- AyA -

Torben Poguntke
World Mobile Group
torben.poguntke@worldmobile.io

Juan Alonso Margareto
World Mobile Group
juan.margareto@worldmobile.io

Antonio Hernández
World Mobile Group
antonio@worldmobile.io

March 31, 2023

Contents

Abstract

The World Mobile Chain (WMC) is a novel telecommunications system that contains a blockchain network, named EarthNode Network. The EarthNode Network is composed of the following:

- One or more Layer 1 blockchains serving as the Financial Settlement Layer
- One blockchain (which could be part of the previous set) acting as the Trust Layer
- The Telecommunications Settlement Layer, which consists of a sidechain and the common components between blockchains in the Financial Settlement Layer. The name of this sidechain is AyA.

AyA is an Adinkra symbol, from West Africa, that translates to Fern. In the Adinkra tradition, it is a symbol of endurance and resourcefulness. The fern is a hardy plant that can grow in difficult places, just like the WMC will grow in the territories where deployment is most complex.

The software of an EarthNode contains an AyA node; it also allows EarthNode Operators (ENOs) to offer their resources to provide infrastructure for Value-added Services and Communications-as-a-Service. Customers keep their financial assets on the Financial Settlement Layer. The chain that serves as Root of Trust holds the Operator's EarthNodeNFT (ENNFT), which allows them to establish their EarthNodes. Delegators hold World Mobile Tokens (WMTs) and stake them to one or more EarthNodes.

AyA provides the Telecommunications Settlement Layer of the EarthNode network. The validator nodes inside the EarthNodes participate in the AyA consensus mechanism to reach agreement and achieve finality.

Each validator must be registered on the Root of Trust chain and be verified against this registration before it can participate in the AyA consensus. The AyA consensus is powered by the selection of a committee (the AyA Committee), which is the set of nodes operating the trustless interface to the Layer 1 chains in the system. This AyA Committee is a rotating and randomly-selected subset of all the EarthNodes.

Keywords: WorldMobile, Blockchain, Sidechains

Acronyms

AC AyA-Committee.

AV AyA-Validator.

BFT Byzantine Fault Tolerance.

DKG Distributed Key Generation.

EN EarthNode.

ENN EarthNode Network.

ENNFT EarthNode Non-Fungible-Token.

ENO EarthNode Operator.

ENOPNFT EarthNode Operator Non-Fungible-Token.

eUTxO Extended UTxO.

FROST Flexible Round-Optimized Schnorr Threshold Signatures.

GDPR General Data Protection Regulation.

GDST General-Data-Settlement-Transactions.

L1 Layer 1.

L2 Layer 2.

Ped-DKG Pedersen's Distributed Key Generation.

TDST Telco-Data-Settlement-Transactions.

UTxO Unspent transaction output.

WMbft World Mobile Byzantine Fault Tolerance.

WMC World Mobile Chain.

WMT World Mobile Token.

Glossary

AyA Name of the Layer 2 Sidechain.

AyA epoch The period a particular AyA Committee is in charge. Its length is bound to Root of Trust.

Delegator An end-user allocating WMT to one or more EarthNodes.

Financial Settlement Layer Public blockchain network where the customers hold their financial assets.

Staker An end-user allocating WMT to one or more EarthNodes.

Telecommunications Settlement Layer World Mobile blockchain network that manages and stores telecommunications data.

Trust Layer Source of truth for the connection to and from AyA.

1 The EarthNode Network

The name, ENN, refers to the combined blockchain system developed by the World Mobile Group. Integrated in the WMC, the ENN provides various functions needed by decentralised applications, including the following:

- A highly decentralised and secure Financial Settlement Layer to handle assets
- A scalable and competitive Telecommunications Settlement Layer, which allows the immutable and trustless storage of data

The WMC also includes the uplink to the telecommunications world. In a nutshell, the WMC builds on the following foundations:

- Connectivity
- Identity
- Finance

Every end-user of WMC will enjoy these three foundations. In addition, WMC allows third-party developers to tap into these foundations and run new types of applications directly on the end-user's smartphone.

The following illustration provides a high-level view of the ENN and its place in the WMC:

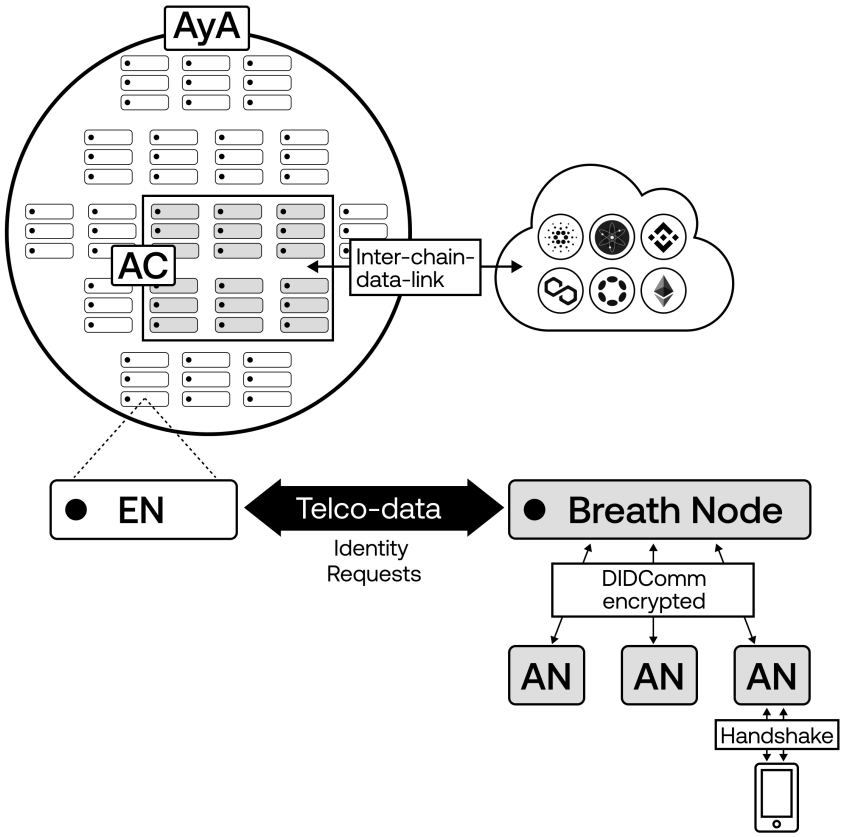

Figure 1: EarthNode Network Overview

1.1 Root of Trust and Financial Settlement Layer

The ENN comprises several Financial Settlement Layers and a Telecommunications Settlement Layer that are bound to a single Root of Trust L1 blockchain. A Financial Settlement Layer is a blockchain network that can operate the assets of the WMC and has a binding to the Telecommunications Settlement Layer. Root of Trust is a single blockchain that serves as a Financial Settlement Layer and also shares security and ensures the integrity of the Telecommunications Settlement Layer.

In addition to security, other important factors for an L1 chain to be considered as Root of Trust are high decentralisation, reliability, handling

for updates and smart contract execution. As World Mobile Token (WMT) was minted on Cardano and enjoys the same benefits as other native assets, it is a suitable candidate for Root of Trust. This paper presents a solution that considers Cardano as Root of Trust. Cardano has a higher complexity due to the eUTxO model than account-based chains; however, the solution also works for such chains. A future paper will elaborate on integration into account-based L1 chains.

The binding between the layers ensures that an AyA-Sidechain cannot validly operate without its Root of Trust. Validators of the sidechain must be registered on Root of Trust to propose and verify blocks, become part of an AC, or become a cross-chain leader.

Any breach of these bindings would result in transactions being rejected on the Root of Trust blockchain, because the validating smart contracts would not be able to verify the signatures of the committee. In this situation, the Telecommunications Settlement Layer would become invalid unless a new valid committee is set up within a specified period.

When invalid, the sidechain cannot generate rewards, as rewards are paid on the Financial Settlement Layers, which no longer accept cross-chain transactions. To re-establish a valid Telecommunications Settlement Layer, a new sidechain would be needed, retiring the previous, invalid, chain.

1.2 AyA —Telecommunications Settlement Layer

There are several options for blockchain solutions acting as Root of Trust and Financial Settlement Layer, however they all come with trade-offs. For example, transaction size limitations, cost of transactions, storage of data, block propagation time, and possibilities for parallel processing. In the world of telecommunications, as well as for the sharing economy, those constraints must be considered to create real-world solutions. We overcome them in a scalable and trustless way with the help of our Telecommunication Settlement Layer - AyA.

AyA differentiates between TDST and GDST.

TDST is specific to the tracking of telecommunication events, such as call starts and ends. It is standardised, and only contains hashes of telecom-

munication events. Only verified and authenticated network participants can submit TDST transactions to the network, and no transaction fees are charged for the blockchain transactions.

The settling of telecommunications events for the WMC is essential for both the ENN and the trustless storage of accounting data. Although not stored directly on the blockchain, the data must comply with the legal requirements of the country where the events occur, such as GDPR. Each country holds a registry, which stores this telecommunications data in a key value store. The key for each event is the hash of its value. This hash uniquely identifies the data entry and is immutably stored with its respective data on AyA.

GDST can be created by any network participant. Whilst TDST does not require the payment of any fees, GDST incur transaction fees that scale with the size and computational power required for execution. This category contains all transactions that are not TDST.
The following illustration shows the connection between a L1 in the Financial Settlement Layer and, potentially, Root of Trust and AyA:

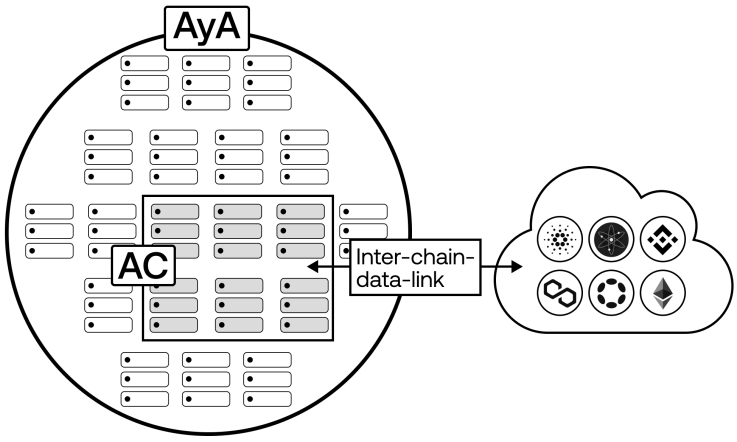

Figure 2: Connection of the Financial - and Telecommunications Settlement Layer

AyA is an L2 solution. AyA performs computation, data settlement, and other competencies that are required to operate a novel global telecommunication network and provides those results to L1 systems. On one hand, an L2 sidechain must follow events on the mainchain and ensure that they happen as reported. On the other hand, it must prove that events on the sidechain are correct and able to be settled on the mainchain. Both of these checks are done by the AC, which is a subset of all registered AV nodes. The AC do this with Cryptographic Proofs that are verifiable on Root of Trust and on other blockchains in the Financial Settlement Layer.

2 AyA Committee

The AC is the cross-chain entity that maintains the connection between the Telecommunications and Financial Settlement Layers. The AC is secured on the Root of Trust blockchain and periodically formed from a randomly-selected sample of the registered validators on the Root of Trust blockchain.

An AC is responsible for verifying that an event on a data ledger system in the Financial Settlement Layer actually occurred, and certifies these chain events on AyA. An AC is critical for the functionality of cross-chain transactions, data and token bridges.

To set up a new AC, the AC members selected to form the new AC must start a DKG as described in the FROST algorithm [CK20]. The FROST key generation uses a modified Ped-DKG algorithm, as described in the following extract:

FROST KeyGen

Round 1

1. Every participant P_i samples t random values $(a_{i0}, \ldots, a_{i(t-1)}) \xleftarrow{\$} \mathbb{Z}_q$, and uses these values as coefficients to define a degree $t-1$ polynomial $f_i(x) = \sum_{j=0}^{t-1} a_{ij} x^j$.

2. Every P_i computes a proof of knowledge to the corresponding secret a_{i0} by calculating $\sigma_i = (R_i, \mu_i)$, such that $k \xleftarrow{\$} \mathbb{Z}_q$, $R_i = g^k$, $c_i = H(i, \Phi, g^{a_{i0}}, R_i)$, $\mu_i = k + a_{i0} \cdot c_i$, with Φ being a context string to prevent replay attacks.

3. Every participant P_i computes a public commitment $\vec{C}_i = \langle \phi_{i0}, \ldots, \phi_{i(t-1)} \rangle$, where $\phi_{ij} = g^{a_{ij}}$, $0 \leq j \leq t-1$

4. Every P_i broadcasts $\vec{C}_i, \sigma_i$ to all other participants.

5. Upon receiving $\vec{C}_\ell, \sigma_\ell$ from participants $1 \leq \ell \leq n, \ell \neq i$, participant P_i verifies $\sigma_\ell = (R_\ell, \mu_\ell)$, aborting on failure, by checking $R_\ell \stackrel{?}{=} g^{\mu_\ell} \cdot \phi_{\ell 0}^{-c_\ell}$, where $c_\ell = H(\ell, \Phi, \phi_{\ell 0}, R_\ell)$.

   Upon success, participants delete $\{\sigma_\ell : 1 \leq \ell \leq n\}$.

Round 2

1. Each P_i securely sends to each other participant P_ℓ a secret share $(\ell, f_i(\ell))$, deleting f_i and each share afterward except for $(i, f_i(i))$, which they keep for themselves.

2. Each P_i verifies their shares by calculating: $g^{f_\ell(i)} \stackrel{?}{=} \prod_{k=0}^{t-1} \phi_{\ell k}^{i^k \bmod q}$, aborting if the check fails.

3. Each P_i calculates their long-lived private signing share by computing $s_i = \sum_{\ell=1}^{n} f_\ell(i)$, stores s_i securely, and deletes each $f_\ell(i)$.

4. Each P_i calculates their public verification share $Y_i = g^{s_i}$, and the group's public key $Y = \prod_{j=1}^{n} \phi_{j0}$. Any participant can compute the public verification share of any other participant by calculating $Y_i = \prod_{j=1}^{n} \prod_{k=0}^{t-1} \phi_{jk}^{i^k \bmod q}$.

Figure 3: FROST Key Generation [CK20]
Provided here without the associated introduction to suggest the level of detail available in the reference

If the process fails at any stage due to the misbehaviour of participating nodes, detection and exclusion is immediate. The misbehaving validator is excluded from the AC formation for a defined number of AyA epochs and can be slashed if the validator has a recent history of repeated transgressions. Punishment, however, requires approval by the current AC.

Eventually, the AC will commit the new AC-PublicKey to Root of Trust for the next AC. The transaction contains the signature of the current committee; the message signed is the new AC-PublicKey and it is incorporated in the sidechain.

To update the AC-PublicKey on the Root of Trust blockchain, the sidechain's AyACommitteeUTxO (in the case of an eUTxO-based chain) or the corresponding state in the AC smart contract (for account-based chains) must be updated. To accomplish this, the AC leader's Certificate-Creator does the following:

1. Observes the event on AyA
2. Validates the signature of the AC
3. Creates a transaction using a smart contract for verification on Root of Trust

When the epoch, or another time constraint, occurs on the Root of Trust blockchain, this event is recognised by the Light-Client-Module. The event creates a transaction on the sidechain that certifies the phase initiated by this epoch or time constraint on AyA. The transaction is validated by the network and, on agreement, is included in a block.

Assuming that the change initiates a progression of the AC turn, the event is picked up by the AC leader of the next AC and creates a StartCommitteeTurn transaction on AyA, which is an AC signature transaction requiring a threshold signature of two thirds of the new AC. The new committee signs the transaction, and it is eventually inserted in a sidechain block. The members of the current AC then use the StartCommitteeTurn event of the new committee to validate their request. If approved, the current AC signs the same transaction and commits an EndCommitteeTurn transaction to the sidechain. Both the new and the current AC have now confirmed the rotation of the AC on AyA.

The AC leader waits for these two transactions to be incorporated, then creates a certificate on Root of Trust to initiate the AC rotation and update the state on Root of Trust. In this transaction, the current AC-PublicKey field is updated. To successfully rotate the AC PublicKey, the membership proof created during the AC formation must be verified and the information cannot be reused in other transactions, for example by spending the UTxO. The AC-PublicKey must match the one determined during the membership proof on Root of Trust.

The change of the committee state is recognised by the Light-Client-Module, which creates a NewCommitteeAcknowledged transaction that is verified by the current AC against the event they received from Root of Trust before eventually being incorporated in an AyA block. This last transaction finalises the process; the new AC is in charge and the members of the old AC can delete their old keys.

2.1 AyA Validator Registration

A valid ENO is in possession of an ENNFT, which allows the registration of an AV. Registrations are handled by using a smart contract on the Root of Trust blockchain. On successful execution of this smart contract, a RegistrationUTxO is created and paid to the smart contract address. A successful registration creates an ENOPNFT, which manages the registration and identifies the operator for this AV on Cardano. The following information is required as input for the smart contract transaction:

1. Arbitrary UTxO to be spent, used as nonce
2. UTxO containing a valid ENNFT, which can be used as the nonce input, and the ENNFT is locked in the RegistrationUTxO
3. AV-PublicKey
4. AV-Address
5. Reference Input AyACommitteeUTxO, which must contain the SidechainIdentityNFT
6. Link to MpOpToken policy for ENOPNFT minting
7. Validator-PublicKey to verify signatures on Cardano

The smart contract verifies that the MpOpToken minting policy successfully mints a unique ENOPNFT, which has to be paid to the ENNFT sending address. The minting of an ENOPNFT has to ensure a unique allocation to its ENNFT. This approach ensures that the relevant UTxOs are spent in this transaction. The ENOPNFT tokenname is stored in the registration UTxO, to allow for changes and de-registration.

The AVRegistrationContract confirms that the provided AV-PublicKey, used to identify the individual AV on Cardano, is stored in the Datum of the RegistrationUTxO and that the registration data is signed by the AV-PublicKey. Additionally, the provided Sidechain Parameter Hash must match with that in the AyACommitteeUTxO's Inline-Datum and it must contain the Identity-NFT of the sidechain for verification. The final condition is that the ENNFT must be locked on the RegistrationUTxO.

During installation of an EarthNode, an AV is set up before registration on Root of Trust because the data needed for the registration is generated during the installation. This means, if the registration is valid, the specific AV is already present on the sidechain and waiting for authorisation to become an active AyA-Validator.

The registration transaction is picked up by a Light-Client-Module belonging to an existing AV and a transaction is issued on the sidechain. This transaction is verified by the AyA network. On approval, a newly-registered AV receives the base stake to become a validator.

This finalises the registration on the sidechain and the new AV is eligible for block proposals as well as AC membership.

2.2 AyA Committee Selection

AC Selection is the process of selecting the members for the next AC-Turn. A turn is the period for which a specific AC is in charge before a new committee must take over. This period is determined as $T = n * epoch_{Cardano}$, where n is a natural number.

An AV can be appointed to an AC if it was successfully registered on the AyA-sidechain. The ACMembershipContract contains a NextACMembersSetUTxO for the sidechain. The datum of that UTxO contains a list of bits, each representing a registered AV. The list assumes a canonical ordering of all existing RegistrationUTxOs during the last deal. This representation of

the members of an AC is very compact and allows several thousand AVs to be stored on a single UTxO.

The sample is created using a smart contract on Root of Trust. When an event to deal out a new AC is received, the smart contract is executed by the current AC, creating a random new bit-list. When the sidechain receives the new list of AVs, it checks for all currently-registered AVs, orders them canonically, and determines the AC from the provided list.

After approval and block inclusion, the current AC picks up the new AC-sample and certifies a transaction to Cardano to create the new NextACMembersSetUTxO. The existing NextACMembersSetUTxO must be spent. The ACMembershipContract must be used to verify the members and ensure on Root of Trust that the AC was built from the intended sample.

Dealing out a new AC sample

In the committee determination phase of a turn, the leader of the current AC recognises the relevant epoch change event on the mainchain, and informs the current AC that it is time to start a deal out of a new AC sample. This results in the following actions:

1. The current AC creates a canonical list of bits representing the registered AV and containing only zeros (meaning that no AV is selected)
2. The current AC verifies the request and incorporates it in a block on AyA
3. The Cardano Relayer picks up the transaction, builds a certificate, and submits it to the ACMembershipValidator's DealOutNewSet endpoint
4. The reference to the sidechain identity UTxO is updated on the AC Turn Rotation (this contains information on the sidechain's state and slot-range specifying when the next distribution is allowed, is needed by the smart contract, and is valid for the starting turn)
5. An arbitrary UTxO is specified in the Redeemer, and spent to prevent replay attacks (this can be the UTxO of the previous NextACMembersSetUTxO, as it has to be spent anyway)

6. The epoch's nonce and the UTxO are used as a random seed to flip the value from zero to one on random AVs in the bit-list until the desired AC size is achieved

7. The AVs with a value of one are selected for the next AC with the number of selected AVs determined using the total size of the bit-list and the total number of existing AVs

8. The datum preserves the selected member list and store time range an AC is valid

9. The last block before epoch switch, known as Nonce-Epoch, defines the state used to calculate the canonical ordering of EN-Registration

The selection mechanism is illustrated below:

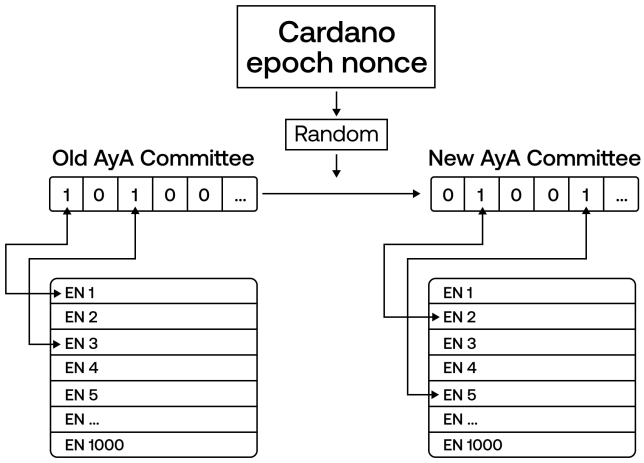

Figure 4: Simplified Committee Selection Process

The Cardano-Light-Client of the current AC leader picks up the transaction and resulting UTxO on Cardano, performs verification and submits a transaction on the sidechain that contains the selected ACMembershipSets bit-list. After this transaction has been verified by the sidechain consensus and included in a block, the new ACMembershipSet can start the process of creating the next AC, as follows:

1. The sidechain rebuilds the canonical list to determine the AC membership

2. The new AC performs a FROST DKG round to create a new shared public key (and signing key)

3. Each AC member posts their public key share to their registration UTxO on Cardano and signs it with their AC-PublicKey

4. After a certain period, the current AC aggregates the new AC-PublicKey on AyA, then initiates the aggregation on Cardano in several transactions

5. The new AC-PublicKey is committed to Root of Trust; simultaneously, a final smart contract transaction sums the aggregated shards created in the previous steps and verifies them against the result determined on AyA

2.3 AyA Committee Turn Rotation

Above, we described how a new AC is formed and committed to the mainchain. The AC Turn Rotation puts a newly-determined AC in charge, and is a committee key rotation mechanism that is injected from Root of Trust. The AC has the special role of verifying and identifying cross-chain transactions to the mainchain (or another chain) and its integrity is essential. Rotating the committee based on mainchain events creates a dependency on the mainchain, which —if not complied with —ends concurrence of the chains. Rotation is also needed to exclude old validators, or to include new ones as these are authorised on the mainchain. The AC module can also exclude malicious AVs from the AC and slash them at the sidechain level to exclude them from block production.

Rotation is initiated by an epoch change on Cardano and picked up by the current AC leader's Cardano-Light-Client. The Light client builds a transaction on the sidechain, which requests that the AC hand over the turn that is verified and is eventually either included in a block or rejected. On inclusion, the new AC crafts a StartNewTurn transaction that contains the relevant parameters of the new AC, such as the AC-PubKey, the slots and times for the next committee selection and rotation, and other epoch parameters.

The new AC signs the hash of the epoch parameters. The transaction is submitted to the sidechain and eventually included in a block or rejected. On inclusion, the current AC crafts a cross-chain transaction that contains the hash of the epoch parameter, the new AC's signature and the epoch parameter itself. The current AC verifies the parameters and, if all checks pass, signs the hash and adds its signature.

The AyACommitteeValidator contract in Cardano verifies the transaction because it must spend the AyACommitteeUTxO and create a new one with the updated epoch parameters in the datum. The smart contract checks the epoch parameters for plausibility and verifies the signatures of the new and current AC. If all checks pass, the AyACommitteeUTxO is spent and a new AyACommitteeUTxO is created with the updated data and sidechain identity NFT. The current leader's Light client picks up the mainchain event and assembles an AcknowledgeNewCommittee transaction on the sidechain.

This rotation mechanism is illustrated below:

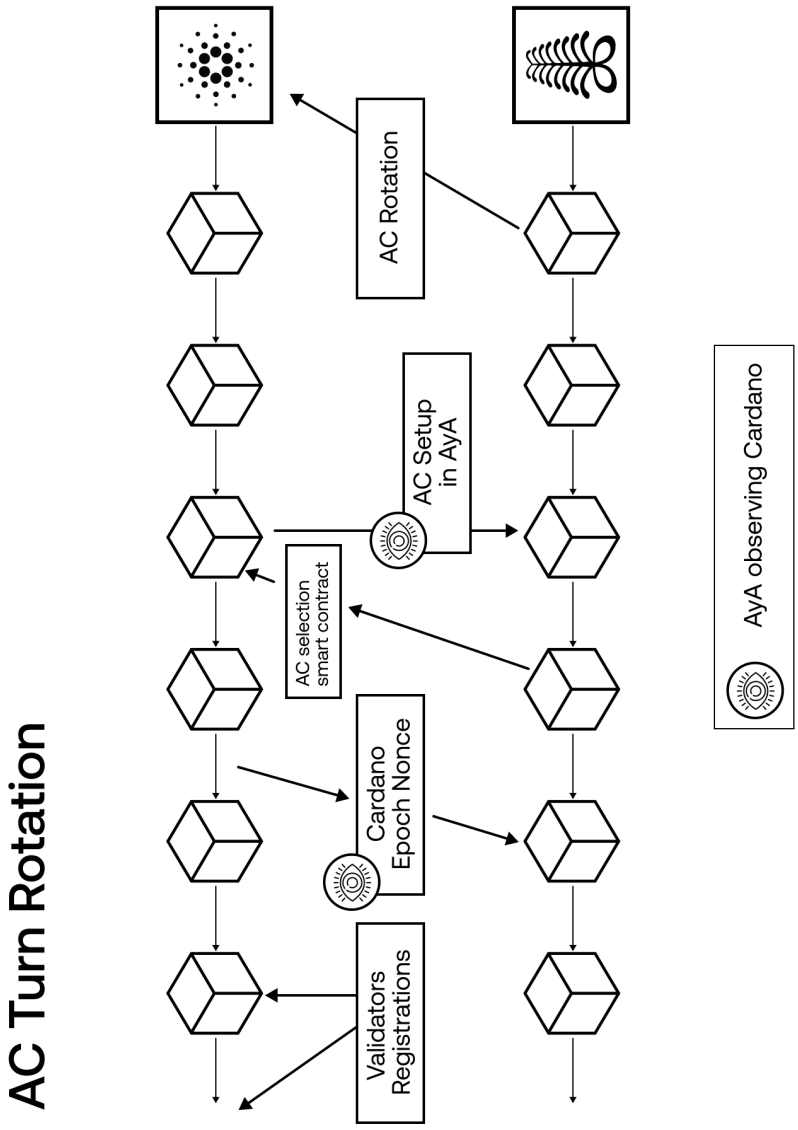

Figure 5: Simplified Rotation Mechanism

3 Concepts and Components

3.1 AyA Initialisation

A sidechain operating as an L2 solution must originate from its Root of Trust. This means that validators approving sidechain transactions must be registered on Root of Trust. If an AV is invalidly registered, it is ignored; any correctly-registered AV that later becomes invalid loses its block production power.

Initial Setup Procedure

The initial setup procedure is as follows:

1. A sidechain identity is created in the form of an NFT
2. The smart contracts on Cardano are parameterised according to the parameters and settings of the sidechain
3. The sidechain is created and kept in a paused state until the set of EarthNodes that have been defined in the genesis parameter of the sidechain have joined the network as block producers and can identify each other (these EarthNodes must have a valid registration before the sidechain enters operation)
4. The EarthNodes run an InitSidechain transaction on Cardano against the AyACommitteeContract to create the first AC. Once executed, the InitSidechain transaction cannot be executed again
5. So-called bootstrapping EarthNodes are those that build the first AC and initialise the sidechain; they are defined in the genesis parameter
6. Other EarthNodes can join the network, but the bootstrapping nodes retain control of the AC until enough AVs have joined the network
7. The condition that must be met to rotate the AC is parameterised. This depends on the allowed period and number of validators in the network. When the condition is met, the bootstrapping AC hands over to the initial AC and AyA enters decentralised operational mode

3.2 Light Client

Messages from the mainchain are received with a distributed, built-in, Light client in the EarthNodes. The Light client is connected to a Cardano-Node and operates primarily as an event listener; it can also look up historical mainchain data through a data provider. The ENO can run a Cardano-Node and, for example, DBsync connected to the data provider as part of the EN. Each EN will be able to choose a suitable source for their individual use case. If an ENO does not want to run its own instances, it could connect to Blockfrost, Koios, a decentralised DBsync, or similar services.

The Cardano-Light-Client can de-serialise transactions from Cardano, and approve signatures and block production. It can also verify smart contract execution. Depending on the selected events and the de-serialised data, the Light client will create a transaction on the sidechain to include the new state in the sidechain and trigger further actions.

After each Cardano-Light-Client action that involves any change, a new leader is elected. The leader is responsible for listening for Cardano events (as are the other members of the AC) and for triggering an action, if needed. All triggered actions will be approved or rejected by the AC.

3.3 Certificate Creator Service

Messages to Cardano will be formed and sent in a built-in service in the AyA-Sidechain Node. The Certificate Creator is connected to a Cardano-Node and operates as a transaction relayer. The ENO can run a Cardano-Node to connect the service. Each EN can select a suitable Cardano-Node connection for their individual use case.

The Certificate Creator Service can serialise transactions for Cardano and check AC signatures. Depending on the events on AyA, the service will create and send transactions to Cardano to update Root of Trust or trigger further actions.

After each Certificate Creator action that involves any change, a new leader is elected. The leader will be responsible for listening for AyA events (as are the other members of the AC) but also for triggering an action, if needed. Any triggered action will be checked first and then and approved, or rejected, by the AC and confirmed by Cardano Smart Contracts to keep

trust and consistency.

3.4 Stake Injection

A validator's stake (base stake and delegated stake) will be updated only at the beginning of a Cardano epoch. When an epoch changes, the Cardano-Light-Client (see subsection 3.2) will identify the event and propagate it to AyA. The AC will react on the verified event and initiate the update on stake allocation.

The process starts when the AC members fetch the information, check whether or not it comes from a trusted source, and vote. If the AC doesn't reach consensus, the update will not be applied.

When the committee reaches a consensus, however, the Certificate Creator (see subsection 3.3) will pick up the update and notify Cardano that the changes will be applied. At the same time, the update to apply the changes is triggered in AyA.

Once the update is finished, the Certificate Creator (see sub-section 3.3) will pick it up and notify Cardano that the changes were successfully applied.

Staking mechanism on Cardano

The stake injection process is a split process where a smart contract locks WMT for a specified AV on Cardano, but the effect occurs on AyA without transferring the tokens from Cardano. Similar to an ENO, which committed to lock 100,000 WMT for operating an EarthNode and securing the network, stakers can contribute to secure the network by committing WMT to their preferred choice of EarthNodes, and earn rewards.

Staking WMT to an EarthNode is straightforward. A WMT holder can create a transaction, using the World Mobile Vault, to stake an arbitrary amount of WMT to an EarthNode. They have the option of deciding how much WMT to stake to a specific EarthNode. They can also stake to several EarthNodes at the same time. The relationship between an AV and a single staker is identified by a UTxO on the staking smart contract. The tokens have to be staked for at least two complete Cardano epochs to be considered a valid stake on AyA and contribute to the consensus.

The user can unlock the WMT that is locked in the UTxO at any time, whereupon the voting power for that validator will be decreased immediately. The total allocation is updated at the start of each Cardano epoch and is based on a snapshot taken when the event occurred.

Stakers are rewarded according to the commission set by the ENO. After the deduction of the commission, the remaining amount is divided between everyone who has staked to that EarthNode, proportional to their stake amount. The smart contract ensures that users can only stake to registered EarthNodes, as the staking transaction must reference the registration UTxO of the relevant AV containing an EarthNodeNFT.

3.5 Mainchain Bindings

An L2 solution must be tightly-coupled to its Root of Trust to ensure the integrity of the sidechain. This can be achieved by different mechanisms and the possible solutions vary with the blockchain type choosen as Root of Trust. Two of the most important links are a periodical update of the verifying committee, which is initiated by Root of Trust, and the registration of validating nodes on Root of Trust. Different use cases entail different bindings, the following list represents the bindings using Cardano as Root of Trust:

1. Stake injection for AVs
2. Epoch binding for AC rotation
   (a) The length of AC epochs will be a multiple of the length of Cardano epochs. So the length of an AC epoch can be defined as $n * epoch_{Cardano}$ where n is a non-zero positive integer
   (b) The AC Member selection is done on the mainchain using the epoch nonce of the previous epoch as a seed of randomness to determine a sample of AVs to join the next AC
3. EarthNodes (also called AVs in the context of the sidechain) register a validator on the mainchain to be eligible to participate as validators on the sidechain
4. The sidechain and its configuration is also registered on Cardano and must be bootstrapped by a valid AC to become an operational sidechain

5. Cross-chain transactions can be approved on Cardano using a Threshold-Signature Schema that is verifiable on Cardano, and created and signed by the ACs on AyA

4 Consensus and Scalability

The AyA sidechain is a blockchain built on the Cosmos SDK framework. Consensus in Cosmos is handled by one of several, essentially separate, modules through the ABCI protocol.The consensus module of the AyA Sidechain is called WMbft.

Its main function is ensuring the correctness and reliability of AyA computations. It is crucial that the WMbft consensus protocol scales linearly with the growth of the World Mobile system. WMbft is nearly optimal in this regard and actually exceeds the scalability of other currently-operational traditional blockchains.

Another unique, and important, feature is that neither the size nor effort required to verify a signature made by WMbft consensus grows as nodes are added to the sidechain. The safety or correctness of the signed blocks, and the reliability of suitable resultant blocks, is ensured probabilistically.

The parameters selected for WMbft, however, are such that the chance of failure of the probabilistic safety or reliability is essentially negligible. Also, the time taken to reach consensus is nearly optimal, given the communication delays between honest nodes, and is linear in network size. The approach to achieving these properties is similar to, but slightly more advanced than, that taken by a major chain already in mainnet [Apt], which builds on some significant earlier work [MY19].

How does WMbft work?

The WMbft consensus protocol uses the typical notion of a blockchain made up of a series of blocks, each chained back to the hash of the preceding block, and a leader node that proposes a new block to be added.

There is exactly one candidate leader node for each successive block. The manner in which the candidate is determined cannot be manipulated, and uses a fresh random value. To produce a previously-committed —yet fresh —random, the last value added to a cryptographic hash chain that was committed at the beginning of the epoch by the respective node is revealed. A fresh random value from the hash chain of the leader is included in its proposed block, as are the hash of the preceding block and the hash of AyA

state.

A less typical notion is the random selection of an endorser subset of nodes for each block; this is the basis for the extraordinary scalability. The endorser set is large enough to ensure that the BFT assumption, which requires that more than two thirds of nodes be honest, has a high-enough probability that the required majority quorum of endorsers is also honest. The fresh random value from the previous certified block is used to determine the leader and the endorser set of the current block.

A certain amount of the work of a node can be left to the endorsers, and —since their number is fixed —the required intercommunication can be far more efficient than it would be if all nodes had to communicate with all nodes. An important example of the work by endorsers is obtaining agreement on adding a block and producing a signature on that block.

When the BFT assumption is met, it means that more than two thirds of the nodes are honest and that they can communicate with each other. If the leader is one of those honest nodes, or simply behaves as one, then WMbft advances to the next block as follows:

(a) The leader signs and sends all nodes a proposal for the next block. This includes a hash of the previous block, a fresh random value from the end of the leader's pre-committed hash chain, and the proposed updated state of AyA

(b) Every honest node sends a self-signed agreement with this to all endorser nodes in the endorser set, which —like the leader —is determined by the fresh random value from the previous block

(c) The endorsers each check that they have an agreeing signature from a majority of all nodes and then sign an endorsement of the proposed new block. This set of signatures, whose size is always bounded by the fixed-size of the endorser set, is what an external entity, such as a Cardano eUTxO script, checks to verify the state of AyA

If, however, the leader candidate does not propose a block that a majority of nodes vote to accept, or the block is not accepted by a quorum of endorsers, then a timeout occurs and that leader, endorser set, and block are essentially skipped. After this, for the next block, another leader and endorser set is

determined from the last fresh random.

At some point, an honest, or at least a correctly-functioning, node is selected as leader and the chain moves forward. The actual rules governing this aspect are somewhat complex, relying on a kind of multi-phase commit that has been proven necessary; in the end, however, so long as the BFT assumption is satisfied, it has also been proven that a single series of blocks without any forks is always ensured.

5 Supplementary Information and Material

Although Cardano is used in this paper as Root of Trust, using its eUTxO and smart contract model, this solution was created to be easily adapted for account-based and EVM-compatible chains. By tackling the complexities of Cardano's eUTxO model first, we aimed to create a general solution for any type of L1 chain. A subsequent paper detailing how this model would be implemented on such chains is already in the pipeline.

Moreover, this paper reflects a work in progress that is not considered finished, but iterative. It focuses on the current state-of-the-art choices for the interconnection of the AyA chain to Root of Trust and the L1 acting as Financial Settlement Layers. A parallel effort to improve this interconnection, with some architectural changes that could potentially reduce the reliance of AyA on Root of Trust, is already in progress.

References

[MR80] R. M. et al. Merkle Ralf. “Protocols For Public Key Cryptosystems. Sunnyvale Ca.” In: (1980).

[GR02] R. G. et al. Gennaro Rosario. “Revisiting the Distributed Key Generation for Discrete-Log Based Cryptosystems”. In: (2002).

[PJ17] J.P. et al. Poon Joseph. “Plasma: Scalable Autonomous Smart Contracts”. In: (2017).

[GP18] P. G. et al. Gaŝi Peter. “Proof-of-Stake Sidechains”. In: (2018).

[MY19] M.Y. et al. Maofan Yin. “HotStuff: BFT Consensus in the Lens of Blockchain”. In: (2019).

[CK20] C. K. et al. Chelsea Komlo. “FROST: Flexible Round-Optimized Schnorr Threshold Signatures”. In: (2020).

[GK21] K. G. et al. Gurkan Kobi. “Aggregatable Distributed Key Generation”. In: (2021).

[Apt] “The Aptos Blockchain: Safe, Scalable, and Upgradeable Web3 Infrastructure”. In: (2022).

[ZD23] D. Z. et al. Zajkowski Dominik. “Technical Specification — Example EVM Sidechain”. In: (2023).