Aventus Network

Technical whitepaper

Andrey Brozhko, C. Emmanuel Ngubo

Version 1. March 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, low and predictable transaction costs. The network currently operates as a layer-2 to 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 and 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's 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, however, 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 designed to be scalable, support the execution of code, and be composable. This is a generation 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, making it faster and cheaper to transact, for example, 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 business.

Aventus

Aventus' journey began in 2018 providing blockchain-powered solutions to the ticketing industry with 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. 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 planned 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 Layer 2 (L2) solution designed to achieve the required levels of scale and privacy on Ethereum without compromising on native security and independence. The team has enhanced and adapted the 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 the Aventus token (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 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, the average cost is $0.01 (paid in AVT). This is not only 99% cheaper than the average Ethereum transaction fee over the past year, 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 business 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 a whitelabel NFT platform that empowers brands & companies in the creation of their own NFT marketplaces with no technical expertise needed. Athletes, artists, musicians, and corporate companies build NFT marketplaces with VereNFT to generate additional revenue while maintaining full control of their brand and their data.

FanDragon

FanDragon's Universal Smart Ticket Wallet provides a platform for dynamic and networked tickets that connect fans with artists and brands before, during, and after the event. The Future Ticket is dynamic and networked, with a 3D ticket that engages with its holder, offering access and entertainment for the lifetime of a fan, not just of the event. FanDragon has most recently done a deal for its ticket wallet with industry titan, Live Nation.

Vow

Aventus helped CashbackAPP increase their net margins by as much as 25 percent in just six months in multiple business jurisdictions through vowcurrency.com. As a business that gives users cashback on purchases, they were able to restructure their loyalty debt obligation on their balance sheet, reduce transaction fees, and improve treasury management while providing customers with more prompt payment.

FruitLab

FruitLab is a social network for gamers that enables creators and community members to earn revenue from clips of their gaming with PIPs. PIPs are tokens for gamers that provide a secure method for creators to monetise content. With more than 100,000 monthly active users, fruitlab is an established and growing platform on web and app for the world's gaming community. Aventus securely and cost-effectively executes all fruitlab token transactions.

Artos

Artos Systems is fixing agrifoods trade, allowing users to showcase their products and close deals quickly. Artos' B2B commerce and deal negotiation platform helps agrifoods companies of all sizes, from startups to global enterprises, generate more new business and close deals faster. Artos has over 30 clients and is rapidly expanding.

2 Architecture

The Aventus Network comprises both Layer 1 (L1) and Layer 2 (L2) technologies. These two layers communicate important transaction information state changes etc between blockchains. 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 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/

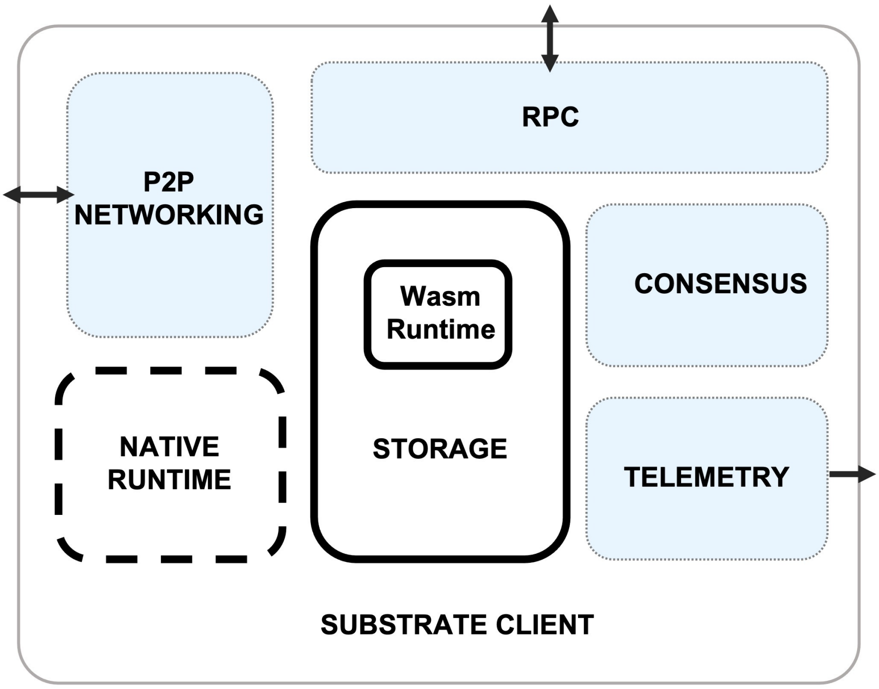

Figure 1: Substrate Client

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.

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 an 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 as 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 two types of nodes on the AvN: RPC 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. 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. The RPC nodes do not have all these responsibilities and thus can be thought of as "light". The term "light" here means that they do not have to store the history of the chain and are not weighed down with the computation-intensive tasks required to validate transactions and author blocks.

There are currently 10 validator nodes and two RPC nodes on the network. The RPC nodes serve to answer queries and propagate requests to the validators as needed; relaying answers back to users, while the validators validate each transaction and process them into blocks. To promote decentralisation, the most prevalent network in most blockchain implementations is the Peer-to-Peer (P2P) network. 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.

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 extrinsic submitted to the chain has to be signed by the sender before this transaction is executed in the runtime by all validator nodes. Given that all validators must share the same state, each transaction is validated and the validators must reach a consensus on the accep-

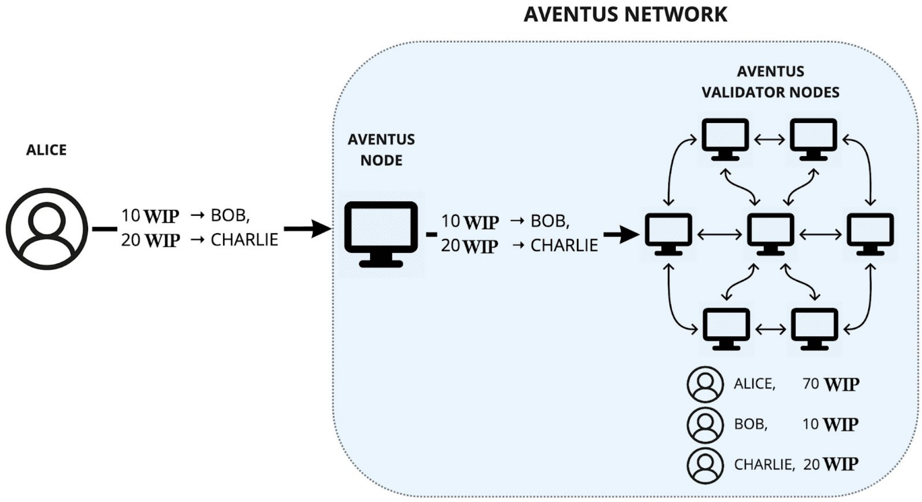

Figure 2: Executing an extrinsic on the AvN

tance 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 Memory Pool (mempool), which is a queue for incoming transactions waiting to be picked up by validators for processing. The validator nodes watch the mempool and validate the incoming data for the correct signatures and valid data structure. On L2, validators are not currently incentivised to prioritise certain transactions based on how much "gas" the extrinsic sender is willing to pay. Hence, we can expect that the transactions are executed in a first in / first out fashion. 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 and no WIP is sent from Alice’s account and Bob and Charlie remain with 0 balance.

Runtime and client

The runtime handles the low-level logic of the blockchain i.e. the state transition logic and how blocks are appended to the chain. The client is the code implementing the communication logic, running on every validator, which receives network connections, receives all the requests from outside the network, and on occasion communicates with the other nodes. The AvN runtime and client are configured

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

differently from the base Polkadot and Substrate configurations. The runtime is created by the client and it operates similar to a virtual machine running inside the client. It is where all the extrinsics[3] are executed. The runtime running in every client operates the same way regardless of the underlying operating system. Therefore, the runtime could be viewed as a shared workspace among all the validators, and the members of the chain. The runtime has limited capabilities to ensure that every action performed is deterministic. Runtimes also perform another major function of enabling forkless upgrades. New upgrades are compiled into WASM and stored on the chain, which therefore enables a forkless upgrade.

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.

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 nodes take turns validating transaction sets and transactions, 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

[3] Also known as Transactions

with an underpinning reality of a probabilistic finality, GHOST-based Recursive ANcestor Deriving Prefix Agreement (GRANDPA) ensures the deterministic finality.

Block creation

Blocks are created on the L2 every 3 seconds and can be viewed on the block explorer [4]. The resolution must be fast. One block is produced every 3 seconds. The whole of the transactions in one block must run under 1 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. So this limit should be adjusted such that the block's transactions do not go over 1 second.

Pallets

Pallets are a special kind of Rust module 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 9 pallets in operation.

1. **AvN** This pallet provides functionality that is common for other AvN pallets such as handling off-chain workers, validations, and 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. **AvN offence tracker** This pallet provides functionality to call Ethereum transactions to slash the offender and implements the OnOffenceHandler.
4. **Ethereum-events** This pallet provides functionality to get ethereum events.
5. **Ethereum-transactions** This pallet handles Ethereum-related transactions.
6. **NFT-Manager** This pallet integrates NFTs into the Aventus blockchain on an infrastructure level allowing for the minting of NFTs without smart contracts.
7. **Summary** This pallet handles the checkpointing to the Ethereum blockchain. Periodically, the merkle root is calculated and submitted to the storage contract on Ethereum.

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

8. **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.
9. **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.

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 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. As stated earlier, there are two types of cryptography used in the AvN L2. The validators, via these cryptography types, generate 5 keys for five different tasks:

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, used to create unsigned transactions.

There is another type of transaction which is unsigned and the difference between the signed and unsigned is that an unsigned transaction is not required to pay transaction fees and be signed. Due to these characteristics, validators use unsigned transactions to communicate amongst themselves. They use them to send

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

orders to the blockchain and pass messages to other validators, for example, the *I'm online* heartbeat message. However, as every validator in the AvN must be known, the AvN requires these transactions to be signed using the AvN key. The validators use this key to sign the unsigned transactions. This is done so the validators can verify that the transaction is from a known validator. These unsigned transactions are also useful for changing of summary slots and 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 Worker (OCW) are commonly used by AVN network nodes to process and offload tasks that take longer than the block creation period. 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. 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, it calls the pre-run setup function defined in the AVN pallet. This pre_run_setup function validates to see if this node needs to do the OCW tasks or not at the current block. If it does, then OCW will continue with the tasks listed below in each pallet section, otherwise the process will terminate immediately.

The pre-run setup covers the following checks:

1. The node is a validator.

2. The node holds a validator account locally.

3. No other OCW working on the same block.

Registration

For a Network User to actively participate in the Aventus Network as a Validator and earn rewards in AVT, they must first register themselves and put down a deposit. This deposit acts as a user's stake in the system and can be used as collateral to ensure proper behaviour via challenges.

To register, a user must send a transaction to a smart contract deployed to Ethereum along with their deposit of 250,000 AVT. This deposit is then stored against their account and the contract emits an event that is listened for by the network to alert all other nodes of a new Validator entering the pool. 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 de-register, a user 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 exiting 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 being online when expected. When a validator is caught acting maliciously, the other validators can raise an offence; and the idea of the offence is to cause economic harm to the validator. There is logic written into the system to regulate and incentivise the proper behaviour of these users to ensure they do not defraud the network.

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.

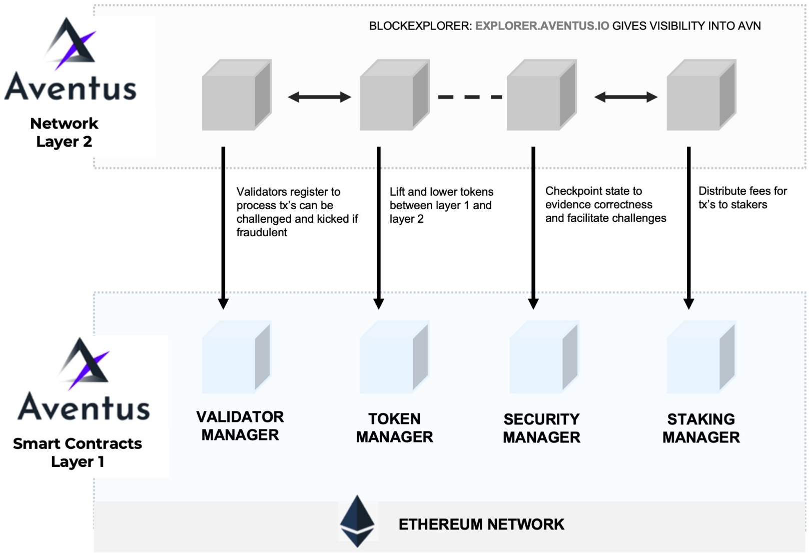
BLOCKEXPLORER: EXPLORER.AVENTUS.IO GIVES VISIBILITY INTO AVN
Aventus
Network
Layer 2
Validators register to process tx's can be challenged and kicked if fraudulent
Lift and lower tokens between layer 1 and layer 2
Checkpoint state to evidence correctness and facilitate challenges
Distribute fees for tx's to stakers
Aventus
Smart Contracts
Layer 1
VALIDATOR MANAGER
TOKEN MANAGER
SECURITY MANAGER
STAKING MANAGER
ETHEREUM NETWORK

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 multiple contracts and pallets. To achieve this on the Ethereum blockchain, *Solidity*[7] smart contracts have to be in place to act as our bridging interface with Ethereum itself. The current AvN architecture uses 4 lightweight and gas-efficient smart contracts:

1. **ScalingManager**: As most transactions on a blockchain involve interaction with blockchain assets (both FT and NFT), this contract handles the successful migration of these assets between layers. It's rightly named the Scaling Man-

[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.

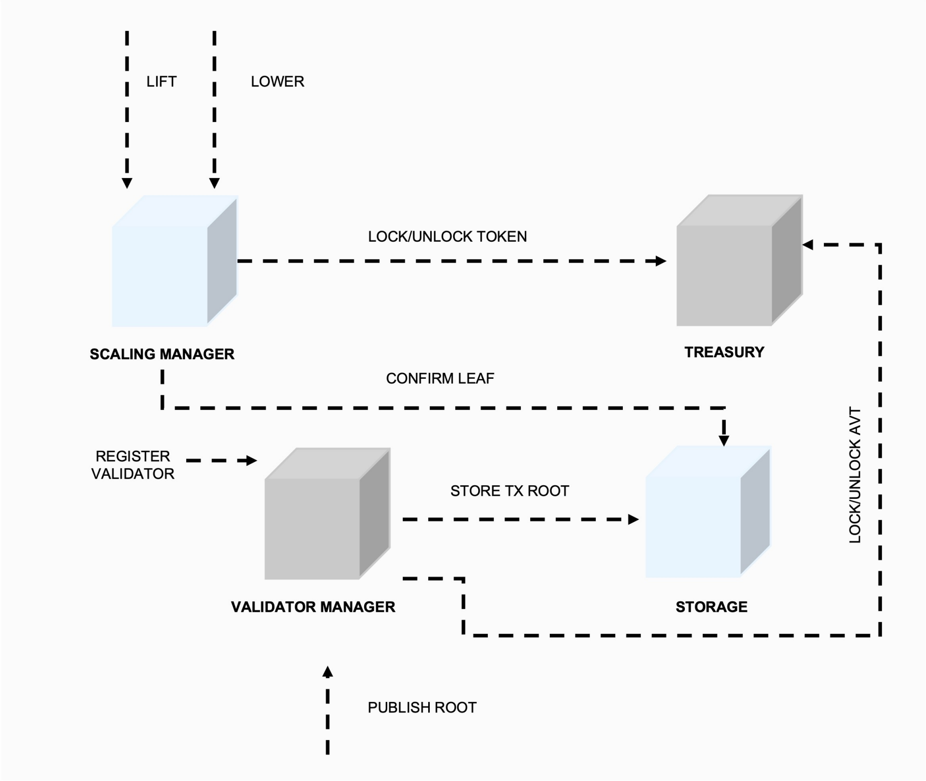

Figure 4: L1 Contract communication

ager as it moves these assets to the more scalable L2 where transactions can be executed on them faster and cheaper than they could have been if they remained in L1.

2. **Treasury**: Assets submitted to the AvN L1 for migration to L2 must be securely locked in a smart contract on L1 before they get released on L2 for the use of the asset submitter. Hence, the Treasury contract holds all token balances currently locked in the system including the validator deposits in AVT.

3. **Storage**: This contract holds the weight of the AvN L2 as it is permanent storage for the published Merkle roots submitted by registered and activated validators on L2.

4. **Validator manager**: This L1 contract manages the authorisation and activity of L2 Validators. As the AvN operates a POS consensus mechanism, all validators must be registered and tender an amount in AVT, from here on referred to as a *deposit*. Hence, this contract handles validator registration, activation, deregistration, deposit claim and slashing, and finally Merkle tree root publishing by the validator.

These four contracts work as a unit to enable communication between L1 and L2 and to enforce the rules preset in the contract. These contracts have 3 main responsibilities which are to manage the L2 validators, verify and validate the Merkle tree roots calculated at specified intervals, and securely move blockchain assets between chains. Figure 4 shows how these smart contracts on Layer 1 achieve these 3 main tasks.

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, AvN nodes, 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, validator registration will always start from L1 and the publishing of Merkle root paths will begin from L2. The main design goal of every L2 solution is to provide scalability to those willing to build on L1 but find 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 hash 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. These signatures are carried out by off-chain workers which exist for the main purpose of executing long-running tasks that the validators would have had to do. 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, and also the possibility of resetting the AvN to a previously accepted state if required. 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 *Ethereum-Events* pallet. When a transaction is executed on any of the contracts in L1, an event is emitted. This is the primary way L1 notifies L2 of significant state changes; and the off-chain worker also has the task of listening for AvN related events from L1. These events go into a queue of unchecked events. Queues are created for the work that is left to be done and 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. It runs without the restriction of the runtime. 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, the event is now ready for processing. Another off chain worker is spun up to process and execute the event transaction.

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 both FTs and NFTs tokens but, for illustrative purposes, this section will be limited to demonstrating how Fungible Tokens can be migrated between chains with ease.

Lifting assets

Lifting assets is the process of migrating a specified amount of any FT e.g. ERC-20, ERC-777, etc., existing on L1, to L2. More specifically, this process involves submitting these assets to the Scaling Manager contract which in turn locks them in the Treasury contract, and upon confirmation to the AvN L2 via an event, a representation of the exact balance of those assets are ready to be unlocked on the AvN via the resulting transaction hash from L1.

In figure 5, Alice initiates the lifting process by calling the lift function on the Scaling Manager with function signature *lift(address FTContractAddress, bytes32*

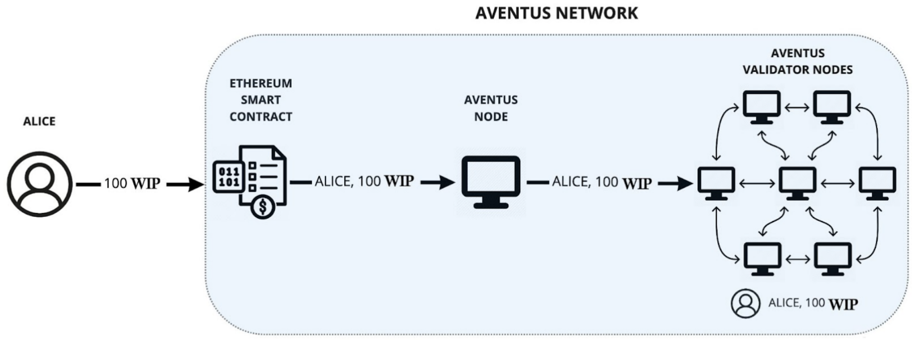

Figure 5: Lifting FT Assets to the AvN L2

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 *required* statements are met, the tokens are locked in the Treasury contract and the *logLifted* event is emitted. As one of the inputs is the L2 public key of the token holder, it is therefore imperative that the transaction initiator have an AvN account through which they can receive/unlock the funds on L2.

The event emitted from Alice's transaction to lift 100 WIP is listened for by the AvN. Anyone running an Aventus Node can pick up this event log for Alice lifting 100 WIP and submit it to the rest of the network for validation as a regular transaction. When the network receives this transaction, it selects another 'primary' node to go and check 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 as incorrect. This transaction would only be found 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, resulting in no WIP being represented in AvN for Alice. 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. 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.

Lowering assets

Similar to the Lifting process, Lowering involves several security checks via multiple smart contracts 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 contracts. 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 state 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 migration of any asset existing on L2 to L1 for use in the wider Ethereum ecosystem.

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 *Storage* smart contract on L1. Bob and Charlie can then request to withdraw their tokens from the *Scaling Manager* 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.

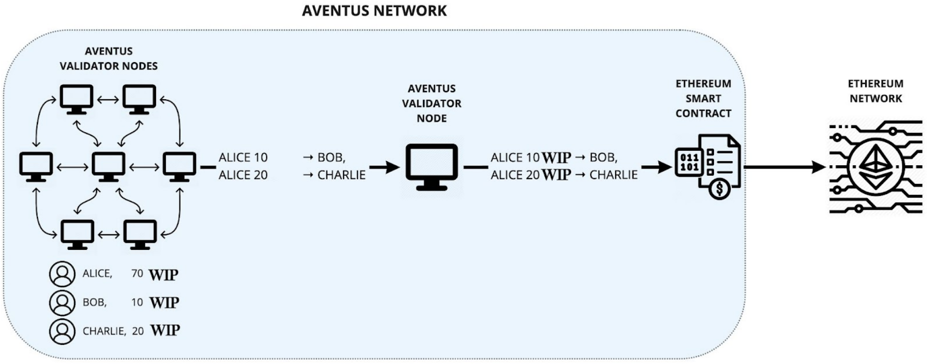

Figure 6: Lowering FT Assets from AvN L2 to L1

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 micro-services architecture which involves multiple RPC nodes, load balancers, queues, databases, and indexers to ensure its availability and robustness.

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 and non-secure as it leaves the infrastructure open to various forms of attacks, not least of which would be Distributed-Denial-of-Service (DDoS). With the Gateway, both 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). Our AWT is an extension of JWT mainly to the use of an elliptic curve compatible with the AvN, allowing for the use of AvN keys for authorisation. 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.

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 transaction before continuing with them. Queries remain free.

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 of approx $0.01 on a scalable and secure network.

2. Validators (transaction processors): Validators deposit AVT when they join the AvN. This stake serves the purpose of being a fraud deterrent. If the Validator seeks to damage the network by violating its rules, they are 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 there is at least one validator on the AvN that hasn't reached its stake 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, meaning there will be no minting of new AVT. 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 toolkits 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 for 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 Polkadot roll-out program, and generally follows 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 using 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 the 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 community governance processes 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.

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 planning to organise and open access to the core AvN source repositories to the public to encourage contributions of code and to enable independent due-diligence and auditing of 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 3rd 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 intends to build on the convenience of the enterprise-grade API provided by the AvN Gateway, and introduce multiple Wallet solutions covering the majority of business use-cases.

Custodial enterprise wallet solution

To enable companies to manage user accounts and associated keys and originate transactions on behalf of their customers, Aventus is working on a Key Vault solution suitable for enterprise-grade key management.

Remote signer enterprise wallet solution

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

Personal user wallet

Aventus is developing a solution to support independent user access to the network for purchasing, holding, transacting, lowering and lifting NFTs and other AvN-based tokens, and developing a metamask-like user interface solution.

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

Develop an AvN indexer to provide 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.

AvN Oracles

Provide AvN Oracle technology and infrastructure for 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

Extending support for a wider set of FTs, NFTs 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 wider set of transaction originators to utilise the cheaper and faster AvN for their use-cases in gaming, ticketing, in music/video, and in 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.
- Ability to function in the absence of other chains (gracefully degrading the security/performance).

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

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 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’, ‘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: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK.” [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 A

Ancillaries

Acknowledgements

The authors owe their gratitude to Alan Vey, Alex Pinto, Nahu Seyoum, Glyn Dimond, Thanos Doukoudakis, Fernanda Ribero 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

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