Swipe

Cross-chain Decentralized Liquidity/Trading Network
&
Cryptocurrency to Commerce Payment Protocol

V2.1

July 12, 2021

Swipe.org & Swipe.io

Abstract

Swipe is composed of two main protocols with focuses on bridging cryptocurrency to commerce and to create a multi-chain/cross-chain liquidity trading network. Swipechain is a phased layer 2 protocol that enables real-time, cross-chain asset trades and settlements utilising Swipe Swap, which is an automated market maker, and a layer 2 blockchain network known as Swipechain. Swipechain will facilitate permissionless digital asset trading based on automated market maker liquidity pools on Swipe Swap which is resilient to attacks and based on market prices. Swipechain is operated by a network of nodes who bond their liquidity provider tokens. The Swipechain nodes will participate in threshold based key generations to create vaults that will store these bonds securely. Swipe's commercial business powers the world's largest cryptocurrency exchanges to seamlessly create payment cards that enable real-time asset spending at over 70 million locations worldwide. All of the Swipe components are powered by the native SXP token.

Information available in this white paper is not an offer of securities or investments in any capacity in any region globally.

Introduction
Swipe & Swipechain

Swipe is an innovative and novel blockchain API solution that connects the world's largest payment networks to the world's largest digital asset exchanges to create seamless payment card experiences for its users. This extensive library of API endpoints gives those clients access to over 70 million locations of spending power with over 130+ fiat currencies access on demand. As Swipe's API Layer is proprietary, the core focus of this white paper is to describe Swipechain, the on-chain protocol, while touching on SXP token's utility for both products.

Swipechain is a layer 2 blockchain network forked from THORChain which will utilise liquidity pools and interface from Swipe Swap, a forked-based automated market maker from Uniswap & SushiSwap, instead of order books that enable liquidity for its cross-chain settlements on trades. The architecture of the two networks will work very similar to their forked cores, but with modification made to fit into the Swipe ecosystem. The protocol is powered by liquidity providers whom are incentivized based on fees and mining pools on their native networks to stake their liquidity provider token (LP Token) into the network. Digital asset trading markets inherit deterministic prices that can be utilised to signal purchasing power to the network which is more user friendly then operating an order-book.

Within the network, transactions that are broadcasted are handled by the same Validator Nodes operating the protocol. These assets between trades are transferred immediately without a trusted intermediary and they are signed via our threshold signature scheme. The protocol's security for the pooled assets can be solved by the architecture of the network. There are bonds that these Validator Nodes place into the system which prevent sybil attacks. As in any Byzantine Fault Tolerance network, we assume that the security of the network is that the majority (2/3) of the nodes never collude with another node. The networks architecture relies on Threshold Signature Schemes for its key generation and key signing events. Swipechain's cross-chain layer will connect a number of blockchains together to pool liquidity with native assets without the use atomic swaps.

Validator Nodes

Validator Nodes are state machines that operate the network for an incentivized structure format. They are not able to make any protocol level governance changes or have any say in network transactions. Their core is to remain anonymous so that they are never trying to maliciously coordinate with each other, communicate, or act in a manner that is not consistent with the architectural requirements of the protocol. These Validator Nodes are earning incentives which accumulate until they exit the network. These Nodes are also penalised if they do not perform the duties of forming blocks, witnessing transactions, and participating in key signing.

To participate as a Validator Node, you will need to bond the required asset capital by sending these assets into the networks primary vault. Once this is completed the protocol will validate you into the whitelisted network and you are able to perform transactions into the network. There are normal synchronizations that occur based on parameters that can be set by Governance will look for nodes that have the highest bonds set to secure the network, and lower bonded nodes will exist securely and safely. This rotation is prudent to ensure that the protocol stays secure and active with regular cycles. It is important to note that nodes can leave the network at any moment which is typically processed by the protocol in the same day. When this occurs, the nodes earned incentives and bond will be returned as well. These nodes are able to re-enter the network by re-bonding their capital.

Swipe encourages the community to participate in the networks operations by running their own independent Validator Nodes so that the protocol can reach a high level of decentralisation.

Liquidity

The protocol's liquidity is important to ensuring that there are competitive trading rates. Liquidity is created by bonding each supported digital asset to the network's native asset in the liquidity pools so that the purchasing ability of the asset is calculated by a ratio of the depth from both sides. By doing this, it ensures that every digital asset in the protocol can be linked via the native asset which enables the network to become conscious of the market rates of each asset at any time. Cross-asset trades can be performed by specifying which asset you want to trade whether there is a bonded pair or not.

Liquidity providers (LPs) add liquidity into the protocol's pools by creating transactions into the network vaults with a specific function. The network then validates the amount of the digital assets sent to become bonded and tracks the pools ownership. These LP's can withdraw and claim their bonded assets by initiating a specific withdraw function into the protocol. Their portion of the digital asset is returned immediately including any fees they have earned during their tenure.

The liquidity provided into the network remain in various pool addresses and they can expand across multiple vaults with multiple blockchain networks hosted, such as Ethereum, Bitcoin, Polygon, and Binance Smart Chain. The protocol is agnostic and is constantly able to validate the amount of the balances in each pool where these digital assets are held. As the network's pool of assets grow, it is assumed that the value of the network's asset grows linearly which enables market arbitrage opportunities to bring equilibrium to market prices versus Swipe Swap prices.

Swipe Swap users can exchange on asset for any other digital asset in the network across numerous blockchains by broadcasting a signed transaction into the Network's vaults. The user will then include their requested trade asset and where the asset will be sent too. The protocol will validate this request in the network and calculate the final market pricing rates between the pair based on the liquidity and current market rates. The formula used to achieve this is based on a traditional market making formula with slippage-based variations.

Trades and exchanges that occur in the network are charged a slippage fee and all outgoing transactions require a trading fee. These fees ensure that the final fees that are collected by the system is paid proportionally to the level of liquidity and that the market users consider this at the time of the trade. Trading fees are slip-fees are required to ensure capital incentives for trades and distribution of fees to the right providers and covers the gas of the transaction when performing cross-chain trades.

Vaults

The Swipe Network which powers Swipechain will manage a number of digital asset vault trading pairs from liquidity providers that have bonded it into the system. These are associated with pools, reserves, and all bonds placed into various vaults. By design, these vaults are non-custodial since the outgoing transactions are performed in line with the parameters set through Governance. These transactions can only be authorised by a valid signed transaction from the originator of the assets and no node in the network ever holds a key that can spend funds without a valid signature. These vaults are managed by threshold signature schemes that require a majority of the nodes to participate in. The system design makes it impossible to track which nodes participate in the outputs and outgoing transactions from a third-party viewer.

Network users query a node for the latest primary vault address, as well learn its expiry time by the same method. It is highly recommended that network participants should query multiple nodes to ensure that they are not subject to an eclipse attack. When there are numerous primary vaults, the protocol will return the vault with the latest expiration time.

Node participants change when vaults are re-generated and digital assets are swept into another vault. Every blockchain network there is a primary vault to receive the incoming deposits of digital assets and multiple secondary vaults that are used to transfer outgoing digital assets. Every node in the node is a party to the primary vault and one of the other secondary vaults.

Once an outgoing transaction is processed on the protocol, the network delegates a secondary vault to transfer the asset. These secondary vaults have a much smaller allocation sizes and can process the transactions in an optimal fashion. Every node in the network will witness the finalised output in order for the ledger to the be completed including gas fees that were used. Nodes that do not participate to the delegated vault are penalised to the value of the transaction and then the primary vault will have to finalise the transaction.

The protocol itself monitors all balances of the secondary vaults in the network and then delegates the outgoing transaction to those with sufficient balances. These secondary vaults will have half of all the pooled capital which is kept in the primary vaults. The network will top-up these secondary vaults regularly by sending assets from the primary vault to the secondary. The primary vault is then cycled when the network changes its active node lists, which is once every few days or earlier if one of the participating nodes leave. Secondary vaults are only cycled when there is a node in the network that is an assigned participant to a secondary node leaves. The process to cycle nodes ensures that the network has active signing participants.

Network Connections

The Swipechain network connects to multiple blockchains are maintained by utilizing one-way state pegs in which case the transactional state is synced to the network instead of the token asset being pegged. In these transactional states are associated data fields, asset payloads, transaction ID, and the receiving and sending addresses. The network will also have embedded block-scanning logic which is unique to each blockchain network and connected to those. When one of these Nodes in the network observes a transaction regarding a vault they are monitoring automatically, they will create a witness transaction then broadcast this transaction into the network using their whitelisted account. This transaction will contain the transaction state and is the same for all other connected chains, irrespective of how that chain stores the transactional data. The protocol is designed to collect witness transactions from all participating nodes and then counts them as votes against a specific transaction ID. Once consensus is reached, the logic is to apply this against the transactional state. If Nodes do not perform their duties here or perform them incorrectly for any reason, they will be penalised by the protocol.

The way these Nodes handle network variability is to maintain a local cache of the relevant transactional inputs and outputs for each external chain. Nodes deal with network variability by maintaining a local cache of relevant transactions for each external chain. Nodes are able to identify activity such as double-spending and chain re-organisations and update the network if any part of a transaction changes. In this way the network is able to stay in sync and apply logic to counter any change in state that has been undone. If a connected chain suffers a contentious fork and not all nodes are on the same block height on the same chain, then it is safest for all nodes to simply stop observing that chain. This will invoke a chain-specific shut-down that returns all assets on that chain to users. Further edge cases generated from unreliable chains are generally not handled, so the network should avoid connecting to low-value, low-security chains.

Threshold Signatures

Swipechain utilises Threshold Signature Schemes (TSS) which enables decentralised key signing without a trusted middleman. With TSS, there are two key components to multi-party computations; key-signing and key generation. This allows the nominated node to construct the key parameters for a new vault with a public key associated from which the vaults for each chain is held. TSS supports both ed25519 and secp256k1 blockchains with vault address derivation being dependent on each specific chain.

When there is an outgoing transaction presented to the network, it is to be validated and signed from a specific vault public key with relevant signers. They will prepare a copy of the signed message from their local key-value and begin a signing transaction. The key-signing transaction starts when the required number of nodes are available and enables a signature from an outbound transaction to be created. All signers then attempt to broadcast the transaction once a valid signature is created and it will be sent to the relevant external network to be accepted. Since there are a number of external networks that handle sequence numbers, UTXO's, and nonces in a dynamic method, a chain-specific module is utilised to convert generic outgoing transactions from the networks into chain-compatible transaction messages.

In order for the network to prevent transaction spoofing, a commit-reveal scheme is used with secret shares to ensure that each node participant is unable to change it afterwards. When key-signing occurs, all participant signers will prepare and sign a locally generated message only, therefore they cannot be spoofed. This process is important because if any of the signers do not participate in the key-signing or key-generation, it will result in a failure, which will be penalised in the system and their next cycle will be removed.

Governance & Rewards

The protocol's architecture follows a very governance-minimal approach which is important as it prevents social-signalling coordination. The rewards portion of the Governance module is very public oriented and will require the consensus of public comment and voting weight to determine which speeds to set certain Swipe Staking products. For the cross-chain aspect of Governance, there is no supported channel where node operates can coordinate or communicate with each other, other than from the network level of completing their tasks. This ensures that there is as much pseudo-anonymity as possible to prevent attacks. The way nodes signal changes are through capital allocation in the network and then developers will need to respond to the networks needs through capital allocations.

Protocol Upgrades

Swipechain upgrades will require that validator nodes to require consensus on the latest version. Validator nodes have the ability to upgrade the application schema, logic, or even the entire protocol itself via a Protocol Upgrade System. The protocol's mechanism for upgrades requires that the block height of the old chain is earmarked to result in a chain-halt, then it will follow a block genesis import and chain-start of a new chain layer with an upgraded network. This is implemented so that all protocol upgrades can be completed with minimal coordination with the caveat of a fall-back safety mechanism that enables backwards compatibility. Both the schema and application logic are versioned so that each node declares the version that they are operating on when they enter the network. The protocol also automates version upgrades by selecting the lowest common denominator of the super-majority. If there are any schemas or logic rollovers that the system detects upon a rotation event, the next block is produced against any new logic and the prior data is saved against the new schema.

Swipe Token

Swipe token (SXP) is the protocol's native digital currency and payment currency for Swipe services that is multi-chain compatible and is currently deployed between Ethereum and Binance Smart Chain with fixed supplies as ERC20 and BEP20 tokens. SXP is utilized directly on Swipechain to secure the network and to earn block rewards for producing blocks and providing liquidity to specific farms. The inflation rate for SXP for Swipechain will be set with consensus of the Swipechain Validators upon the main network launch including supply caps through on-chain proposals. All multi-chain SXP will become redeemable for the native Swipechain SXP when the main network is fully launched and will become interoperable between all compatible chains.

SXP Utility

From an on-chain protocol level, SXP is the Governance token for Swipechain and helps secure the protocol by bonding and protecting the liquidity pairs created by users. SXP Holders can vote on protocol improvements, new farm pairs, and other Governance proposals deployed by bonded Validators. SXP is also utilized to access the Swipe API by enabling commercial partners to pay in SXP for services which utilize Swipe or to receive discounts for Swipe related payment services.

Conclusion

Swipe aims to facilitate a permissionless cross-chain liquidity network for Swipe Swap to perform interoperable trades. Swipechain is blockchain-agnostic so it can scale to numerous other blockchains outside of Ethereum and Binance Smart Chain. Swipe's core API enables partners to issue global linked payment cards through an advanced API layer. Overall the components of the Swipe Network power an ecosystem poised to help bridge crypto and commerce. The protocol itself will have incentives and penalties to ensure market participation stays secure and rewarding by validator nodes. The protocol has end-to-end encryption built in; therefore, it ensures that communication between nodes are secure. Bonds that are held within the network are designed to ensure that nodes operate honestly, or the economic incentive will not be worthwhile including reliable pricing mechanisms. Assets can be regarded as always safe as long as the system has more Bonded Assets than Pooled Native Assets. Swipechain will enable a protocol that has secure process for holding assets by utilizing the information it holds in its own state machines, information from other clients connected to the network, and with the incentive/penalty mechanisms.