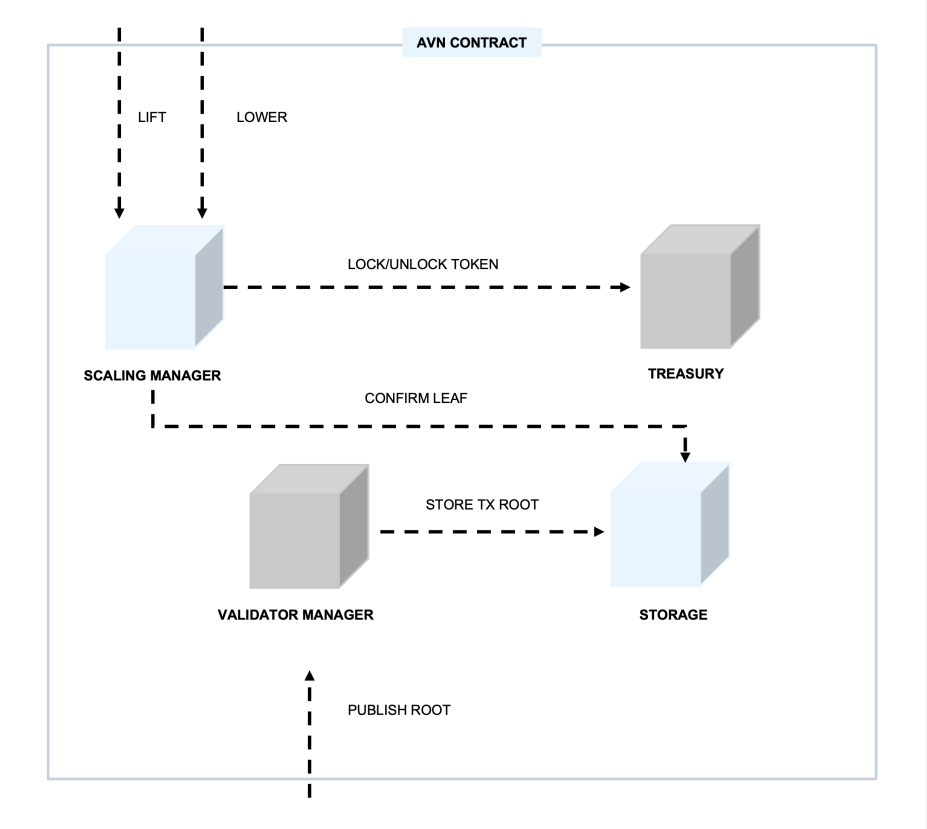

Figure 4: L1 Contract communication

This smart contract merges the previous four smart contracts (Treasury, Scaling manager, Storage, Validator Manager) removing the need for inter-contract calls. This single contract is cleaner, more gas efficient and handles reflective tokens better. Additionally, having this single contract also increases transparency and the ease with which the transaction history can be viewed. As discussed in the previous chapter, Aventus L2 is built on Substrate, and Substrate uses the SCALE codec. The contract is designed to decode Substrate SCALE-encoded

transactions. This means that all tier 2 transactions can now be published in their raw form to L1.

This removes additional processing from L2, achieving our goal of publishing 100% of the L2 transactions on L1. Additionally the use of more compact encoding saves gas on L1. The validation code now enables faster and cheaper publishing to L1 as the number of validator nodes grows.

L1-L2 communication

Thus far we have alluded to the fact that there is some sort of protocol that enables the communication between L1 and L2, and we have explored multiple participants in the communication procedure i.e., validator nodes, L1 smart contracts, RPC nodes, OCWs, etc. In this section, we will dive deeper into the design of the communication link, the inherent delays, benefits of the design, etc.

Communication between L1 and L2 is bidirectional. Communication can start from either L1 or L2 and this is determined by the nature of the transaction. For example, the publishing of Merkle root paths will always begin from L2. The main design goal of every L2 solution is to provide scalability to those willing to build on L1 but finding it too expensive and/or slow. Whatever the approach may be to providing scalability, it is expected that the L2 inherits from the security of L1 i.e. that although the transactions may be processed off the L1 chain, their immutability must be secured by the consensus and finality mechanisms of the L1 chain. The same applies to Aventus.

The AvN inherits security from Ethereum via the process of checkpointing handled by the *Summary* pallet. Every transaction executed on the AvN L2 is validated via the consensus mechanism on the chain. Periodically, the Merkle root of all the transactions executed on the AvN is calculated and the resulting root hash must be signed by $\geq \frac{2}{3}$ of the validators on the network before it can be accepted on Ethereum as valid. This implementation of consensus is based on a 'Plutocratic Finality' model - collecting signatures, aka a thumbs up, from each validator on the network that the data is correct before writing it via a Merkle Root to Ethereum.

While the *Summary* pallet handles the creation of summaries on L2, the Merkle root must be written to L1 in the form of a transaction, and all Ethereum-related transactions are handled by the *Ethereum-Transactions* pallet. This pallet ensures that transactions written to L1 from L2 are only written once and there is no replay attack. Publishing the current state of the ledger in the form of a

Merkle root hash on L1 provides the means to verify every transaction on the AvN till that point. However, due to how high gas fees are on the L1 blockchain, the rate at which summaries are calculated and published must be controlled. This rate has a knock-on effect on how quickly transaction journeys that start on L2 can finish on L1. At the time of writing, summaries are calculated every 24 hours on the L2.

There is still yet another pallet involved in L1-L2 communication, the *EthereumEvents* pallet. When a transaction is executed on the L1 contract, an event is emitted. This is the primary way L1 notifies L2 of significant state changes. Events that happen on L1 and should have a follow-up on L2 need to be declared by a L2 extrinsic. This adds them to a queue of unchecked events that keeps track of follow-up work that needs to be executed in the L2.

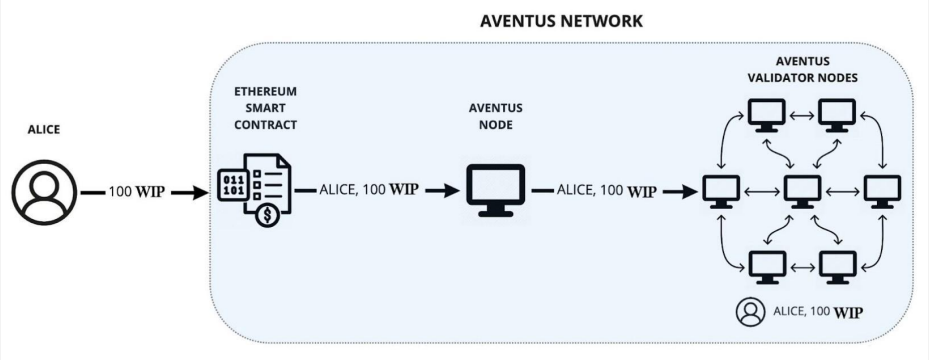

Figure 5: Lifting FT Assets to the AvN L2

Every L2 validator will look at the queue and check if it's their turn to do that kind of work. If it is, they will start an OCW to check the validity of an event. There is a challenge period of 60 blocks during which an event can be flagged as fraudulent, and this challenge must be from over 1/3 of the votes from validators. At the end of the challenge period, if there are not enough challenges, the event is deemed successful and marked as ready for processing. Another OCW is spun up to process and execute the event transaction, thereby completing the L2 action.

Based on this design, both L1 and L2 have a bidirectional communication path through which messages and assets can be transferred.

Migrating blockchain assets

The AvN supports the migration of tokens and for illustrative purposes, this section will cover the demonstration of the process by which FT tokens can be migrated between chains.

Lifting assets

Lifting assets is the process of migrating a specified amount of any FT e.g. ERC-20, ERC-777, and ETH etc., existing on L1, to L2. The AvN contract also allows for lifting native ETH to the Aventus network. More specifically, this process involves submitting these assets to the AvN contract which in turn registers the user's balance of the token and locks them on L1. The contract emits a corresponding event, and upon confirmation in L2, via an extrinsic with the hash of the L1 transaction, a representation of the exact balance of those assets is created in the lifter's L2 account.

In figure 5, Alice initiates the lifting process by calling the *lift* function on the AvN contract with function signature *lift(address FTContractAddress, bytes32 t2PublicKey, uint256 amount)*. The function takes as input the Ethereum address of the smart contract governing the asset on L1, the L2 public key of the token holder and the amount of the token the holder wishes to lift to L2. Upon successfully executing this transaction, given that all the "*require"* statements are passed, the tokens are locked in the contract and the ***logLifted*** event is emitted. One of the inputs is the L2 public key of the token holder, indicating the accounts that will be credited with the tokens. This usually belongs to the initiator of the L1 transaction.

The event emitted from Alice's transaction to lift 100 WIP is listened for by the AvN and by the service called *LiftSweeper*. Upon receiving the L1 event LiftSweeper triggers the network processing of the lifts on the AvN (i.e. on L2) designated to their specified L2 address. When the network receives this transaction, it selects another 'primary' node to go and check (using an offchain worker) if the event from the contract is valid. The result of that check is broadcast to the rest of the nodes of the network, which then validate this transaction by again comparing the hash provided matches with the event log originally publicly emitted by the contract and challenging it if they find discrepancies in the data.

Once consensus on this transaction is achieved, it is processed by the network in a new AvN block, and the balance of 100 WIP is stored against Alice's public address in the network solely under her custody.

Alternatively, this lift from L1 could be rejected if more than 1/3 of the validating nodes challenge the lift transaction to be incorrect, resulting in no WIP being represented in AvN for Alice. This transaction would only be found to be incorrect in two conditions, both involving a mismatch between the event submitted by the node and the L1 hash Alice has submitted to claim the tokens on L2. If the original Validator is found to be acting maliciously in this case by submitting incorrect data with their transaction, this Validator is punished to disincentivise malicious behaviour in the network (you can read more on validator management and penalisation in the Validator Management section in Chapter 2). However, if the fault lies with the L1 hash supplied by Alice (human error) to claim the WIP then Alice must retrace her steps. For the duration in which these tokens remain on L2, they cannot be used on L1.

ERC-20 and ERC-777 lifting costs no more than standard token transfers on Ethereum and ETH can now be lifted, for less than half the cost of an ERC-20 transfer. For ERC-777 tokens, operator lifting allowed another authorised party to lift tokens on your behalf. The AvN contract enables proxy lifting so the same can be done with ERC-20 tokens.

Lowering assets

Similar to the Lifting process, *Lowering* involves several security checks in the smart contract and passing consensus on both L1 and L2. Every transaction from the AvN to Ethereum must be signed by at least 2/3 of the validator nodes to be considered valid and verifiable by the L1 contract. There is a pallet created specifically for this called *Ethereum-transactions*. This pallet ensures every transaction to Ethereum is sent only once and it is properly authorised.

The network periodically checks back into L1 Ethereum with a transaction update containing the details of each transaction so that an immutable commitment from the L2 network also exists on L1. This underwrites the network with the security of Ethereum and allows for the smooth and safe migration of any asset existing on L2 to L1 for use in the wider Ethereum ecosystem.

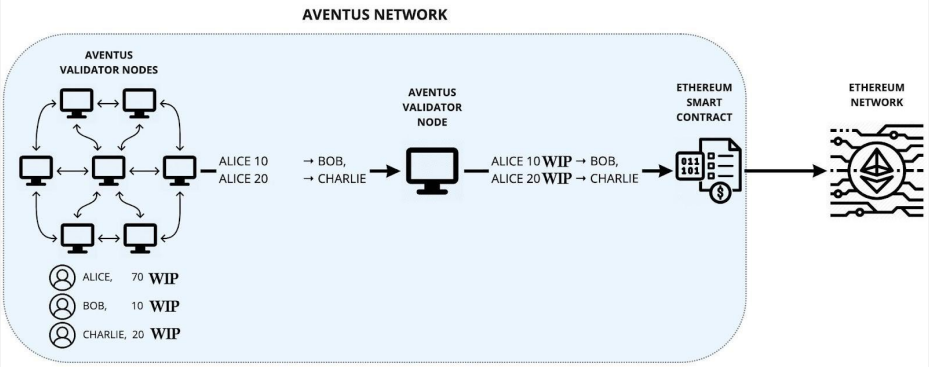

Figure 6: Lowering FT Assets from AvN L2 to L1

In figure 6, we see Alice transfer 10 WIP to BOB and another 20 WIP to CHARLIE. While Alice has no intention of lowering her remaining balance of WIP, BOB and CHARLIE are free to do so and initiate the lowering process by submitting the transaction on the AvN L2 to lower their balance of WIP. As every transaction on L2 is verifiable on L1 via the Merkle root hash published to the smart contract on L1. BOB and CHARLIE can then request to withdraw their tokens from the same contract on L1 by providing the *Merkle path* and the *encoded leaf*. Although this process is straightforward, withdrawal delay is subject to the summary schedule period on the network.

AvN Gateway API

The Gateway API is the fastest, least expensive and most convenient way to interact with the AvN. The function of the Gateway is to provide a familiar web API entry point to the AvN for integrating 3rd party applications and building new AvN-native products. Via the Gateway, users are able to create accounts, submit required volumes of transactions to the AvN, and query the blockchain state. The Gateway operates to enterprise-grade SLAs; it is built on modern microservices architecture which involves multiple RPC nodes, load balancers, queues, databases, and indexers, as shown in figure 7, to ensure its availability and robustness.

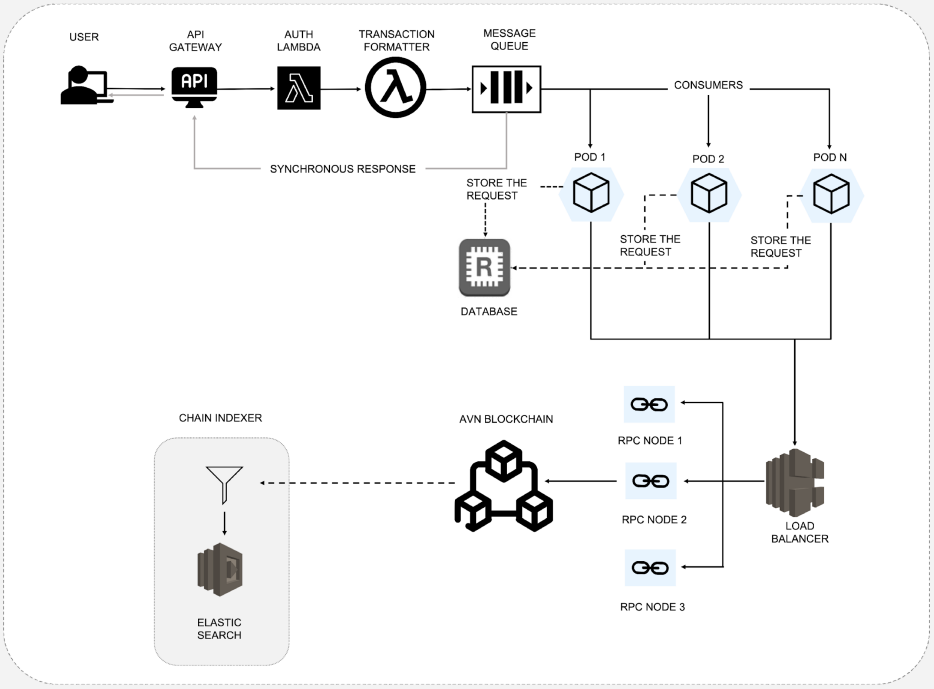

Figure 7: Gateway architecture

Prior to the Gateway, users attempting to access the AvN would either have to run their own node or connect to an RPC node. This is both expensive, cumbersome and can be insecure as it leaves the infrastructure open to various forms of attacks, not least of those Distributed-Denial-of-Service (DDoS). With the Gateway, both of these concerns have been addressed. The user can simply access the network by pointing the Gateway at a specified endpoint and transacting using an AvN address with a minimum balance of 1 AVT, free of the burden and expense of running a node. To solve any security concerns and prevent abuse of the network, all requests are done via HTTPS and are authenticated by our custom implementation of Javascript Web Token (JWT) using timestamps, Aventus Web Token (AWT). AWT is an extension of JWT. Each AWT is signed with the user's AvN account private key, and this signature can be verified using the user's AvN public key.

We decided to implement AWT, and extend the JWT standard, so we could streamline gateway authentication by allowing users to employ their AvN keys. The AvN, as many other blockchains, uses more advanced cryptography than that recognised in the JWT standard, which meant that a vanilla implementation would not be able to support AvN keys.

The Gateway has evolved over many different versions with support for transactions on any lifted ERC-20 token as well as varying operations on NFTs,

staking, split fee payment mechanism, total asset query, a whole bunch of utils and a non-zero nonce checker. With Staking now directly on the AvN, the Gateway can now allow for a greater degree of access to the staking program and flexibility in how users choose to stake, withdraw and view current staking statistics on the AvN.

Traditionally in blockchain interfaces the initiator of a transaction would have to pay the processing fees for the transaction. Aventus Gateway supports split-fee payment mechanism, which allows for a Delegate-payer: a specified account on the AvN can choose to cover the fee for a transaction. With this new mechanism, companies building on the AvN can underwrite their users' transaction processing fees, ensuring seamless consumer UX and enabling different formats of service relationships.

Another useful capability of the Gateway is the API facility that enables users to query the blockchain and instantly retrieve the IDs of all the blockchain NFT assets owned by an account. Last but not least, the non-zero nonce checker is introduced as a way to allow continued access to the gateway to regular users who might have a balance below 1 AVT but would still like to query the chain.

Every transaction that writes to the ledger via the Gateway is still subject to transaction fees, in AVT, however the Gateway does empower users with methods that allow them to know the cost of a transaction before continuing with them. Queries remain free.

Sesame Wallet

As part of our effort to make the Aventus network more accessible we now have a mobile app that’s powered by the Gateway API, see figure 3. This app is designed to cater to both new and existing users, allowing new users to easily create an account and providing existing users the functionality to recover existing AvN accounts. All users are able to create transactions, transacting on AVT, ETH and other ERC-20 compatible tokens, and in future iterations of the wallet, be able to view and transact on NFTs. The wallet also provides access to all staking functionality, enabling users to stake AVT and withdraw their stake at will. The wallet is also designed to interact with other dapps that allow for *WalletConnect* connections. This app is available for both iOS and android users.

4 AVT — The Aventus Token

The Aventus Token (AVT) is the native utility token in the Aventus Network. It's the fuel of the network, powering every transaction, supporting every validator, and proofing governance. Since the launch of the mainnet, there have been millions of transactions processed on the network, with each transaction yielding rewards in AVT for all the stakers.

There are four user personas:

1. Users (transaction originators): Users pay AVT as fees to the AvN for processing their transactions, enjoying low and predictable transaction fees on a scalable and secure network.

2. Validators (transaction processors): Validators deposit AVT when they join the AvN. This stake serves as a fraud deterrent. If a Validator seeks to damage the network by violating its rules, it is penalised directly.

   This aligns their incentives with those of the network.

3. Stakers (non-transacting): Anyone holding any amount of AVT can stake their AVT to earn rewards, assuming that AvN hasn't exhausted its stake capacity (reached validator staking limit).

4. Voters (non-transacting): AVT holders will see their votes carry weight equivalent to the amount of AVT they hold.

AVT[8] was launched on the Ethereum mainnet and has a total and max supply of 10,000,000. Approximately 60% of these AVTs were bought for 60,000 ETH[9] during an ICO in September 2017 within seconds.

At the time of writing, AVT is listed on some of the top centralised and decentralised exchanges, including Coinbase and Uniswap.

[8] Smart contract on Ethereum mainnet 0x0d88ed6e74bbfd96b831231638b66c05571e824f
[9] ether (ETH) is the native token of the Ethereum blockchain

5 Roadmap and Future Work

In the current stage of evolution of blockchain technology a number of platform capabilities are commonly viewed as 'standard', i.e. a sufficient level of their development is assumed to indicate the maturity of the platform / network. These are:

- Distributed control, security and privacy: decentralisation of validators and community governance.
- Business continuity: economic incentives for participants to maintain a functioning network in the long term.
- Enterprise infrastructure: business technical toolkit such as wallets, indexers, oracles etc required for any real-world business use-case.
- Developer infrastructure: developer resources such as libraries, API/SaaS/PaaS providers, integration documentation, etc.

Additionally, different blockchain networks seek advantage in any (or all) of the three interrelated problem areas listed below. Superiority in any of the following would usually be regarded as a winning quality:

- Cost
- Speed
- Interoperability (avoiding asset silos)

Major chains currently tend to emphasise and invest in competitiveness in the first two of the above, sometimes sacrificing aspects of the 'qualifiers' such as decentralisation to achieve attractive headline figures. There is a growing volume of effort underway to resolve the third problem, such as the Baseline project in the Ethereum ecosystem and Polkadot parachain architecture. However, this problem does not appear to have been definitively solved to this day.

Decentralisation

Our vision of the end-state of AvN features validator nodes distributed in geography and control, composing a fully decentralised PoS network managed and maintained by the community. Aventus has adopted the best practices and learnings from the Polkdadot roll-out program, and is generally following its milestones on the path of achieving the end-state vision.

Throughput, consensus and finality

This is the core value proposition of blockchain networks, and must be highly reliable. The significant complexity of scaling networks in a way that they continue to operate reliably and securely is apparent from the multiple reports on security breaches and system/network outages in other ecosystems. This is a high complexity engineering problem which requires deliberate attention, and the AvN team is planning to continue developing the network capabilities in this area by utilising the latest technological and scientific innovations.

Economics and rewards

Aventus will develop a system for dynamic AvN gas prices, and associated rewards to stakers and infrastructure providers (validator and node operators), as well as ability to lift or acquire AVT, stake validators and automatically monitor, pay / collect the rewards - all on the AvN. We will follow the community guidance and industry best practices to design and implement an appropriate (for the state of technology and the ecosystem) penalisation functionality, as the current simple approach is effective and efficient, but may result in misaligned incentives and punishments for operational errors once the network grows larger.

Network Governance

The Aventus team is looking at enabling change management in economic protocol and technology via a community governance process with on-chain (AvN) voting and execution in order to fully decentralise, and thereby avoid concentration of influence in the executors of community decisions. This will be supported by the development of the system for forkless automatic network software upgrades following the votes.

Recently, we have made significant strides in the area of governance with the revitalisation of our governance platform through the launch of six proposals. Each proposal required the Aventus community i.e. both AVT holders and stakers to vote to "accept" or "reject" the proposed company hosting a validator node. Given that there were six proposals, there were six companies seeking to be validator nodes. The result of the governance voting saw all proposals pass with a minimum count of 1.4 million votes each.

Open-sourcing AvN core

From the very start, it has been our intention to give the AvN community full control over the network, including its development and maintenance. We are

organising and gradually opening access to the core AvN source repositories for the public. This encourages external contributions, and enables independent due-diligence and auditing of Aventus technology.

Improved nodes/validators

We are planning to further improve the core technology and the usability of the validators to reduce the effort required from the community to run the AvN nodes and validators on commonly available hardware. Here are some of the initiatives from the AvN roadmap addressing this area:

- Automated QA of AvN components and their (and network) upgrades.
- Productise business continuity/resilience functionality in the nodes.
- Package nodes into easily distributable/installable software modules.
- Introduce telemetry and resilience functionality (such as telemetry, telemetry-exporter).
- Document operating procedures, upgrade and backup schedules, security best practices.
- Implement functionality for advanced economic incentives for running validators.

Enterprise infrastructure

AvN Wallets

The goal is to enable a convenient independent access to AvN for businesses and end-users, thereby facilitating the growth of account and transaction numbers as well as the ecosystem of third-party companies operating on AvN.

Many B2B2C use-cases require the capability for users to independently view/access/transfer their AvN-based assets across accounts. It is expected that the majority of users would be on-boarded onto AvN via online platforms providing end-user services, games and applications. However the philosophy of blockchain requires the presence of the self-sovereign wallet option, with self-custody of the keys. Aventus is encouraging 3rd party developers to build or port their existing wallet solutions to Aventus by providing grants, support and infrastructure, as well continuously working on enhancing the convenience of the enterprise-grade API provided by the AvN Gateway.

Custodial enterprise wallet solution

To enable companies to manage user accounts, associated keys and originate transactions on behalf of their customers, Aventus will be further enhancing the existing Aventus Key Vault solution for enterprise-grade key management.

Remote signer enterprise wallet solution

For the business cases where the keys need to be in the possession of the end-users, Aventus intends to develop a wallet and the associated server-side infrastructure components for transaction signing and relaying onto the chain.

Personal user wallet

Aventus ecosystem features the Sezame user wallet - a mobile application which enables independent user access to the network for purchasing, holding, transacting, lowering and lifting of NFTs and other AvN-based tokens. Aventus intends to develop and support others in expanding the capabilities of the existing products as well as growing the number of different end-user tools for interacting with AvN.

AvN Gateway product

Currently, users and businesses can benefit from the convenience of AvN Gateway API provided as a service by the Aventus team. However some corporate clients may require control and ability to maintain their own infrastructure for accessing AvN as part of their business continuity policy. Aventus will offer a packaged product based on the AvN Gateway technology.

AvN Indexer

Enhance the capabilities of the AvN indexer to provide additional information about AvN transactions (including failed), pallets, rewards and various other network statistics (ratings of active validators, tokens, funded accounts, etc) to simplify access to the information stored on the AvN for business as well as general public.

AvN Oracles

Aventus is planning to work on developing AvN Oracle technology and infrastructure to enable common DeFi and other ecosystem applications.

AvN developer sandbox

Aventus is currently providing external parties with a stable, supported, documented sandbox environment - a public testnet - to allow testing of integrations and network updates prior to their deployment against/on AvN mainnet. We will continue enhancing our level of service to the community with improvements in the following areas:

- Fully functional AvN deployment.
- Developer and user documentation.
- Account/keypair generation.
- Signing.
- Integration with AvN Gateway.
- AVT Faucet.

AvN capability evolution

Aventus is strategically interested in extending support for a wider set of FT, NFT and future token standards, as well as different blockchain platforms, distributed services (such as IPFS) and innovative business logic associated with various token types opens up the network to a broader set of actors by enabling more transaction originators to utilise cheaper and faster AvN for their use-cases in gaming, ticketing, music / video and other industries.

Polkadot parachain

Aventus is working on bringing AvN into the Polkadot ecosystem via AvN becoming a Polkadot parachain. Furthermore, we intend to make AvN a bridge between the Ethereum ecosystem and Polkadot, while increasing the utility of AVT, preserving prior AvN transactions and maintaining the ability for AvN to function independently.

- Support multiple token types and standards for cross-platform transfer.
- Maintain the use-case for AVT as the ‘fuel’ for AvN transactions.

Full standard ERC-721 support in AvN

Our roadmap contains plans to further improve AvN NFT implementation by ensuring full support for ERC-721[7] token standard, and by offering lift and lower user flows as currently supported for all fungible tokens.

Scalable NFTs with ERC-1155

The emerging 1155 [8] standard offers opportunities for more scalable 'hybrid' tokens. AvN is planning to adopt ERC-1155 and implement full support for the compatible tokens including lifting and lowering.

Interoperability with IPFS

AvN will standardise and support access to data located on IPFS.

Innovative tokens (NFTs and beyond)

Innovation in the blockchain space continues, in the NFTs and other emergent token types. AvN intends to stay on the forefront of such developments. Aventus team will research and develop newly invented capabilities for NFTs such as 'breading', 'evolving', 'expiring', 'emoticons' as well as enable the creation of custom AvN tokens by network users.

Privacy (roll-ups)

Privacy blockchain technology has matured to the extent that it can now be deployed for production use-cases. AvN will implement Ethereum and Polkadot compatible algorithms to enable privacy preserving transactions on and across chains.

6 Conclusion

We have introduced Aventus Network, a third generation composable blockchain network capable of providing the foundation layer for business applications in a wide range of domains, including loyalty, vouchers, gaming, financial assets, virtual goods, supply chain and healthcare.

We demonstrated how the network is constructed, elaborating on the fundamental architectural decisions, technical design and functioning of the blockchain platform. The technology allows for the high-throughput operation of the blockchain independently or as a Layer 2 on Ethereum, while also being integrated into the Polkadot ecosystem in the near future.

Finally, we have presented a roadmap of future work intended to enhance the platform's usability, security, privacy and interoperability.

Bibliography

[1] Aventus, “Aventus Classic Whitepaper,” 2019. [Online]. Available: https://github.com/AventusProtocolFoundation/docs/blob/master/resources/Aventus%20Classic%20Whitepaper.pdf

[2] M. Bez, G. Fornari, and T. Vardanega, “The scalability challenge of ethereum: An initial quantitative analysis,” *Proceedings - 13th IEEE International Conference on Service-Oriented System Engineering, SOSE 2019, 10th International Workshop on Joint Cloud Computing, JCC 2019 and 2019 IEEE International Workshop on Cloud Computing in Robotic Systems, CCRS 2019*, pp. 167–176, 5 2019.

[3] “Hard Fork Completed | Ethereum Foundation Blog.” [Online]. Available: https://blog.ethereum.org/2016/07/20/hard-fork-completed/

[4] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” 2016.

[5] “Layer 2 Scaling | ethereum.org.” [Online]. Available: https://ethereum.org/en/developers/docs/scaling/#layer-2-scaling

[6] “POLKADOT: VISIONFOR A HETEROGENEOUS MULTI-CHAIN FRAME-WORK.” [Online]. Available: https://github.com/ethereum/wiki/wiki/ Chain-Fibers-Redux

[7] “EIP-721: Non-Fungible Token Standard.” [Online]. Available: https://eips.ethereum.org/EIPS/eip-721

[8] “EIP-1155: Multi Token Standard.” [Online]. Available: https://eips.ethereum.org/EIPS/eip-1155

Appendix

Ancillaries

Acknowledgements

The authors owe their gratitude to Alan Vey, Alex Pinto, Nahu Seyoum, Glyn Dimond, Thanos Doukoudakis, Fernanda Ribeiro, Micael Franco for their tireless work on building, improving and evangelising the Aventus Network, and for the insights and contributions to the content and design of this paper.

We would also like to thank the community of engineers, blockchain experts, and users of Substrate library and many other frameworks, protocols and components we have built upon, who thereby contributed their knowledge and skills to the development of Aventus Network.

List of Figures

Abbreviations

AIP	Aventus Improvement Proposal
AVT	Aventus Token
AWT	Aventus Web Token
BABE	Blind Assignment of Blockchain Extension
DDoS	Distributed-Denial-of-Service
ECDSA	Elliptic Curve Digital Signature Algorithm
FT	Fungible Token
GRANDPA	GHOST-based Recursive ANcestor Deriving Prefix Agreement
JWT	Javascript Web Token
L1	Layer 1
L2	Layer 2
mempool	Memory Pool
NFT	Non Fungible Token
NPoS	Nominated Proof of Stake
OCW	Off-Chain Worker
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance

PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
RPC	Remote Procedure Call
VRF	Verifiable Random Function
WASM	WebAssembly