Copy

Litepaper

Introduction

Throughout the centuries, the tools of money have evolved to be evermore inclusive and accessible in an increasingly globalized and borderless world — from trading metal coins to investing in stocks or sending online bank transactions. However, the centralized traditional financial systems, which historically provided these tools, tend to be unable to deliver flexible and composable services. Global fiat transfers and interactions in traditional finance suffer from high fees, slow speeds and limited optionality. In contrast, the explosive growth in the world of decentralized finance (DeFi) has brought about tools for building innovative financial products for future generations. But to date, bridging compliant fiat fintech services over to DeFi ecosystems has been a struggle. Enter Pendulum.

Built on Parity's Substrate framework, Pendulum establishes the missing link between fiat and DeFi with a sophisticated smart contract network. Pendulum chain aims to become the one-stop hub for the internet of fiat. Innovations that Pendulum will bring include:

- Cross-chain trust-minimized bridges
- A network optimized for a broad basket of fiat-pegged stable tokens
- Next-generation smart contract technology
- Opt-in compliance layer with privacy features
- Seamless on/offramps standards for integrations into local banking networks

Archived copy · cryp2nova.com

This litepaper will present an outline of the technology and the plans to build Pendulum chain into a critical piece of Web3 infrastructure.

Features

Cross-chain bridges

One of the core pillars of Pendulum is its capacity to collect and connect fiat-pegged tokens from the most prominent blockchain ecosystems into a single, optimized blockchain system. By giving project developers and token holders access to a broad basket of fiat tokens, Pendulum unlocks an evolution in money markets and borderless financial transactions.

Connecting across different ecosystems requires different solutions depending on the nature of the target network: in some cases it will be network-specific bridges, in other integrations into multichain bridges or the DotSama relay chain through the cross-chain messaging protocol. In order to ensure that the bridged tokens are distributed as wide as possible within the DotSama ecosystem, a Statemine/Statemint integration is planned. One key design principle is to ensure that the bridge technologies are as trustless and robust as possible. In the below section, we will look at some of the planned bridge technologies and options.

Spacewalk: Stellar bridge

The Stellar network↗ is an open blockchain with a focus on efficiency in speed and transaction costs, as well as integrations into the traditional financial system. It has a rich ecosystem with a focus on compliant fiat-pegged tokens and local (as well as instant, in a growing number of countries) fiat on- and offramps. Historically, Stellar has been optimized for speed and low transaction costs and not to execute sophisticated smart contracts at scale, which has largely isolated the network from the DeFi industry. Connecting Stellar with the DotSama ecosystem means that it will be possible for Stellar tokens to be exposed to more sophisticated smart contracts, while users in the DotSama ecosystem can access a larger basket of fiat stable tokens.

Archived copy · cryp2nova.com

Spacewalk↗ is a trust-minimized bridge and the first to connect the Stellar network and the DotSama ecosystems. Based on XCLAIM and interBTC, it is implemented as a Substrate pallet and allows any Substrate-based blockchain to implement a direct Stellar bridge.

Spacewalk bridge diagram

The architecture of the bridge consists of the following components:

- **Vaults:** this is a set of escrow accounts used to lock assets in Stellar. Their behavior is defined in XCLAIM and interBTC. In Spacewalk they have an additional property: each vault has an allowlist of assets that it can lock and support for bridging operations between Stellar and the Substrate chain. This allowlist is implemented through trustlines↗ of the Stellar account. There can be at most 1000 supported assets per vault due to limitations in Stellar. Stellar users initiate a deposit by sending tokens to an appropriate vault, which they request from the bridge pallet prior to the deposit. Likewise vaults will unlock and send tokens back to Stellar accounts during a withdrawal. Every vault needs to provide collateral with DOT or KSM (or related) tokens with the bridge pallet. These tokens are slashed in case the vault misbehaves.
- **Bridge Pallet:** this is the main component of the Spacewalk bridge that implements all logic on the side of the Substrate-based chain. Its behavior is based on interBTC. It is particularly responsible for minting tokens during deposits and burning tokens during withdrawals. It is able to support any Stellar asset by employing the Tokens↗ and Currrencies↗ pallets of the Substrate Open Runtime Module Library. The storage of the bridge pallet maintains the complete state that is required for the bridge to work correctly. This state contains (among others): the account ids of the vaults, the asset allow lists of each vault and book keeping information about the state of the Stellar network.

Archived copy · cryp2nova.com

- **Stellar Oracle:** is a decentralized system that provides information about the state of the Stellar network to the bridge pallet. In interBTC this is implemented through a Bitcoin chain relay. However, for reasons explained above we cannot implement a chain relay for Stellar in the same way. The Stellar oracle is trustless and reliable and its functionality is based on specific unique aspects of Stellar:
    - The Stellar network has multiple tier levels, where the nodes in Tier 1 enjoy the highest level of trust of its peers. There are currently 23 Tier 1 nodes; this set and its structure is rather static and only changes rarely. It only ever changes through a voting process. We will incorporate complete information about the Tier 1 network in the bridge pallet.
    - Every Stellar node has a static signing key pair and signs messages that it gossips to the network. Particularly, every node announces through a signed message that a block has been finalized. The decentralized oracle will forward these signed messages from Tier 1 nodes to the bridge pallet. This way the bridge pallet can reliably infer what Stellar blocks are finalized.

Cosmos bridge

Similar to Polkadot, Cosmos is a decentralized ecosystem of independent parallel blockchains that can scale and interoperate with each other via a common messaging standard. This network of networks has seen enormous growth and has some of the most popular fiat-pegged tokens in the cryptocurrency sphere.

Pendulum's Cosmos bridge will be based on the Substrate-IBC pallet↗ developed by Astar↗.

Archived copy · cryp2nova.com

Relay chain integration (XCMP)

The relay chain sits at the heart of the Polkadot and Kusama networks of networks; it provides both security and interoperability between the parachains. The cross-consensus message format (XCM) describes the methods for message transfer between different consensus systems. Cross-chain message passing (XCMP) is a protocol that builds on the XCM architecture. The XCMP protocol allows parachains to exchange messages with other parachains on the same relay chain and guarantees the delivery of these messages. The message delivery is not only guaranteed but also trustless, meaning that Polkadot's shared security ensures the correctness and ordering of the message delivery.

To communicate, parachains first have to establish a messaging communication channel with each other. These channels are one-way, but there can be up to 1 channel for every (sender, recipient) parachain pair, allowing bidirectional communication. The channels work with a queue of ordered messages queued by the sender and eventually acknowledged by the recipient parachain. Both parachains are expected to monitor the state of the relay chain to know what is currently in the message queue. However, "XCM is not designed in that every system supporting the format is expected to be able to interpret any possible XCM message. Practically speaking, one can imagine that some messages will not have reasonable interpretations under some systems or will be intentionally unsupported." [Source: https://wiki.polkadot.network/docs/learn-crosschain]

While it can be used in many ways, the most common use-case for inter-chain messaging is probably handling and moving assets between different parachains. For example, XCM allows the teleportation of assets between different parachains. Pallets like the 'xtokens'↗ module make it easy for parachains to leverage the capabilities of XCM to integrate cross-chain token transfer functionalities to their parachain. This is optional however, since every chain has to proactively set up communication channels with other chains and listen to respective messages.

Archived copy · cryp2nova.com

Forex-optimized network

Executing foreign exchange (“forex”) at scale on the network demands access to ample liquidity of trustworthy fiat tokens, as well as robust infrastructure optimized for the fiat decentralized apps (“dApps”). The question of liquidity access is solved first and foremost through cross-bridging tokens from other networks (described elsewhere in this paper), while the question of token _quality _is addressed by a decentralized incentive scheme. On the infrastructure-level, Pendulum plans to provide a suite of core components that developers can use to build their applications.

On-chain token governance

With any open-ended and permissionless system comes a relatively high level of noise compared to closed and censured systems. With the explosion in fiat stabletokens, it is natural that some have been more robust and trustworthy than others. As Pendulum plans to attract high-quality fiat tokens from around different ecosystems, there should be some mechanisms that encourage the best of tokens to be promoted and widely used on the network. This mechanism is part of the decentralized governance structure of Pendulum.

Overall, the Pendulum on-chain governance process is expected to be established similarly to the core Polkadot governance mechanism ↗, with one additional feature: a token committee. Much like the The Technical Committee on the Polkadot, the token committee has been granted the right to award a limited set of assets on the network favorable terms, such as lower transaction fees, if they fulfill certain standards. This structure incentivizes availability of robust and trustworthy tokens.

Archived copy · cryp2nova.com

Fiat-first runtime modules

To give the optimal developer experience, a suite of Substrate runtime modules (“pallets”) are provided. Common features, such as price feed oracles or particular swap designs, are offered through the Pendulum API which makes it simple to include in a dApp. By designing Pendulum from the ground up to support developers building fiat-focused smart contracts and dApps, the network can attract the next generation of forex projects.

Traditional finance networks integrations

Building integrations into the traditional financial networks broadens the scope of Pendulum as both consumers and financial institutions are able to participate in the network activities. With an emphasis on both the fiat deposit and withdrawal processes and an *optional* data layer for the transmission and management of compliance data, Pendulum allows dApps to build seamless user experiences for consumers. At the moment fintech companies are hesitant to go near DeFi for concerns of regulatory issues. This compliance process, on a scalable parachain designed for fintech companies, can allow traditional finance to start taking advantage of fiat use cases on DeFi.

Direct fiat on/offramp

The often complex user journey when moving funds from traditional financial institutions onto blockchain has been one of the major obstacles to broad adoption of cryptocurrencies and blockchain technology as a whole. Pendulum aims to reduce this barrier with a twofold approach: direct on/offramp partners and ramping standards. On/offramps (“ramps” or “anchors”) services are entities converting fiat currency to tokens on a blockchain and vice versa. By encouraging such fiat ramps to integrate directly into the Pendulum network, customers can on/offramp between Pendulum and their local banking networks in their native fiat currency.

Archived copy · cryp2nova.com

Pendulum will develop a suite of open-source ramp standards (the technical and business rules by which a ramping service should act) which will be usable for any ramp in the entire DotSama ecosystem. By driving innovative ramping solutions to the network, Pendulum will foster more liquidity and closer cross-parachain interoperability.

Opt-in compliance data layer

In order to make the TradFi integrations as seamless as possible, Pendulum includes a voluntary and trustless data layer for the transmission of compliance data. The layer governs the secure, end-to-end encrypted passing of information between two entities on the network, for example, in the context of an offramp transaction. The standard is currently being defined alongside experienced compliance service providers with the goal of minimizing the number of compliance checks that a given customer must undertake in the process of interacting with multiple regulated services. For example, a customer may onramp with credit card in one country, but eventually offramp with a neobank in another — the customer can in this case volunteer to let the two services securely share the compliance data, thereby avoiding multiple compliance processes.

Next-generation smart contracts

Pendulum is built on Substrate, a blockchain framework developed by Parity Technologies. The framework was used to build both Polkadot and Kusama. The advantages of Substrate are many: in addition to having native compatibility with the Polkadot chain, Substrate has cross-coding language support, forkless upgrades with built-in upgrade coordination, deterministic finality (for fast consensus reaching), and a suite of pre-built but customizable components (“pallets”).

As a framework, Substrate comes with a wide range of features for creating and deploying a blockchain system, which can be customized according to preference. The following section presents a highlight of some of the technical decisions of the Substrate implementation and the reasoning behind them.

Archived copy · cryp2nova.com

In order to bring the most capabilities and affordances to developers, Pendulum will introduce and implement a suite of next-generation smart contract technologies. The approach is twofold: implement, invest and develop WebAssembly (“Wasm”), which is the future of smart contract execution layers, while also supporting the incumbent Ethereum Virtual Machine (“EVM”), which, despite some of its limitations, is still favored by a large number of developers.

WebAssembly (Wasm)

Wasm, a Web-technology developed and maintained by a W3C workgroup that includes, among others, Google and Mozilla is heralded as the next base layer for decentralized applications. Using Wasm for smart contracts has lots of advantages like performance that is near native machine code, a small size, and efficient just-in-time execution. Smart contracts can be written in any of the many languages that can compile to Wasm, including C/C++, Rust, Go, and also Solidity, the most widely used programming language for smart contracts. Pendulum developers will be able to write smart contracts in the language of their choice and use existing tools and methods, which ultimately flattens the learning curve for the community and decreases implementation costs for dApp and project builders.

While Wasm has already seen broad adoption on the open Web, the integration into blockchain systems is still in its early stages. For the long awaited Ethereum 2.0, Wasm has been a candidate to replace the EVM replacement, but not yet fully finalized. Within the DotSama ecosystem, Pendulum is participating in the community effort to improve the performance and security of Wasm.

EVM support

The EVM is a milestone in the history of blockchain technology, the very first smart contract execution engine. However, it is quite inefficient because every instruction operates on 256 bit values, which is unnecessary complex for most applications. This makes executing smart contracts for EVM quite inefficient compared to WebAssembly. Nevertheless it is still the most popular virtual machine standard for smart contracts.

Archived copy · cryp2nova.com

Substrate comes with a library of modules called Frontier ↗ that allow to create an Ethereum compatibility layer. Frontier comprises an EVM execution engine which can run EVM smart contracts, in particular, smart contracts that have been written in Solidity and compiled to EVM byte code. For every Substrate account there will be an associated Ethereum address so that users can operate with Ethereum-like addresses instead of with the native address format of Substrate. Furthermore, it provides an Ethereum compatible RPC interface so that users can utilize their familiar wallets from the Ethereum ecosystem like Metamask for example.

Pendulum will integrate Frontier to allow execution of smart contracts originally written for Ethereum and compatible blockchains. On the one hand, this allows Pendulum and its community of developers to tap into the massive library of readily available Ethereum smart contracts, and on the other hand smart contract creators can directly deploy their projects to Pendulum and utilize them for the basket of stablecoins accessible on Pendulum. This hybrid approach of the contracts pallet and Frontier combines the best of both worlds and allows smart contract creators to use their favorite programming language and to target their favorite machine.

Scalability

Pendulum will focus on high scalability. This allows for a large number of transactions per second and will keep transaction fees low as surge pricing effects will lead to highly increased fees in heavily congested networks.

The Polkadot network is a collection of blockchains called *parachains*, where Pendulum will be one of these parachains. They are connected to a central special purpose blockchain called the relay chain. The relay chain's purpose is to achieve global consensus among all parachains in the network. The number of transactions per second that Pendulum will achieve is determined by its interaction with the relay chain and how the block validation mechanism works.

Archived copy · cryp2nova.com

A blockchain behaves like a globally distributed state machine: it stores one unique state that all nodes in the network agree on. Furthermore the logic of the blockchain defines a state transition function that determines how the global state changes given a block of transactions. At certain intervals a node in the blockchain is selected to *author* a new block. It will then gossip the block through the network and the other nodes will *validate* that the block determines a correct state transition and that they agree about the new state.

In Polkadot different parts of the network are responsible for block authorship and block validation: authorship happens in the parachain whereas validation is performed in the relay chain. The relay chain nodes need to fetch both the state and state transition function from the parachain nodes before they can start to validate a parachain block. This is already done very efficiently – only the relevant parts of the state are transmitted – but still requires a lot of communication between parachain and relay chain nodes and limits the transaction throughput.

For that reason currently only about 8% of the parachain blocktime can be used to execute transactions. This roughly translates to 250 transactions per second for basic payment transactions and is more limited for transactions that execute complex smart contracts.

There are many improvements planned for Polkadot that will massively increase its throughput and will greatly impact the scalability of Pendulum. Combined these improvements will increase the number of Pendulum's transactions per second by up to two orders of magnitude. Examples of these efficiency gains are:

- Currently the parachain and relay chain blocks need to be created synchronously during the same timeframe. In the future this will be decoupled and allows for a higher ratio of the blocktime to be usable for transaction execution.
- Relay chain nodes will be able to process multiple parachain blocks at once.
- The communication between relay and parachain blocks will become more efficient so that less data needs to be transported or can be prefetched ahead of time.

Archived copy · cryp2nova.com

- Offload Polkadot governance and DOT token processing from the relay chain into a separate parachain so that the relay chain nodes can focus on parachain block validation only.
- Introduce multiple relay chains that can split work even further
- There will be many efficiency improvements for the execution of WebAssembly smart contracts.

Although these improvements will make Pendulum a highly scalable blockchain, we will further increase scalability through second layer technologies such as Plasmas and Rollups.

Privacy

While blockchain transactions in general tend to be pseudonymous this level of obfuscation is in some cases not sufficient — for example, a business may not want to reveal their cashflows on a public ledger. Pendulum will introduce a zero-knowledge privacy layer, which allows users to perform a set of transactions without revealing the details unless explicitly allowing third parties to see the transaction data.

To make it harder to trace the path of assets through the network, protocols like Tornado Cash ↗exist, breaking the link between source and destination addresses. Zcash was the first blockchain to integrate zero-knowledge cryptography in the form of so-called zk-SNARKS enabling users to shield transactions, thus keeping the transaction information private and in control of every user. Having the option to reveal the details of a transaction is important because regulators or auditors might require insights into transactions for legal matters.

On Zcash, two different types of addresses exist, private 'z-addresses' and transparent 't-addresses'. Multiple transaction types exist, depending on the source and destination address type. For example, a transaction between two z-addresses appears on the public blockchain, but the addresses, transaction amount, and memo fields are encrypted and not publicly visible. However, the details of a transaction between two t-addresses are publicly visible. Therefore Zcash offers conditional/opt-in transaction privacy depending on the used address types.

Archived copy · cryp2nova.com

A different approach, assuming transaction details are not publicly visible, would be to have the dApp store the relevant transaction details (sending/receiving address, amount, timestamp, etc.) off-chain, which they might disclose to a third-party (regulators/auditors) if needed.

So far, the third party would not know if these are the correct details of the transaction that happened on-chain. That's why for every private transaction, the blockchain would store a corresponding zero-knowledge proof which can be used to prove that the information revealed by the dApp is actually connected to the target transaction.

For Pendulum, we will develop a conditional transaction privacy feature that works similarly to one of the two mentioned approaches.

MEV protection

Miner Extractable Value ↗ is a form of front-running executed by miners on a network, which has recently become a prominent issue in arbitrage transactions on Ethereum and others. Pendulum is likely to pick one of two ways to mitigate against MEV: through direct protection or protection through privacy. Direct protection is a method where an independent network of nodes order transactions to be incorporated in the next block, thereby obfuscating the transaction order to MEV exploiters. Transaction privacy can be achieved through either zero-knowledge proofs (zk) or a trusted execution environment (TEE). Since TEE requires custom hardware, thus increasing the barrier to entry for node operators, the most likely path to achieve privacy would be some form of zk.

Archived copy · cryp2nova.com

There are fundamentally two ways for miners to extract additional value when bundling blocks of transactions: value extraction by reordering transactions or denying some of them. Miners can use reordering to capitalize on the profits of their own transactions by putting them before or after user transactions. Likewise, miners can decide not to include a particular transaction or even replace it with their own. Preventing or minimizing these capabilities minimizes the disadvantages for the casual user.

One way to prevent miners from establishing a transaction order that benefits them most is by splitting the block production into two separate steps, building and execution. In the building step, the builder gathers the transactions it wants to include in the next block from the pool. The set of transactions is sent to a block executor who will shuffle the transaction and arrange them in a specific order. The builder and executor use a cryptographic protocol where the builder gives instructions to the executor about how to order the transaction. This happens in a blind fashion: the builder choses the instructions randomly but does not know what concrete order of transactions these instructions imply – only the executor is able to understand them and to act on them. However, the builder will be able to validate retrospectively that the instructions have been followed correctly. This separation of concerns ensures that as long as the builder and executor don’t collude, they cannot deliberately extract value from the transaction order. While this reduces the potential extractable value, it also introduces a performance overhead since block production is now a 2-step process.

Encrypting transactions before sending them to the transaction pool lessens the motivation of miners to deny transactions since they cannot know which transaction to reject to gain a personal advantage. A two-layer encryption that first uses the block builder's public key and second the block executor's public key ensures that only the block executor knows the transaction details while the block builder that chooses the transactions does not. However, the necessary decryptions consume more resources and increase the gas costs. Furthermore, the block builder and block executor nodes must be chosen beforehand since the transaction is encrypted with their respective public keys.

Archived copy · cryp2nova.com

Team

An ambitious vision with exciting technical plans is great and needed, but ultimately a project's long term success rests with the quality of its team. Pendulum is developed by SatoshiPay ↗, a global fintech company founded in 2014. Since its founding, SatoshiPay launched products such as B2B cross-border money transfer services, a Stellar open-source wallet and micropayment processing services. SatoshiPay CEO Alex Wilke ↗ has 6 SatoshiPay years and 18 years of operational experience behind him. CSO Dr Aaron Linder ↗, Physics PhD, leads the vision of the project and the technical team is led by CTO Dr. Torsten Stüber ↗, Computer Science PhD. Founder & Chairman Meinhard Benn ↗, who has been a blockchain programmer since 2011, guides the project with his high level oversight. Also, Danny Masters ↗, another early crypto adopter and current chairman of CoinShares ↗ is on the Satoshipay board of directors.

Summary

For fintech companies who need to level up efficiency, Pendulum is an interoperable parachain offering composable fiat services like: global payments, DeFi applications and yield farming. Unlike existing money ecosystems such as Terra, it supports compliant stable tokens. Pendulum's dApp ecosystem strategy includes building key partnerships (fiat anchors, chain bridges), incubating projects (forex AMMs, forex money markets) and grant programs (wallets & tools, fintech integrations). Pendulum can swing fintech fiat services into DeFi. Decentralized fiat. Limitless future.

Previous
Our Journey

Next
Tokenomics

Archived copy · cryp2nova.com

Last updated 2 years ago

Was this helpful?

Archived copy · cryp2nova.com