The VIP Environment

The VIP is more than a currency. It is a secure application environment built on existing and specially developed hardware and software networks and protocols.

The concepts in this module should be considered more use cases than technical specification. The actual specification will be detailed in the VIP Treasury business plan and it could look very different from the ideas that follow.

VIP stands for Voice, Iris, Palm, but spaces in the environment are associated with identities using the latest biometric technology. It is also possible to secure a space with an identity associated with a photo-id secured e-wallet, but there are some access restrictions on those spaces.

For those with biometric identities, access to the space can occur anywhere in the world with no wallet, phone, or watch required. Those with e-wallets need a device like a phone or watch, or they must memorize or have available a very long private key.

Spaces can also be associated with multiple identities. Each of the identities in a space can have different access rights.

The primary element of a space is an account. The VIP allows the owner of a space to create as many accounts as they please at no charge. The cost is ultimately covered by the ground rent. A person can create an account in a space not associated with their identity to allow for the transfer of funds.

Accounts hold VIP$. Any movement of VIP$ between accounts is called a transaction and is recorded for 100 years. Generally, the owner of a space can move their own VIP$ from account to account. However, there are exceptions.

Earmarking

An account can be earmarked. An earmarked account can only be used to purchase a defined set of products. Earmarked accounts within a space are typically created by another entity.

Funds can be moved from an earmarked account to a more restrictively earmarked account, but not to a less restrictive account. Other restrictions could apply. Only a purchase transaction for an item covered by the earmark can move the currency into the merchant's earmark-free account.

The creator of an earmarked account can set an expiration date at which time the money returns to a non-earmarked account. See the module Earmarking for a complete discussion.

The Environment

Any number of owner-defined and well-known attributes can be associated with an account, contract, folder, or other high-level data type. Attribute values can be transactions, accounts, contracts, applications, folders, documents, photographs, video, audio, or simple data types. Large data elements could require a fee in addition to the free service.

Owner-defined events can be defined when VIP$ are added or removed from an account, or when an owner-defined attribute changes. Events can occur at predefined intervals, at a specific time each day, or at a specific date and time.

Events can also be associated with the next transaction, any particular type of transaction, or any transaction for a given product or product category. No VIP activity over a certain interval is an event that could, for instance, trigger a wellness check.

There is programmatic access to all transactions where the owner is a party, or where the owner has access rights. VIP$ can be moved to any account in the owner's space, or to another space where the owner has deposit rights from any account where the owner has withdrawal rights. These are transactions.

Any two parties can create a transaction with signatory consent from their biometric identities, either in actuality or programmatically.

Notification rights associated with spaces and apps determine who can receive programmatic VIP alerts. There is programmatic access to LGATS in formats such as JSON or XML.

All apps must be run in a simulated test environment with both developer and AI agreement that the app is doing what it should. This includes passing AI code reviews. The VIP Treasury requires a fee and agreement from all parties to undo

transactions from bad code. The fee is not too high, because the AI needs to learn to spot the problem.

In addition to accounts, spaces can contain contracts. Contracts have one or more signatories. Prior to signing, a signatory is associated with a space, not an identity. There can be more than one identity with signing rights in a space. Signatories have contract-related statuses, indicating whether the signatory has seen the document, intends to sign, does not intend to sign, or has signed.

Sovereign spaces are leaf nodes of a cellular democracy. Polls, ballots, and quadratic voting apps can be distributed and tallied from any dominion node. Ballots and polls can be distributed across a dominion node to all members of a cellular or district council. Events can be triggered by the close of voting, or by specific outcomes.

The VIP allows a person to vote on dominion issues from anywhere in the world. Assuming false and anonymous identities while debating issues is impossible. Ensured identities should improve the level of discourse and the meeting of minds.

It is likely that one day of the week, such as Sunday, will be the voting day, with ballot issues open for debate for a minimum of 7 and maximum of 15 days. The VIP allows multimedia presentations on a ballot measure to be associated with that measure. Straw polls and online interactions can also be associated with a ballot measure.

With permission by the owner, read access rights for well-known attributes of well-known folders can be given to generic members of specific groups. For example, EMTs could access the complete medical history of an unconscious patient.

Sovereign dominions have the unrestricted right of exile, and non-sovereign dominions can exile those who refuse to face justice or serve their sentence. The VIP enforces exile by disallowing any transactions within the dominion, including access to the owner's space while in the dominion.

VIP-enforced budgets, required for consumption tax and certain Earth Dividend projects, are automatically converted to a folder of earmarked accounts.

Sovereignties have chartered access rights to the spaces of nested "sovereignties" and subjects. All such access rights must be in the sovereignty's VOS. Access rights can allow Earth Dividend funds to flow between identical Earth Dividend accounts

of different members of the sovereignty. For instance, the family shopper can have control over the food distributions for all family members.

Simple mutual consent is formulated as a contract. Signing creates a saved transaction. Ride-sharing is an example of such a contract.

Dollar Accounts

Because rent is payable in U.S. dollars or VIP$ at the peg, the dollar or other fiat currency accounts, funded and defunded by electronic funds transfer or wire, must be associated with VIP identities. Dollar accounts are also required for trading VIP$ at the market.

Biometric Identity

Because the VIP$ is a biometric currency, identities must be saved in the secure data store. Details can be found in the module VIP Identity.

VIP Readers

To perform a transaction, a VIP reader is required to read biometrics. If possible, this can be a freely downloaded smartphone app. Merchants have VIP readers at checkout and reader kiosks, and fiat currency ATMs (at current market price) will be available around town in those counties that sign the agreement.

Both the software for all transfers, and the environment for hardware specifications are developed by the VIP Treasury.