Spendchain

Cross-Chain Interoperable Payments Blockchain

chain@spend.org

May 9, 2019
Draft v0.1.0

Abstract. Digital payment systems today comprise of complicated settlement processes in our current financial networks that cost merchants up to 5 percent in processing fees while involving numerous parties[1] to facilitate a single transaction. These legacy payment systems are useful to consumers due to merchant adoption of these payment instruments. Merchants are forced to adopt these payment methods to ensure there is no lack of processing while assuming risks to fraud and chargebacks. Card fraud loss amounts exceeded $22.8 billion dollars in 2016[2] which represented a 4.4% increase from previous year and continuously rising. Blockchain based payments have been researched as an excellent method of replacement for legacy systems[3] however, the lack of execution of a system that is fraud free has yet to be designed with mass adoption in mind in traditional commerce. Having a platform that accepts both traditional fiat currencies and cryptocurrencies selections while maintaining on-chain secure, scalable, and decentralized processes has yet to exist to truly build a fraud-free system of processing and removing numerous potential points of failure. Spendchain proposes to be the world's first cross-chain interoperable blockchain payment system working on numerous fiat and cryptocurrency options, all within one user experience, giving users a wide array of options without degrading their user experience in traditional commerce.

Table of Contents

1. Issues

Legacy payment systems worldwide lack the ability to remove central points of failure and prevent fraud losses. This infrastructure is widely accepted by merchants worldwide due to consumer adoption of these payment instruments such as credit cards or bank transfers. Blockchain based, both on-chain and off-chain, transactions exceed billions of dollars daily while failing to reach practically any usage in retail and commerce. Current blockchain payment and legacy payment infrastructures lack the technology to eliminate fraud, lower merchant processing costs, and enable acceptance of numerous cryptocurrencies with the ability to settle them to traditional fiat. Current traditional payment infrastructure and existing blockchain powered payment network do not provide a wide-spread, easy to integrate and fast settlement of cryptocurrency in the real world.

Bitcoin was originally created by Satoshi Nakamato to be the world's first peer-to-peer cash system designed to eliminate modern day payment methods that rely almost "exclusively on financial institutions" to process these electronic payments.[4] Blockchain based payment systems show us a glimpse of how we can begin eliminating these centralized points, but any current system shows the lack of settlement and mainstream consumer adoption. Many companies that design solutions to these problems either focus on the legacy banking system[5] to initiate seamless cross-border transfers or are limited to centralized cryptocurrency merchant systems with no settlement capabilities.[6] No system exists currently that enables cross-chain interoperability of multiple blockchains to ensure our payment systems can accept fraud free instruments while maintain a secure, scalable, and decentralized platform. Users don't have other options that work in the sense of removing centralized points of failure without comprising user experience or options.

One of a merchant's greatest fears are being exposed to fraud chargebacks. The inventory is now gone without payment being rendered causing financial havoc to merchants especially start-ups. Navigating through a fraud chargeback is tiresome and typically results with a loss of a time and money. Merchants and consumers need a method that enables fraud-free payment processing while enabling the acceptance of both fiat and cryptocurrencies seamlessly and instantly.

2. Introduction to Spendchain

Spendchain aims to be the world's first cross-chain interoperable blockchain payment protocol creating a fraud-free, optional biometrics-based system, utilizing mobile phones. Spendchain may be utilized for both consumers and merchants to have access to a payment platform that gives them a wide selection of payment instruments. These options enable merchants to process at a much lower or free rate than their current processing platforms and users will enjoy rewards unparalleled to their existing payment methods.

Merchants will be able to utilize Spendchain in their existing point-of-sale systems to accept both local fiat currencies and cryptocurrencies all without worrying about being susceptible to fraud chargebacks. Settlement of cryptocurrency to fiat will be instantaneous. if the merchant chooses this as a settlement option. The merchant will enjoy this benefit while paying a fraction of what it would cost on their existing legacy payment platform or they may choose to keep cryptocurrency in native form without conversion for free.

Spendchain will consist of simple integration and implementation for both users and merchants. There will be a wide array of SDK and API services available as well as full nodes that may be used to access Spendchain and all of its features. For merchants it will be as simple as downloading a Merchant Node and running it on a supported instance or using the Spend Pay feature built into the Spend Wallet application. They will be able to integrate the Pay feature directly within their existing point-of-sale system through various supported third-party applications and SDK's Spend will build for merchants and open-source for further development within the community.

Consumers may utilize Spendchain to access payment instruments that give them rewards for every purchase they make on the platform. By accessing this feature in Spendchain users may participate in the protocol through Proof-of-Purchase which enables them to earn on their verifiable purchases. Consumers will be able to run their own Client Node (Full Node) or access Client based services on the Spend Wallet and other third-party applications. Consumers may also participate in the networks governance protocol to ensure that the platform remains decentralized and operational worldwide.

3. Architecture

Overview

Designing the architecture of a blockchain that will handle commerce related transactions on a scalable measure goes beyond the standard development protocols available today. The architecture proposed for Spendchain will go through numerous parallel development pieces to combine the consensus, governance, and technology to meet user demands.

Spendchain's decentralized payment protocol utilizing mobile payment devices will be have axiomatic designs to follow a solid foundational infrastructure. Axioms(A_n) will be marked with prerogative numerations. ($A_i > A_{i+1}$):

A_1 Secure	A_2 Speed	A_3 Validation
○ Non-Forgeable; ○ Technical Compliant; ○ Fraud Free; ○ Biometric Authentication*.	○ 40,000 transactions per second (TPS); ○ One(1) second block confirmation finality; ○ Performance of centralized payment providers.	○ Network Rewards System ○ Network Transaction Validation ○ Decentralized Governance
A_4 Scalability	A_5 Security	A_6 Utility
○ On-chain protocol upgrades ○ Interoperable platform for cross-chain communication of other blockchains	○ On-chain encryption of merchant transactions to ensure GDPR and other privacy measures; ○ Byzantine Fault Tolerance with Proof-of-Stake.	○ Open blockchain platform for mass adoption of any merchant and platform to start accepting fraud free payments.

*Off-chain feature

Distributed Ledger Technology enables these platforms, such as Blockchains, to activate key solutions asynchronously to Spendchain such as the ability for open community development, transparent on-chain transactions, prevent double spending, removing points of central failure, and more.

Spendchain will comprise of nodes in different positions where each node is required to serve different functions. This architecture is proposed in line with our Axiomatic Designs where A_1 and A_2 are of prerogative numerations with their permissions and responsibilities below:

Node type	Operators	Requirements	Capabilities
Validator Nodes	The top 41 nodes of the network whom are voted in by token weight.	• Stake SPND deposit; • Dedicated IP; • Meet infrastructure requirements; • Act in accordance to privacy measures and GDPR.	Validator Nodes have the capability to do the following: • Govern Protocol Changes; • Validate Merchant Transactions; • On-board Merchant Nodes; • On-board Financial Nodes; • Perform Settlements; • Verify transactions on the network • Send & Receive transactions; • Validate & read data • Earn network fees & block rewards
Merchant Nodes	Merchants enabling Spendchain payments	• Stake SPND deposit; • Run a Merchant Node; • Register with Validator Nodes;	Merchant Nodes have the capability to do the following: • Process Proof-of-Purchase transactions; • Send & Receive transactions; • Validate & read data; • Access Network Rewards to offer users.
Financial Nodes	Financial Institutions, Payment Processors, and others who will settle SPND and currencies deemed stable.	• Stake SPND deposit. • Run a Financial Node; • Register with Validator Nodes;	Financial Nodes have the capability to do the following: • Settle transactions for Merchant Nodes; • Process conversions of fiat and cryptocurrencies to selected Merchant Node preferences; • Verify transactions on the network; • Send & Receive transactions; • Validate & read data; • Earn settlement fees.
Client Nodes	Everyone.	• Stake SPND resources.	Client Nodes have the capability to do the following: • Verify transactions on the network; • Send & Receive transactions; • Validate & read data

Spendchain's multi-level node operation model enables participation for users around the world in a decentralized fashion. Each node has a specific duty to perform and will be governed by the network to ensure they fulfil their obligations. Stake requirements create an obligation for the node to operate without malicious intent or will be subject to financial losses from loss of deposits.

Consensus

Spendchain Validator Nodes run a Byzantine Fault Tolerance (BFT) protocol as the consensus method of the blockchain which processes the final order of network transaction sequences. The core of the consensus engine will be on Tendermint Core[7]. With this consensus engine Spendchain will be able to perform high frequency throughputs and gives near instant block finality with one second transaction times which enables Spendchain to perform its necessary functions per A_2. on a scale of major payment processing platforms such as Visa[10]. The Terndermint Core is known for powering the Cosmos blockchain[11] who will play a central hub in blockchain interoperability which aligns with A_4.

Validator Nodes are also responsible for the addition of Merchant and Financial Nodes entering the ecosystem. This requires consensus of at least 2/3 of Validator Nodes. All proposals and network requests are on-chain and will be public for Validator Nodes and community feedback.

Governance

The governance model for protocol changes and upgrades are performed on-chain with the votes of Spendchain Validator Nodes are responsible for the governance of the network. During the proposed software upgrades, any Validator Node that fails to upgrade during the allocated time slot or shortly thereafter will be dropped out of the network and from all responsible duties and all staked SPND will be unbonded.

Encrypted Transaction Processing

Spendchain will ensure privacy remains intact while being transparent in merchant processing. Due to local regulations and privacy policies it would be foolish not to build into the protocol GDPR and other privacy measures for longevity. For Spendchain to meet its axioms designs for A_1, A_2, A_3, and A_5, Nodes are designed to run in secure enclaves of trusted execution environments. A trusted execution environment (TEE) is a secure area of a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and privacy. A prime example of TEE in modern blockchain application would be the use of this method and multi-node disbursement in the Enigma Project[8]. Spendchain will use a more direct version of encrypted transaction processing in TEE's as it will be between two counter-parties, the client and the merchant.

A TEE as an isolated execution environment provides security features such as isolated execution, privacy of applications executing with the TEE, along with confidentiality of their assets.[9] In general terms, the TEE offers an execution space that provides a higher level of security than a rich mobile operating system open (mobile OS) and more functionality than a 'secure element' (SE).

The TEE is an isolated environment that runs in parallel with the operating system, providing security for the rich environment. It is intended to be more secure than the User-facing OS and offers a higher level of performance and functionality than a Secure Element (SE), using a hybrid approach that utilizes both hardware and software to protect data. It therefore offers a level of security sufficient for many applications. Only trusted applications running in a TEE have access to the full power of a device's main processor, peripherals and memory, while hardware isolation protects these from user installed apps running in a main operating system. Software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other. Service providers, mobile network operators, operating system developers, application developers, device manufacturers, platform providers and silicon vendors are the main stakeholders contributing to the standardization efforts around the TEE[10] on Spendchain.

An important feature of TEEs is local and remote attestation. This feature enables nodes or external parties to verify that the code they plan to interact with is indeed the certified Spendchain code. In case of remote attestation, each node does this step before establishing secure communication channels with other nodes. In the light of Foreshadow[11] attack, Spendchain will not solely rely on TEEs for achieving A_1 and A_5 and will consider other measures such as leveraging SPND deposit collaterals, double attestation efforts, or additional cryptography on platform processing.

Security

Considering all the benefits of running blockchain based payments for anti-fraud and double spend measures there still remains security issues being an open-source network running on the internet. Being a public network, security (A_1) and robustness are critical requirements. Common network threats are listed below but not limited to:

Double Spend

The consensus algorithm and cryptographic measures are set up, such that double spends are prevented by the network protocol, as long as 2/3 of Validator Nodes are honest

Manipulation Attacks

To ensure that processing data is secure and encrypted, all communication done on the network between nodes is encrypted and that data is not able to be decrypted by an attacker due to it being sealed in the TEE.

An attacker can however breach into a node, use its staked SPND deposit collateral and do transactions against non-SPND currencies that can be easily manipulated on other trading markets and can cause price manipulation attacks on the network. To prevent these type of attacks Spendchain will employ the following measures:

1. Validators and required to perform due diligence on all Validator and Financial Node operators prior to joining the network
2. Create time-lock restraints on SPND deposit collateral releases to attempt to circumvent any of these attacks.

Financial Node Attacks by Theft of Settlement Funds

Financial Nodes are responsible of the settlement of merchant payments and are required to maintain sufficient reserves to perform transactions. These reserve collateral accounts where the staked SPND represent a large financial gain for a hacker to attempt to siphon.

Validator Nodes that have multi-signature access to these reserve collateral accounts may move the collateral when a Financial node fails to perform its obligations or acts malicious. These multi-signatures would require 2/3 of Validator signatures to perform any changes. Therefore, for an attacker to get access to drain these reserves would be required to attack and control 2/3 of Validator Nodes.

External Malicious Data Entry

Since the network works to support cross-chain interoperability, there remains the threat from external blockchains being maliciously attacked with double spend or malicious data exports. To prevent and resolve these measures Validator Nodes are responsible for executing `block` commands which consensus of 2/3 of the Validators to ensure a block from external sources get removed from the network.

The network is also designed to prevent Eclipse Attacks when malicious peers attempt to connect to the network and broadcast external chains. `Block` commands will help resolve these issues and the deployment of peer selections in a random cycle will help with cycling through trusted nodes.

Nodes on the network begin do act maliciously

If nodes on Spendchain begin to act maliciously without being attacked by an external force, such as performing malicious transactions, they will have all or part of their staked SPND deposit collateral forfeited and will be blacklisted from the network. This will help encourage Nodes to act with trust and stability.

Network drop of connected Nodes

All Nodes on Spendchain are free to drop out of the network and stop performing their network duties. There should be a process though that ensures the network won't be impacted. To ensure this, staked SPND deposit collateral has minimum lock-in vest periods before they may be unlocked. Thereafter, if there are any unsettled merchant transactions open while a node attempts to unlock, there will be a deduction made and distributed to the appropriate nodes to complete later.

Unauthorized use of Merchant or Financial Nodes

Maintaining Node security is an independent task that is designated to each individual Merchant or Financial Node. If an attacker gains unauthorized access to a Merchant or Financial Node the most, they can do is block external processes or use its system that interacts with its secure enclave code. Since Node data is sealed in these TEE's, it renders the attack on that part of the instance futile. If a Node starts supplying fake data or begins attempting to process transactions it would require that these commands bypass remote attestations protocols. This would also require that the attacker has stolen the private keys for all involved parties on those Nodes.

If this attack occurs and the hacker attempts to withdraw funds from the system, it would still require a signature from the administrator of the Merchant or Financial Nodes (think of a smart contract and a contract owner interacting with that smart contract) and still require 2/3 of Validator Node approvals.

Therefore, trying this attack and disconnecting communication from external nodes in the network will likely be picked up by Validators as a malicious attack and result in appropriate preventive measures.

Unauthorized use of Validator Nodes

In the unlikely event that one of the twenty-one Validator Nodes becomes breached there are preventive measures that the remaining Validators may take to ensure stability back into the network. The same issues would be present as if a Merchant or Validator Node is stacked. However, what an attacker may also attempt to do is revoke all the appropriate Validator or Merchant nodes its connected to an attempt to add their own malicious nodes into the protocol.

To ensure this process does not occur it would require the attacker to have control of 2/3 of the Validator Node private keys and access to them. This is the due to Spendchain requiring 2/3 of Validator Node approvals to make any changes to the system including adding Merchant or Financial Nodes.

Network spam attack

All Nodes on Spendchain are able to perform transactions. When a transaction occurs on the network it requires a fee to be paid (think of gas on blockchain). Any user performing an attack would be costly and would only give a temporary potential congestion of the network as Spendchain will be designed to handle approximately 40,000 transactions per second. Therefore, not only does it become a costly attack for any attacker to flood the network but also requires staked resources of SPND to perform transactions.

There will be options for nodes to also set up protective measures on their instances such as firewalls and access through DMZ-typed gateways to ensure network security from external spam attacks.

Privacy

Spendchain will take privacy seriously as it will perform financial transactions on that network. Encrypted Transaction Processing is enabled on secure enclaves running on TEEs that will secure the data contained that even Node operators cannot directly access or view these raw transaction data.

In the event these preventive measures fail, Spendchain will employ additional privacy enhancements. For example, Spendchain will utilize tree signatures[11] for a threshold on multi-signatures which will provide a good balance between accountability and privacy. Spendchain will also look for future protocol improvements such as adding procedures of Confidential Transactions[12]

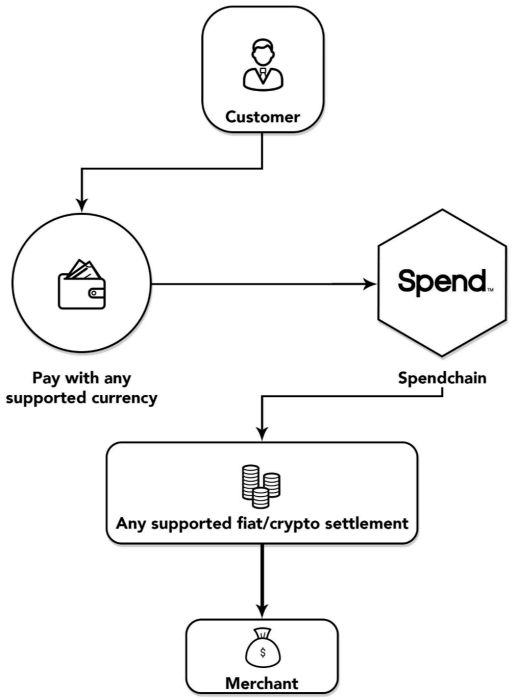
Compliance

Merchant Nodes and Financial Acquirers are required to pass KYC to in order to process financial services transactions for Client & other Nodes. This ensures the longevity of the system by keeping out restricted regions and bad actors from Spendchain. Spendchain plans to utilize decentralized based identity systems like Civic(Identity.com)[13] to pass these checks through the network. These data entries are recorded on the blockchain and accessible to Validator nodes. Validator Nodes are responsible for these checks and balances. Thereafter the cross-chain compatibility of these verified KYC processes will be emended into the processes for Validators to ensure compliance measures are being handled. Validators are also responsible for revoking any Merchant or Financial Node due to future KYC issues that may occur.

The compliance measures of the protocol are designed so that the system maintains and follows local regulations worldwide to prevent the attack of its operations. We realize this may be a negative feature in terms of decentralization and open-finance. However, please keep in mind that we are not welcoming bad actors to the platform. Spendchain is being designed to break the friction of legacy payment systems and give governance to the users/operators of the platform. Validators may decide to change this feature in the future with consensus.

4. Application

Spend Pay



Built into the Spendchain blockchain protocol is a feature called `pay`. This feature enables an on-chain payment function that allows a Client Node to pay for a service/good from a Merchant Node. This feature may be accessed via the Spendchain client, Spend Wallet, or other methods. Since this feature is on-chain a user can run this completely independently and locally if they desire. Pay requests may be made from Merchant Nodes to Client Nodes through various options. The functionality is designed to support incoming and outgoing requests between Client and Merchant Nodes.

Merchant Nodes have an optional method to include Financial Nodes to settle their transaction in real-time utilizing this `settle` flag. Depending on the Merchant Node's settlement flags, the transaction will follow one of two flows that either involve a Financial Node with a settlement fee or able to process directly with the Merchant Node without any additional fees.

Merchant Nodes

Merchant Nodes are able to accept payments from Client Nodes through the `pay` feature in Spendchain. `Pay` enables the Client Node to send a payment to the Merchant Nodes for free on any supported currency of the network. Client Nodes will have access to this feature through a few methods:

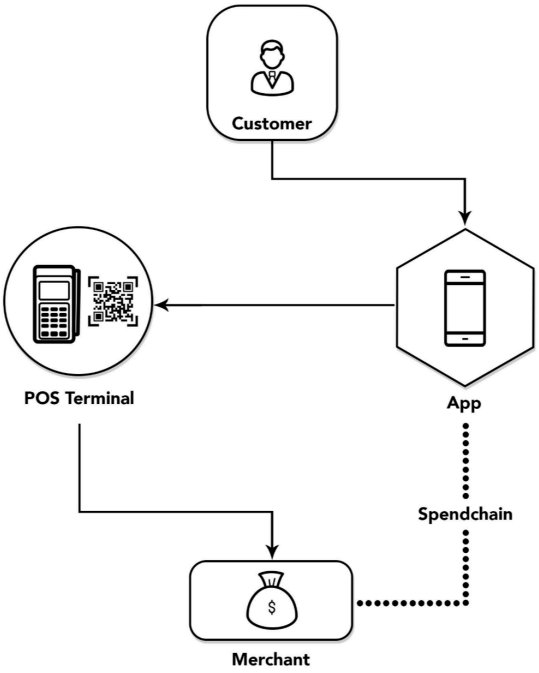
1. Utilizing the Spend Pay feature in the Spend Wallet
2. Performing an on-chain `pay` feature to send the invoiced amount to the Merchant Node's address or SNS(Spend Name Service).
3. On third party devices that support Spendchain services.

Financial Nodes

Financial Nodes handle the settlement of various payment instruments to the selected settlement currency for the Merchant Node. When a transaction is broadcasted using the `pay` feature, if the Merchant Node has a `Settle` flag as `true` then the transaction is broadcasted to the next Financial Node in que for settlement services.

Spend Pay Example – Spend Wallet

Spend Pay's first integration will be in the Spend Wallet app that will enable users worldwide to make payments directly to a supported merchant. Users will have an option directly on the Spend Wallet to select the currency of choice, scan a QR code at the merchant, and payment will be made on-chain directly to the merchant. The first phase of this application will be off-chain as we roll out our main network.

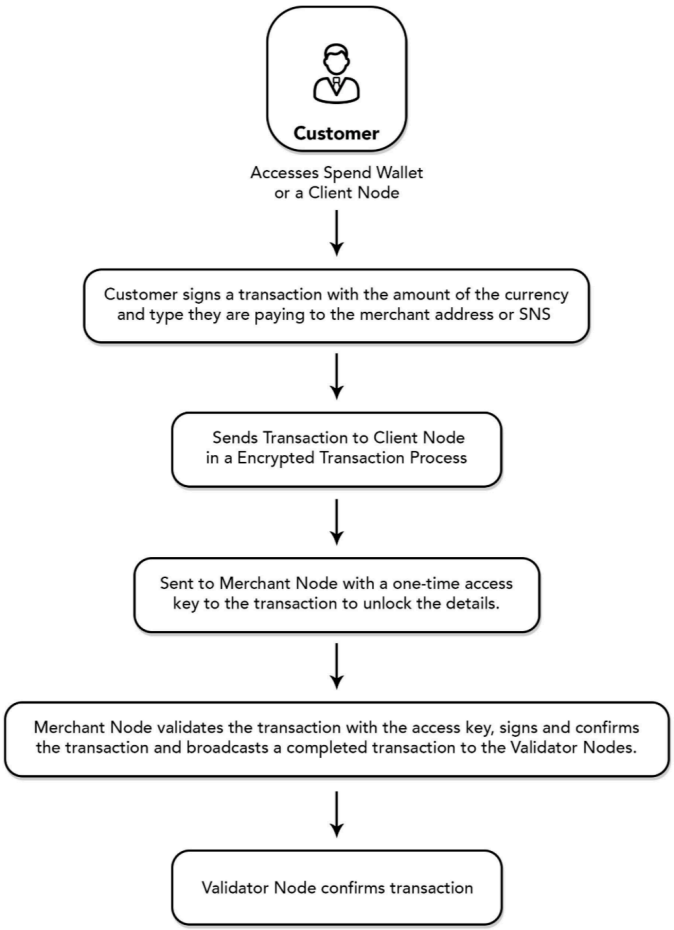


5. Network Settlement

Node Settlement

Merchant Nodes

Merchant Nodes operating on Spendchain have the access to settle blockchain assets without the use of Financial Nodes. These Nodes can settle on both the processing and refund side of the transaction with their customers on the `credit` and `debit` functions of Spendchain.



Financial Nodes

Financial Nodes operating on Spendchain have the ability to settle all blockchain based assets to fiat-based currencies or stable coins by charging a maximum of 100 bps fee (1%) or less. This fee is pre-programmed into the blockchain to ensure there is a transparent fee model available and financially incentive to perform these transactions and carry a settlement reserve liquidity pool for Merchant Nodes. These fees are dynamic and may be adjusted by

Financial Nodes. They can utilize the Spend Authorization Engine[14] or their own method of settlement. Please see the Settlement Process below to see how this process flows

Settlement Process

To become a Financial Node, it means you bear the responsibility to be available with near 100% uptime to process `settlement-request` transactions from Merchant Nodes. Financial Nodes are an essential part of Spendchain to help bridge the gap between all supported currencies on the platform and enable fraud-free settlements for Merchants. These Financial Nodes have a pre-determined reserve of fiat, Bitcoin, and stablecoins to perform these settlement requests from Merchant Notes. Financial Nodes are required to publish real-time conversion rates that they will honor for the Merchant Nodes.

By enabling a settlement process, you are now introducing a counterparty risk between a Financial Node and Merchant Node. To mitigate this risk the following methods below are recommended alongside a safety protocol designed by nature:

- All settlement processes involve a stake of SPND in the equivalent amount escrowed by network to ensure no bad acts occur.
- Merchant Nodes are recommended to follow all on-chain procedures to ensure that flows work with proper governance.
- Financial Nodes are required to use a settlement stake to perform transactions to ensure that they are performing their duties in good faith.

Scenarios	Process Flow
Merchant has USD set as their `settlement-currency` as a fiat selection	The next available Financial Node will receive the broadcasted settlement request on a `pay` transaction. The Financial Node will receive the SPND value of the currency sent by the Client Node and covert it to USD net settlement-fees. Thereafter, the Financial Node will send the USD to the Merchant Note and a Validator will confirm the transaction.
Financial Node refused to transfer the automated `settlement` of the `settlement-currency` to the Merchant Node	If the Financial Node acts in bad faith and maliciously changes their protocol to not `settle` the `settlement-currency` of the transaction to the Merchant Node, that Financial Node is subject to loss of their settlement stake for that transaction and loss of their staked SPND deposit collateral for operating the Financial Node. The Validator Node will then settle the transaction for the Merchant Node. Therefore, it is highly problematic and costly for a Financial Node to be malicious.

Settlement Currencies

Any transaction that is performed on the Spendchain `pay` function are using the native based Spendcoin (SPND). When a Client Node performs a transaction, the client can facilitate any supported fiat or cryptocurrency that has a base asset of SPND. After a transaction is broadcasted to the network the Client Node will deduct the equivalent SPND amount in your selected payment instrument to settle with the Merchant Node.

Merchant Nodes, per the protocol, have a default `payment-receive` method of SPND. Merchant Nodes however have the ability to change their `Settlement` flag to `true` and then select the `payment-receive` to any supported currency that Financial Nodes support. These settlement currencies have been approved by Validator Nodes and made acceptable to the network which will consist of fiat, Bitcoin, or stable coins. Financial Nodes will then perform the conversion for Merchant Nodes and hedge the risk of the transaction. The settlement time for the transaction is expected to be around T for crypto conversion, T_{+2} for fiat conversion.

6. Spendcoin and Rewards

Native Cryptocurrency

The native cryptocurrency fueling all services on Spendchain is Spendcoin (SPND). Initially, Spendcoin will be deployed on the Ethereum Blockchain as an ERC20 token with a 2 billion supply. For any blockchain network to be stable, it needs to create an incentive program to ensure the operators of the blockchain run the governance and functions properly. Spendchain offer its users three (3) forms of rewards. **Settlement** and **Client** Rewards are specific per transaction and are dynamic by design. **Validator** rewards are 2 SPND per block which results in an inflation of 63,720,000 SPND per year and represents approximately a 3.2% inflation rate with a decreasing rate year-over-year.

Spendcoin is a unit representing fees/compensation for Merchant and Financial Nodes performing transaction. Current Distribution of Spendcoin allocation is as following:

Allocation	Percentage & Amount	Purpose
Network Distribution	62.5%, 1,250,000,000	The Network Distribution allocation was designed to promote the incentives of Proof-of-Purchase to Platform Users, Client Nodes, and customers performing transactions with Merchant Nodes.
Spend Company	12.5%, 250,000,000	Spend will be building open source blockchain tech stacks and financial services tools to support the Spendchain ecosystem of on-chain and off-chain products such as the Spend Visa Card and Spend Wallet App. This inflation is released 1% monthly.
Founders & Advisors	12.5%, 250,000,000	The Founders & Advisors allocation is designed to compensate the founders and advisors of the project for work performed on the protocols. These funds are released over 5 years.
Partner Program	12.5%, 250,000,000	The Partner Program is designed to give partners joining Spendchain or the Spend ecosystem of products in some fashion an incentive to build or support the platform.

Protocol Rewards

Spendchain will support on-chain based rewards for three categories: Settlement, Client, and Validator. All these parties included represent how the network will operate and be properly rewarded for their services on the platform

Settlement Rewards

Financial Nodes operating on Spendchain have the ability to settle all various fiat and cryptocurrencies to the `settlement-currency` that the Merchant Node that they are settling for has selected. To perform this function, the Financial Node is performing the conversion and hedging the risk for the Merchant Risk. Where there is risk, there is reward. The Financial Nodes can set their `conversion-fee` on-chain dynamically with a maximum set fee of 100 bps (1%) of the transaction amount.

Client Rewards

Consumers making purchases from Merchants running Spend Pay will be able to enjoy up to 20% rewards back funded by the network's distribution protocol

through its Proof-of-Purchase protocol. These rewards are based on Merchant & Validator node approvals and is unique per Merchant Node based on its marketing plan and strategy for the network.

Validator Rewards

Validators are responsible for running the network. Since transactions are practically free on Spendchain, Validator receives block rewards for forging blocks on the ledger. (this of this as a miner's reward) They receive this as an incentive to operate the network in compliance with its governance requirements.

7. Block Infrastructure

Spendchain will be going through many infrastructure changes and proposals throughout the development of its protocol. The Development team will be working closely with various teams to ensure that Spendchain has a solid foundation of parallel pieces needed to launch it successfully. The information below will give a basic understanding of how metadata is transmitted on the protocol to various Nodes.

Data Structure – Blocks

The initial consensus engine will be built on the Tendermint Core similar to Cosmos Blockchain. This will allow us to utilize a data structure[15] for our blocks to perform with high capacity and throughput.

Date Structure – Transactions

Transactions executed on Spendchain will follow the standard UTXO model that is found in most blockchains such as Bitcoin. There will be improvements made to Spendchain to improve transactions by creating more restrictive output locking. Transactions that are included in blocks will include these components:

A. Encrypted Transaction Data designed to be verifiably by Validator, Merchant, and Financial Nodes whom are responsible for that specific transaction with a secret shared access key.
B. The transaction hash of the raw transaction data.

Various implementation models might be deployed that will require a different subset of data. The raw transaction data will never be transmitted publicly without encryption directly. There might be additional steps taken when performing transactions with encrypted data to ensure privacy such as additional obfuscation of the following but not limited to:

1. Transaction data:
    a. Transaction inputs
    b. Transaction outputs
2. Secret Access Keys that give the right parties in control of these keys access to view data on the following:
    a. the customer's wallet,
    b. the merchant's wallet,
    c. Related Merchant/Financial Nodes.

Merchant Policies

Spendchain requires that during the on-boarding process of Merchant Nodes, that they submit what's called a `refund-policy ` on-chain so that their terms and conditions for these policies are made public for all participants in the network. Having public policies that are recorded on the blockchain helps limit the number of disputes about policies and procedures on the platform.

Refund Policy

Merchant Nodes upon being on-boarded onto Spendchain are required to set their `refund-policy` so that Client Nodes and all participants can transparently see when this policy was put in place and if any changes were made. This allows more retail transactions to take place where the consumer is completely aware of the transactions.

In the event that there is a dispute on a `pay` transaction for a `purchase` then the parties may utilize the dispute manager all on-chain with a Validator by broadcasting a `dispute` transaction. The resolution period is 21 days upon broadcasting the message and you are able to submit case files directly to a Validator.

The Validator Node than reviews material provided during the `dispute` transaction request. If the Validator node believes the claim is valid and, on its face, able to be resolved through a `refund` it will cycle the claim to be voted on by the other Validators. In order for the dispute to be resolved favorably it requires 2/3 votes on Validator Nodes. Spend Foundation is still working on this process and it might change in the future.

8. Network Summary

Performance & Scalability

To ensure that Spendchain handles its goals appropriately it needs utilizes the Tendermint consensus engine to create 1 block finality with a high throughput to handle commercial transactions per second similar to those of Visa. The protocol requires its axiomatic design to operate on servers with low latency and asynchronously work together to support over 40,000 TPS to support all scalable features in the future.

Current estimates support the proposed system. However, its noteworthy to state that the Development team is aiming for better throughput and more scalable systems for other future potential protocol proposal upgrades. This may include sharing methods, side-chains, and other network enhancements that may be voted in by Validator Nodes. Spendchain will operate the protocol with standard network stacks to ensure a smooth initial launch. Spendchain will initially use the standard network protocol stack, such as TCP+TLS, for different node-to-node communications and vote to change this protocol in the future.

Redundancies

It is important to create a scalable global system that ensures low latency and high performance. To maximize this effect, we will be working on spreading Validator Nodes originally across the world in various regions to match all peer connections to be efficient.

Protocol Upgrades

Throughout the lifecycle of a software-based project, it goes through numerous updates, patches, and changes. It is important to note that Spendchain will be an open-source blockchain where anyone around the world can follow git-based development and contribute to the codebase. Originally the Foundation will be working on the development of the project till launch. Thereafter, we hope to begin engaging the community to help make changes and upgrades to the software.

Validator Nodes are responsible for platform upgrade approvals upon the launch of the protocol. Validators may also propose protocol upgrades to build new features into Spendchain. Once a proposal is submitted, Validator Nodes may vote to approve the changes and implement a soft or hard-fork to enable the new updates.

9. Software Development Kits (SDK)

Spendchain will consist of various SDK's to operate it in numerous languages that developers are comfortable with. We will be including widgets and simple button-based SDK's to integrate into any payment system for platforms looking to utilize Spend Pay. The Spend Wallet application will natively support these protocols as well. As the Foundation decides which ones to add, we will update this Whitepaper respectfully.

10. Conclusion

Spendchain has designed a bank level payment system free from fraud for merchants while creating an incentive for consumer-based clients to be rewarded. Throughout this protocol, Spendchain ensures compliance with privacy measures and local regulations to ensure its users a longevity. Spend.com will design the first payment protocol running fully on Spendchain via the Spend Wallet application.

Enabling an open-financial system is important to help fix the issues we have with centralized point of failure legacy systems. Users around the world are able to participate in the networks governance and help contribute to Spendchain. As this is the first initial version of the Spendchain technical paper, we hope to begin receiving community input and additional research to make improvements where applicable before we launch the main network.

References

1. "How Credit Card Transaction Processing Works: Steps, Fees & Participants" https://wallethub.com/edu/cc/credit-card-transaction/25511/
2. "The Latest Credit Card Fraud Statistics and Insights" https://losspreventionmedia.com/credit-card-fraud-statistics-and-insights/
3. "How A Blockchain Payment Processor Can Improve Industry Transactions" https://www.forbes.com/sites/samantharadocchia/2018/09/28/how-a-blockchain-payment-processor-can-improve-industry-transactions/#5892ead8550a
4. "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf
5. "Ripple Is Aiming to Overtake Swift Banking Network" https://www.bloomberg.com/news/articles/2018-11-13/ripple-is-destined-to-overtake-swift-banking-network-ceo-says
6. "Coinbase Launches Commerce Button to Accept Crypto Payments." https://www.coinspeaker.com/coinbase-launches-commerce-button-paypal-like-plugin-accept-crypto-payments/
7. "Tendermint – Blockchain Consensus" https://tendermint.com
8. "Enigma Privacy Protocol Solves Key Blockchain Issues" https://blokt.com/interview/enigmas-privacy-protocol-solves-key-blockchain-issues-preventing-global-adoption
9. "Trusted Execution Environments" https://en.wikipedia.org/wiki/Trusted_execution_environment
10. "Blockchains and Trusted Execution Environments" https://www.csail.mit.edu/event/blockchains-and-trusted-execution-environments-towards-new-security-paradigm
11. "Tree Signatures using Hash Trees" https://medium.com/@g.andrew.stone/tree-signature-variations-using-commutative-hash-trees-4a8a47d4f8ce
12. "Confedential Transactions" https://elementsproject.org/features/confidential-transactions
13. "Decentralized Identity using Civic" https://www.civic.com/blog/5-key-benefits-of-decentralized-identity/
14. "Spend Authorization Engine" https://spend.com
15. "Date Structure" https://www.techopedia.com/definition/1149/data-structure