

# Spendchain

## Cross-Chain Interoperable Payments Blockchain

[chain@spend.org](mailto:chain@spend.org)

Nov 9, 2019

Main Network

Draft v0.9.4

**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<sup>1</sup> 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<sup>2</sup> 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<sup>3</sup> 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

<b>1. Background</b>	3
<b>2. Issues</b>	4
<b>3. Introduction to Spendchain</b>	12
<b>4. Architecture</b>	13
Overview	14
Consensus	16
Governance	17
Encrypted Transaction Processing	18
Security	18
Privacy	22
Compliance	23
Proof-of-Purchase	23
<b>5. Application</b>	24
Spend Pay	24
<b>6. Network Settlement</b>	25
Node Settlements	25
Settlement Process	26
Settlement Currency	26
<b>7. Spendcoin (SPND) and Rewards</b>	27
Settlement Rewards	28
Client Rewards	28
Validator Rewards	28
<b>8. Data Infrastructure</b>	29
Transaction Data Structure	29
Block Data Structure	30
Merchant Policies	31
<b>9. Network Summary</b>	32
Performance & Scalability	32
Redundancies	33
Protocol Upgrades	34
<b>10. Software Development Kits</b>	34
<b>11. Conclusion</b>	35

# 1. Background

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 widespread, easy to integrate and fast settlement of cryptocurrency in the real world.

Bitcoin was originally created by Satoshi Nakamoto 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.<sup>4</sup> 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<sup>5</sup> to initiate seamless cross-border transfers or are limited to centralized cryptocurrency merchant systems with no settlement capabilities.<sup>6</sup> 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. Issues

Digital payments today are remitted in many forms around the world with a collective \$3 trillion USD per day<sup>7</sup>. The majority of these digital payments are facilitated by using a method or combination of methods below

<i>Direct Bank Transfers</i>	<i>Payment Cards</i>	<i>Mobile Wallets</i>
<ul style="list-style-type: none"> <li>○ Swift;</li> <li>○ Wire</li> <li>○ ACH;</li> <li>○ SEPA;</li> <li>○ EFT;</li> <li>○ CHIPS;</li> <li>○ Local Transfers.</li> </ul>	<ul style="list-style-type: none"> <li>○ Visa;</li> <li>○ MasterCard;</li> <li>○ American Express;</li> <li>○ Discover</li> <li>○ Union Pay;</li> <li>○ JCB;</li> <li>○ Diners Club.</li> </ul>	<ul style="list-style-type: none"> <li>○ Apple Pay;</li> <li>○ Google Pay;</li> <li>○ Kakao Pay;</li> <li>○ WeChat Pay;</li> <li>○ AliPay;</li> <li>○ Paypal;</li> <li>○ Venmo.</li> </ul>

Through these various payment methods, a vast majority of all commerce and transactions operate through these payment network rails.

### Direct Bank Transfers

Swift	Fedwire	CHIPS	ACH
5 Trillion USD <sup>8</sup>	2.1 Trillion USD <sup>9</sup>	1.4 Trillion USD <sup>10</sup>	120 Billion USD <sup>11</sup>
30.7 Million Transactions	528,000 Transactions	420,000 Transactions	70.1 million Transactions

Typically, a non-cash payment instrument is usually layered by a traditional account held at an insured financial institution such as a bank or credit union. When there's an exchange of money via these methods, whether it's online or offline, it is transmitted between financial institutions. This method requires it to be reconciled by a variety of domestic and international standards that are required to facilitate these bank transfers between businesses and consumers. These electronic transfers come in the form of SWIFT, Wire, ACH/IAT, CHIPS, rTGS, BePS, KFTC, and NeFT. These electronic transfers rely on an outdated infrastructure that to this day remains vulnerable to fraud and inefficiencies consumers need a method that enables fraud-free payment processing while enabling the acceptance of both fiat and cryptocurrencies seamlessly and instantly.

## Out-Dated Infrastructure

The technology used by the global financial network is consisted of a variety of incompatible legacy systems and standards; many of which in the current electronic payment/settlement system have remained relatively unchanged for over 40 years. A prime example is the Automated Clearing House (ACH) system operated in the United States. ACH is still performed via fixed-width text files that are precisely 94 characters per line. These transmissions are uploaded to various FTP servers and downloaded at specific times of the day to settle the transactions. Until 2016, these transactions cleared the next business day until the NACHA announced an update allowing for ACH's to be able to be performed within the same business day. This so-called upgrade involved no changes to the protocol's specifications.

What prompted this change was the requirement to process transactions twice a day instead of only once. The Society for Worldwide Interbank Financial Telecommunication, formally known as SWIFT, the federal reserve's Wire network, and New York Clearing house association's CHIP Network are all more examples of outdated payment infrastructures. each of these payment protocols requires substantially greater checks and balances from ACH and benefit from greater speed, which increases the complexity of the global payment system. All these payment protocols transact *3.6 Quadrillion USD* in global volume.

## Fraud Issues

Numbers don't lie. In 2016 alone, thieves were able to steal \$81 million USD by impersonating Central Bank SWIFT operators in their day to day role. During that weekend, they routed four transactions through the New York Fedwire, mainly through an automated system, moving \$101 million USD from Bangladesh to the Philippines. The New York Fedwire official caught the thieves because of a misspelling of the name belonging to the beneficiary he was finally alerted and was able to contact Bangladesh Bank officials to prevent the transit of another \$920 million USD.<sup>12</sup>

In 2018, a larger heist was unraveled when a perpetrator was able to use a password provided by bank officials to directly access the SWIFT 15 network to launder funds in equivalent to 1.77 billion USD . This scam went undetected for nearly seven years despite many warnings against fraudulent SWIFT messaging from the deputy governor of the Bank of India.<sup>13</sup> These protocols have multiple layers of supervision involved to combat fraud.

## Transaction Barriers

Funds that are transferred over Wire, SWIFT, ACH, and CHIPS incur costs of approximately 18 billion USD a day.<sup>14</sup> These transfers on average typically take three to five days for settlement and usually four percent of these payments fail because of technical issues.<sup>15</sup> The blockchain could potentially offer several enhancements in these systems, namely cryptographically secure transactions, immutability, and data redundancy. For instance, ripple, a prominent US startup, allows financial institutions to quickly settle cross-border payments using its xRapid network, claiming a 60% reduction in net cost.<sup>16</sup> Remittance providers such as Western Union and MoneyGram have also piloted using native ripple blockchain tokens (XRP) for settlement. Using products such as these, we believe that blockchains have the potential to influence well beyond the primary layer of the global financial network.

## Bank Cards

Major card schemes are highly relied upon instruments due to massive global merchant adoption as shown below:

<i>Visa</i>	<i>MasterCard</i>	<i>UnionPay</i>
<ul style="list-style-type: none"><li>○ 20 billion USD<sup>17</sup></li><li>○ 305 million transactions</li></ul>	<ul style="list-style-type: none"><li>○ 12 billion USD<sup>18</sup></li><li>○ 184 million transactions</li></ul>	<ul style="list-style-type: none"><li>○ 41 billion USD<sup>19</sup></li><li>○ 105 million transactions</li></ul>
<i>Discover</i>	<i>American Express</i>	<i>JCB</i>
<ul style="list-style-type: none"><li>○ 466 million USD<sup>20</sup></li><li>○ 6.4 million transactions</li></ul>	<ul style="list-style-type: none"><li>○ 3.2 billion USD<sup>21</sup></li><li>○ 19.8 million transactions</li></ul>	<ul style="list-style-type: none"><li>○ 731 million USD<sup>22</sup></li><li>○ 8.1 million transactions</li></ul>

*Figures shown above reflect Daily Transactional Data*

The use of payment cards such as credit or debit cards involve multiple steps that tend to run concurrent with the tendency of high fees and frameworks designed to guarantee funds for parties conducting the transaction. Depending on which card you use will determine a variable interchange rate if you're conducting a transaction that has a different currency than what you currently hold. These fees can become expensive and exhausting in the current payment scheme. Payment cards also mandate a secondary network provided by entities called “card associations.” Card associations work with payment processors to conduct the three broad stages of a payment card transaction: authorization (verifying funds in accounts on either side of a transaction), clearing (transferring funds between banks after the exchange of goods or services) and settlement (paying a merchant).

In order to accept payment cards, merchants incur disproportionately high processing fees which are often one of their largest operational costs. However, realizing that payment cards are one of the most convenient used solutions, and will not disseminate, we have tailored our business model around a payment card and our own payment network to offer a full spectrum of services tailored to meet all needs

## Mobile Wallets

Major mobile wallets are highly relied upon instruments due to massive global merchant adoption as shown below:

WeChat Pay	Alipay	Paypal (incl Venmo)	Paytm
4.7 billion USD <sup>23</sup>	3.3 billion USD <sup>24</sup>	425 million USD <sup>25</sup>	55 million USD <sup>26</sup>
175 million transactions	130 million transactions	8.3 million transactions	11 million transactions

As we are entering a world of digitization and mobile adoption, third-party mobile wallet companies are becoming more of a mainstream component to payments. Their abilities to aggregate various features of a bank accounts and payment cards make them even more popular to consumers due to the ease and conveniences offered. There are companies that create digitization of payment cards such as Apple Pay, Google Pay, Samsung Pay, and more which simply allow the mobile devices to virtualize the payment cards into a NFC format. Another business model are those similar to AliPay, WeChat Pay, PayPal, Venmo, and Square cash who have created a suite of services that bring great value to mobile payment and like-banking infrastructures. These companies and mobile wallets have seen a great deal of growth over the last few years, especially markets in Asia, however within these companies there are present limitations and issues that need to be solved to bring a scalability comfort worldwide for mobile wallets.



## Incentive Issues

To date, even the most successful and largest mobile wallet applications run a wide array of their services through underlying regulated or insured payment methods, such as a bank account or payment card. By adding these layers into their protocols, it does bring a great ease of accessibility and convenience but, relinquishes any incentives for the user to continue using the product other than the two mentioned above.

## International Growth

The mobile wallet applications that have seen substantial growth in the payment and banking industries have yet to create a stability of international growth. Each company has their specific region of preference, such as WeChat, which is a great tool used in China, but not on the Western side of the hemisphere. The reason these hindrances occur is because they use domestic financial institutions that have inclusions on the rest of the world. Growing their reach is challenged due to adapting these systems into foreign institutions, regulations, and currencies. Social payment apps such as Venmo and Square Cash are great tools for friends and loved ones to send funds back and forth, but it then ties to a certain geographic due to the boundaries they have within their current financial network schemes. These features are great to build communities, but they hinder in worldwide adoption due to their regional constraints.

## Payment Processing

Payment Processing Costs of the World's Largest  
Retailers by Revenue in 2016

<i>Amounts</i>	<i>Merchant</i>	<i>Country</i>
\$4,989M	Walmart	United States
\$1,516M	The Kroger Company	United States
\$1,179M	Costco Wholesale	United States
\$1,170M	Home Depot	United States
\$1,120M	CVS Health	United States
\$1,059M	Amazon.com	United States
\$956M	Target	United States
\$833M	Lowes	United States
\$807M	Albertson Companies	United States
\$740M	Apple	United States
\$525M	Seven & I Holdings	Japan
\$416M	Wesfarmers Limited	United Kingdom
\$399M	Woolsworth Group	United Kingdom
\$283M	Schwarz Gruppe	Germany
\$262M	Carrefour	France
\$252M	ALDI Einkauf	Germany
\$249M	Tesco	United Kingdom
\$238M	Metro Group	Germany
\$223M	AEON Group	Japan

While the majority of payment processing costs for any given retailer can be attributed to payment card interchange fees, they also include costs such as bank charges, cash and check handling fees, or administrative fees for store credit programs.

## Insufficient Rewards Systems

Current debit card payment rails issued by banks lack cash back programs that are lucrative. The average cash back percentage for a debit card is 0.1%. Most debit cards do not have a rewards or points program. There used to be plenty of banks offering rewards on debit card purchases, until legislation limited the fees that banks could charge merchants on debit card transactions. Since the bankers are now making less on interchange, they have practically removed all debit card reward programs. Credit cards typically have desirable cash back percentages, but they typically are either doing this on a promotional basis or doing it until they can charge you a high interest rate ranging from 8-24% on your purchases.

The average interest rate is actually 19% according to studies done on this topic.<sup>27</sup> Now users are searching for a balance of a debit card and credit card that has a comprehensive rewards program that doesn't have a skyrocket APR that essentially negates the benefits. These issues with the current rewards system leave consumers and merchants looking for alternative methods of processing and usage to be able to compete in a market where rewards are given as marketing incentives.

## Overall Problems

Current debit card payment rails issued by banks lack cash back programs that are lucrative. The average cash back percentage for a debit card is 0.1%. Most debit cards do not have a rewards or points program. There used to be plenty of banks offering rewards on debit card purchases, until legislation limited the fees that banks could charge merchants on debit card transactions. Since the bankers are now making less on interchange, they have practically removed all debit card reward programs. Credit cards typically have desirable cash back percentages, but they typically are either doing this on a promotional basis or doing it until they can charge you a high interest rate ranging from 8-24% on your purchases. The average interest rate is actually 19% according to studies done on this topic.<sup>30</sup> Now users are searching for a balance of a debit card and credit card that has a comprehensive rewards program that doesn't have a skyrocket APR that essentially negates the benefits.

Is the proliferation of blockchain technology evidence of an alternate payment system that will exist parallel to regular payment channels? Or, can blockchain play a useful role in enabling millions of under-banked

and unbanked people to transfer payments leveraging the blockchain platform. Utilizing this technology will enable lower transaction fees and worldwide inclusion. We believe that customers can use these products at a significantly lower cost and low entry barriers when running transactions through the Spend platform.

Some solutions that Spend aims to combat include:

- Value lost in monetary transitions
- Cross-border payment inefficiencies
- Lack of common standards
- Regulatory costs
- Fraud Issues
- Infrastructure variances/outdated platforms
- High Bank fees
- Location based and credit surge in fees
- Lack of incentives and rewards

## 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
<ul style="list-style-type: none"> <li>○ Non-Forgeable;</li> <li>○ Technical Compliant;</li> <li>○ Fraud Free;</li> <li>○ Biometric Authentication*.</li> </ul>	<ul style="list-style-type: none"> <li>○ 40,000 transactions per second (TPS);</li> <li>○ One(1) second block confirmation finality;</li> <li>○ Performance of centralized payment providers.</li> </ul>	<ul style="list-style-type: none"> <li>○ Network Rewards System</li> <li>○ Network Transaction Validation</li> <li>○ Decentralized Governance</li> </ul>
$A_4$ Scalability	$A_5$ Security	$A_6$ Utility
<ul style="list-style-type: none"> <li>○ On-chain protocol upgrades</li> <li>○ Interoperable platform for cross-chain communication of other blockchains</li> </ul>	<ul style="list-style-type: none"> <li>○ On-chain encryption of merchant transactions to ensure GDPR and other privacy measures;</li> <li>○ Byzantine Fault Tolerance with Proof-of-Stake.</li> </ul>	<ul style="list-style-type: none"> <li>○ Open blockchain platform for mass adoption of any merchant and platform to start accepting fraud free payments.</li> </ul>

\*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	<p>The top 21 nodes of the network whom are voted in by token weight.</p> <p><i>50M SPND min. requirement</i></p>	<ul style="list-style-type: none"> <li>• Stake SPND deposit;</li> <li>• Dedicated IP;</li> <li>• Meet infrastructure requirements;</li> <li>• Act in accordance to privacy measures and GDPR.</li> </ul>	<p>Validator Nodes have the capability to do the following:</p> <ul style="list-style-type: none"> <li>• Govern Protocol Changes;</li> <li>• Validate Merchant Transactions;</li> <li>• On-board Merchant Nodes;</li> <li>• On-board Financial Nodes;</li> <li>• Perform Settlements;</li> <li>• Verify transactions on the network</li> <li>• Send &amp; Receive transactions;</li> <li>• Validate &amp; read data</li> <li>• Earn network fees &amp; block rewards</li> </ul>
Merchant Nodes	<p>Merchants enabling Spendchain payments</p> <p><i>500K SPND min. requirement</i></p>	<ul style="list-style-type: none"> <li>• Stake SPND deposit;</li> <li>• Run a Merchant Node;</li> <li>• Register with Validator Nodes;</li> </ul>	<p>Merchant Nodes have the capability to do the following:</p> <ul style="list-style-type: none"> <li>• Process Proof-of-Purchase transactions;</li> <li>• Send &amp; Receive transactions;</li> <li>• Validate &amp; read data;</li> <li>• Access Network Rewards to offer users.</li> </ul>
Financial Nodes	<p>Financial Institutions, Payment Processors, and others who will settle SPND and currencies deemed stable.</p> <p><i>5M SPND min. requirement</i></p>	<ul style="list-style-type: none"> <li>• Stake SPND deposit.</li> <li>• Run a Financial Node;</li> <li>• Register with Validator Nodes;</li> </ul>	<p>Financial Nodes have the capability to do the following:</p> <ul style="list-style-type: none"> <li>• Settle transactions for Merchant Nodes;</li> <li>• Process conversions of fiat and cryptocurrencies to selected Merchant Node preferences;</li> <li>• Verify transactions on the network;</li> <li>• Send &amp; Receive</li> </ul>

			transactions; <ul style="list-style-type: none"> <li>• Validate &amp; read data;</li> <li>• Earn settlement fees.</li> </ul>
Client Nodes	Everyone.	<ul style="list-style-type: none"> <li>• Stake SPND resources.</li> </ul>	Client Nodes have the capability to do the following: <ul style="list-style-type: none"> <li>• Verify transactions on the network;</li> <li>• Send &amp; Receive transactions;</li> <li>• Validate &amp; read data</li> </ul>

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<sup>28</sup>. 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<sup>29</sup>. The Tendermint Core is known for powering the Cosmos blockchain<sup>30</sup> 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<sup>8</sup>. 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.<sup>9</sup> 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<sup>31</sup> 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<sup>11</sup> 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 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<sup>32</sup> 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.<sup>32</sup>

## 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)<sup>33</sup> 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.

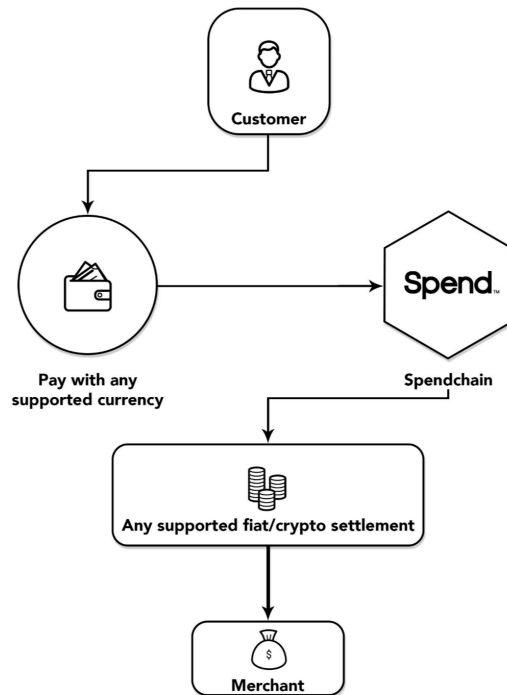
## Proof-of-Purchase

This consensus method is a protocol created to work in tandem with the Tendermint core of Spendchain which operates a Byzantine-Fault Tolerance Proof-of-Stake blockchain. Proof-of-Purchase enables users whom use the protocol to complete purchases with other members/merchants on the network to be eligible to earn a rewards percentage based on the total output of the transaction. This has been utilized on the Spend Wallet mobile application and Spend Visa Card as a primary distribution tool to help earn SPND from the blockchain.

Users who have been early adopters of the blockchain and/or protocol have received SPND while earning them from their purchases via Proof-of-Purchase.

## 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.

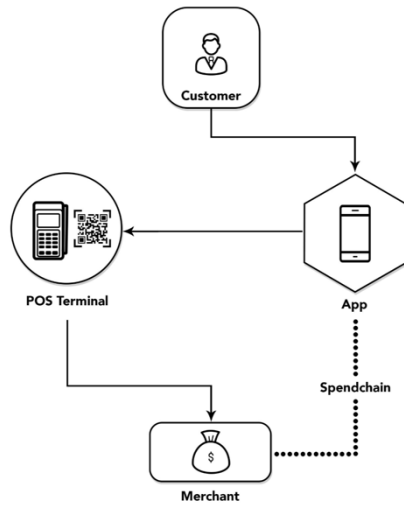
## **Validator Nodes**

Validator Nodes are responsible for securing the network, verifying transactions, and producing blocks on Spendchain. Validators operate on the Spendchain network by staking/bonding Spendcoin on the network. The top 21 Validator based on token vote weight will be assigned Validator status on Spendchain and will handle validator responsibilities. Validator nodes collect transaction fees and earn block rewards.

## **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.





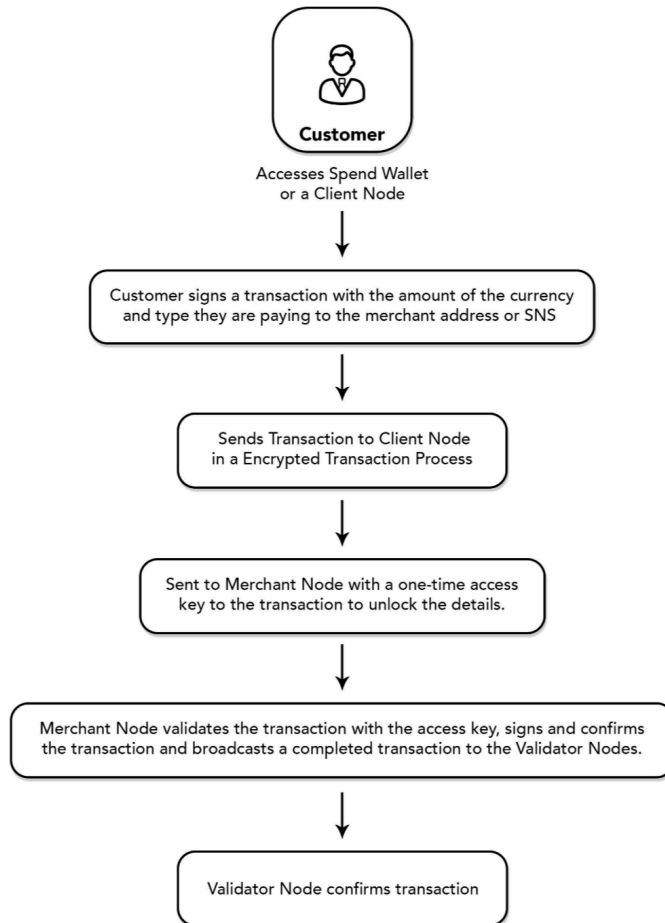
## 5. Network Settlement

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.

### 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<sup>34</sup> 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	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

`settlement` of the `settlement-currency` to the Merchant Node	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 and Binance Chain as a BEP2 token with a 2 billion supply. These tokens will be converted to the native Spendchain Spendcoin when the main network launches with a genesis of 4 billion Spendcoin minted on Spendchain granting an equivalent proportion to the non-native tokens. Spendcoins were created by the Spend Foundation, a non-profit organization in Europe and 50% of the supply has been gifted to Spend

Europe Ltd. The remaining 50% supply will be distributed to the network through Proof-of-Purchase which has enabled users to earn Spendcoins since its launch to use within the ecosystem of products that are available for them.

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**, **Financial**, and **Client** Rewards are specific per transaction and are dynamic by design. **Validator** rewards are per block and static. These rewards are set by the Validators through on-chain governance. Initial rewards will be set at 10 SPND per block, with block times aimed to be one to five seconds, which will be under a 10% annual inflation rate. This inflation rate on the network will be a decreasing rate year-over-year. The maximum validators can change the inflation rate is to 10% and the lowest rate being 1%.

Spendcoin (SPND) is a unit representing fees/compensation for Merchant and Financial Nodes performing transaction and used by Validators to secure and protect the network with an incentive to run validator nodes. Current Distribution of Spendcoin allocation is as following:

Allocation	Purpose
Distribution	As Spendcoin never conducted an Initial Coin Offering (ICO), the network Distribution enables users to earn Spendcoin through various public programs and have the ability to access services in the ecosystem with the use of Spendcoins.
Spend	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 , Spend Wallet App, and the Spendchain blockchain infrastructure.

## 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 6% rewards back funded by the network's distribution protocol through its Proof-of-Purchase protocol. These rewards are based on Validator nodes to accept through Financial Node marketing requests that are consistent with the protocols intended use.

### **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<sup>35</sup> 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 then 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. "Swift Financial Traffic Figures" <https://www.swift.com/about-us/swift-fin-traffic-figures>
6. "Central Bank Data" <https://www.frbservices.org/resources/central-bank/index.html>
7. "NACHA ACH Volume" <https://www.nacha.org/news/ach-volume-grows-more-25-Grocery%20Discounters%20Report%20by%20FBIC%20>
8. "ACH Specifications" <http://www.treasurysoftware.com/ACH/ACH-Specifications.aspx>
9. "ACH Moving Payments Faster" <https://www.nacha.org/rules/same-day-ach-moving-payments-faster-phase-1>
10. "FinCEN" <https://www.fincen.gov>
11. "Hackers Steal \$81 million" <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html>
12. "Bangladesh Bank Robbery" [https://en.wikipedia.org/wiki/Bangladesh\\_Bank\\_robbery](https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery)
13. "Nirav Modi and the \$177 billion PNB fraud" <https://www.thehindu.com/business/Industry/all-you-need-to-know-about-nirav-modi-and-the-177-billion-pnb-fraud/article22753973>
14. "Fraud RBI Deputy" <https://www.governancenow.com/news/regular-story/pnb-fraud-rbi-deputy-governor-had-warned-about-swift>
15. "World Payment Reports" [https://www.capgemini.com/en-us/wp-content/uploads/sites/2/2017/10/world-paymentsreport-2017\\_year-end\\_final\\_web-002.pdf](https://www.capgemini.com/en-us/wp-content/uploads/sites/2/2017/10/world-paymentsreport-2017_year-end_final_web-002.pdf)
16. "SBI Group" <http://www.sbigroup.co.jp/english/investors/disclosure/presentation/pdf/170727presentations.pdf>
17. "McKinsey Industrial Study" <https://www.mckinsey.com/~media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20mixed%202015%20for%20the%20global%20payments%20industry/Global-Payments-2016.ashx>
18. "Ripple Solutions" [https://ripple.com/files/ripple\\_solutions\\_guide.pdf](https://ripple.com/files/ripple_solutions_guide.pdf)
19. "XRP with Western Union and MoneyGram" <http://fortune.com/2018/02/14/ripple-xrp-western-union-moneytransfers/>
20. "Union Pay Statistics" <http://travelpaymentsdirect.com/unionpay/up-statistics/>
21. "Visa USA figures" <https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf>
22. "MasterCard data" <https://newsroom.mastercard.com/press-releases/mastercard-incorporated-reports-fourth-quarter-and-full-year-2016-financial-results>
23. "AXP Analyst"

- <http://www.snl.com/interactive/lookandfeel/102700/AXP2015AnalystDay.pdf>
24. "JCB World Card Issuing" [https://www.global.jcb/en/businesses/card-issuing/world-report/pdf/WR\\_No.56.pdf](https://www.global.jcb/en/businesses/card-issuing/world-report/pdf/WR_No.56.pdf)
  25. "NIH Gov Report" <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4341817/>
  26. "Card Association Schemes" [https://en.wikipedia.org/wiki/Card\\_association](https://en.wikipedia.org/wiki/Card_association)
  27. "AliPay Statistics" <https://expandedramblings.com/index.php/alipay-statistics/>
  28. "Mobile Wallets" [https://www.ipsos.com/sites/default/files/ct/publication/documents/2017-08/Mobile\\_payments\\_in\\_China-2017.pdf](https://www.ipsos.com/sites/default/files/ct/publication/documents/2017-08/Mobile_payments_in_China-2017.pdf)
  29. "Paypal total volume" <https://www.statista.com/statistics/277841/paypals-total-payment-volume/>
  30. "Paytm" <https://expandedramblings.com/index.php/paytm-statistics-facts/>
  31. "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>
  32. "Coinbase Launches Commerce Button to Accept Crypto Payments." <https://www.coinspeaker.com/coinbase-launches-commerce-button-paypal-like-plugin-accept-crypto-payments/>
  33. "Tendermint – Blockchain Consensus" <https://tendermint.com>
  34. "Enigma Privacy Protocol Solves Key Blockchain Issues" <https://blokt.com/interview/enigmas-privacy-protocol-solves-key-blockchain-issues-preventing-global-adoption>
  35. "Trusted Execution Environments" [https://en.wikipedia.org/wiki/Trusted\\_execution\\_environment](https://en.wikipedia.org/wiki/Trusted_execution_environment)
  36. "Blockchains and Trusted Execution Environments" <https://www.csail.mit.edu/event/blockchains-and-trusted-execution-environments-towards-new-security-paradigm>
  37. "Tree Signatures using Hash Trees" <https://medium.com/@g.andrew.stone/tree-signature-variations-using-commutative-hash-trees-4a8a47d4f8ce>
  38. "Confidential Transactions" <https://elementsproject.org/features/confidential-transactions>
  39. "Decentralized Identity using Civic" <https://www.civic.com/blog/5-key-benefits-of-decentralized-identity/>
  40. "Spend Authorization Engine" <https://spend.com>
  41. "Date Structure" <https://www.techopedia.com/definition/1149/data-structure>