

VULACOIN: A BLOCKCHAIN BASED SYSTEM FOR PROVIDING A PAYMENT MECHANISM FOR PAY-AS-YOU-GO INTERNET ACCESS

VulaCoin is a crypto-based mobile wallet that helps pre-paid users digitise their cash with an internet-time pinned stable coin. VulaCoin represents a reliable, traceable payment mechanism that can provide the backbone to facilitate the micro pay-as-you-go offering. The wallet allows users to store, send and spend VulaCoin at no transaction cost to the user. Vulacoin offers a seamless user experience and a consolidated transparent platform for the ISP. Historically ISPs have not been able to successfully facilitate high-volume transactions on networks in the past (i.e., handling access to the network and payment for the usage) that is required on a micro pay-as-you-go basis. With the VulaCoin solution, this is now manageable.

Use of blockchain

Vulacoin verifies and validates all transactions by making use of a blockchain. Due to the distributed immutability of data and consensus nature of a blockchain, it has been determined to be the optimal solution given the transactional nature and use case of VulaCoin – ensuring security, transparency, traceability, efficiency, speed and automation.

Selection of blockchain

The blockchain technology satisfying the requirements of the system was chosen to be Solana. With the proof-of-stake and proof-of-history consensus algorithms, transaction speeds are minimized and more suitable for a short transaction confirmation time.

Some of the advantages of selecting Solana as the technology base include:

1. **Decentralised and open source.**
2. **High assurance code**
3. **Peer reviewed**
4. **Fast transaction speeds and low transaction fees.**
5. **Proof of stake and proof of history consensus.**

Users of the network

A user is defined as an individual with an amount greater than zero VulaCoin attached to their cellphone number. Once a cellphone number gets their initial VulaCoin in their wallet, a new wallet is created dynamically to hide the complexities of blockchain from the user. This allows for ease of adoption of the current technology. The services made available to the user immediately include internet access.

Users can purchase top-ups for the service using existing infrastructure in the local currency in vouchers, card transactions and top-ups through local stores. Users can transfer their digital tokens to other users in the VulaCoin ecosystem at no transaction cost.

Blockchain transactions

At the time of writing, the transaction cost for any Solana transaction is approximately USD 0.00025 per transaction. Currently, the cost of the transaction transfer is absorbed by VulaCoin.

The following transactions are applicable in Vulacoin:

- **Minting tokens, such as when a top-up is initiated, perform a single transaction on the blockchain.**
- **Burning tokens, such as when an ISP withdraws their Vulacoin, perform a single transaction on the blockchain.**
- **Purchasing a bundle involves two transactions. One transaction involves transferring Vulacoin to the ISP. The other transaction transfers VulaCoin to the VulaCoin wallet as a transaction fee.**
- **Pre-funded wallets effectively involve three transactions. The first transaction is a transfer from the pre-funded wallet to the user wallet. After that, a regular purchase action is performed, involving two transactions.**

Use of Smart Contracts Protection of keys and Architecture

The private key is a multi-signature key, broken up into three shards, with each shard having a different signee, stored in various Amazon KMS services, which in turn is stored on HSM modules. Keys are never stored on the hard drive. Upon each request, the blockchain service (the only authorised service able to access all three parts) will put the keys together and authorise the transaction from the backend.

The backend, in turn, needs an API key to communicate with the blockchain service, which is also stored in Amazon KMS. The backend is also the only service allowed to access the blockchain service. The blockchain service is not connected to the internet but in the same VPC as the backend. By disabling all ports on the backend except port 443 externally, and port 80 internally, the entrance points to the server are limited. A simplified breakdown of the architecture is presented below.

