SushiChain

WHITEPAPER

Kingsley Hendrickse

SushiChain whitepaper version 0.0.1 (English)

Sushi Chain

Table of Contents

Disclaimer

The sole purpose of this white paper is to provide an overview of the SushiChain platform to those interested in learning more about the platform. The author believes that the information presented in this white paper is correct at the time of writing. It attempts to provide accurate information to potential community members in order for them to conduct their own analysis of the platform prior to taking any decisions to acquire Sushi or become full community members.

This white paper is not an offer to buy securities and is not in any way a solicitation for investment and therefore is not subject to any laws or regulations designed to protect investors. Any forward looking statements or information found in this white paper are purely estimates and are subject to unknown risks and uncertainties which may affect the outcomes and results as expressed in the forward looking statement or information.

This white paper is the official primary source of information about the SushiChain platform. Before taking part in this community you should check your local and federal laws for your country or jurisdiction.

Abstract

Bitcoin and subsequent cryptocurrencies have become very popular over the last few years for many reasons. However it is the underlying blockchain technology that Bitcoin is built on which provides huge potential to improve our future technology.

While cryptocurrencies provide the infrastructure for decentralised financial transactions there are other use cases emerging for blockchain that do not focus primarily on financial transactions. Platforms such as Ethereum have emerged which provide the ability to power blockchain based applications using smart contracts.

Our technology is constantly evolving and over recent years there has been an increasing trend of people using apps for all sorts of things both on their smartphones and computers. More and more people are looking to download the latest new and interesting apps and developers are catering for their needs by producing cross platform apps that solve all manner of problems.

With the rising popularity of both blockchain and apps the SushiChain platform aims to provide a platform for developers to produce a new evolution of apps that are built on the blockchain.

Developer Platform

SushiChain provides a plugin style architecture for building decentralised applications. This is achieved by running a local node and building the dApp by extending from a parent class in the node that provides access to functionality. The dApp infrastructure has hooks that fire when a block is pushed which gives access to the transactions contained within the block.

In addition a transaction contains a key field which is used to hold the name of the dApp. In this way dApp authors can listen for the name in the keyword field of a transaction and perform any logic based on this. Conversely dApps can be executed by sending a transaction containing a specific keyword that corresponds to an existing dApp.

When a node is started up it must be provided with a wallet. dApps only have access to the wallet of the node and therefore cannot operate on any other wallet except its own. This in turn means that dApps are very safe as they cannot perform autonomous functionality outside of the scope of the running node and the associated wallet.

A node can also be started in private mode which means it will not broadcast itself on the network and other nodes will not be able to see it. But the private node will still be connected to the network and be fully capable of executing dApps.

Since dApps are executed on the node there is no restriction to what can be built and there are no fees for executing dApps. This makes building and running dApps extremely cheap and scalability is achieved by starting up more nodes. A dApp can therefore consume other external APIs and execute any kind of code the author would like from local file operations, to third party integrations.

SushiChain also has a full API so developers can also choose to build a dApp using the APIs instead of running in a node. This provides complete flexibility to build dApps in any programming language. The API has websocket hooks for notification of new blocks in a similar way to the node dApp infrastructure.

A dApp can access the full functionality of its wallet and so can for example listen for some event and then send tokens or data in accordance with some logic flow as determined by the event. A basic example would be a dApp that waits for a specific amount of token to be deposited in a specific wallet from a specific sender and then automatically sends a token or data transaction back to the originator or elsewhere.

We believe this style of off chain logic provides a huge amount of flexibility in writing dApps and is at the same time very safe and if required also very private. SushiChain does not currently support on chain smart contracts but we have not ruled out adding such functionality in the future albeit probably in a very controlled and limited way.

We will be providing a Developer Platform containing tutorials, guides and help for developers wishing to build dApps on SushiChain. This platform will also be accompanied by a range of tools and templates aimed at making the development and testing process as easy and effective as possible.

dApp Store

SushiChain will feature a dApp store where dApp authors may list their dApp with a description and other appropriate details and information.

Listed dApps will be searchable, sortable and have both a rating system as well as a comments system. This will provide a mechanism by which to give dApp authors constructive feedback so they can take on board users opinions and experiences to better improve their dApps.

Initially all dApps can be listed with no restrictions but over time we will introduce some rules around minimum level of quality, age appropriation and content. We want to encourage a safe and secure ecosystem around dApps and will try to put in place safe guards around many of these areas over time.

Integrated Wallet & Chat

SushiChain has full command line support for wallets and interactions with the blockchain. In addition to this we will be providing an official cross platform light wallet which will be an Electron application. The application will allow adding of multiple wallets and will have full functionality to see balances of all tokens, send and receive tokens as well as executing dApps and purchasing human readable addresses.

When a new wallet is created it will be done in a secure manner forcing a user to create a password protected encrypted downloadable wallet file. There will be several tools provided in the wallet as well to allow users to encrypt / decrypt wallets and find information about the wallet. The wallet in general will not expose the raw private key and at most will expose a WIF (Wallet Information File) inside the encrypted wallet file.

Building on the official Electron wallet we will also be providing an integrated chat system. The chat system will be capable of full wallet functionality right within the chat. Sending and receiving tokens, purchasing human readable addresses and executing dApps. Phase one of the chat system will be purely peer to peer fully encrypted communication. A later phase will introduce multi chat, chat rooms and various other levels of chat functionality.

SushiChain currently has a built in peer-to-peer chat system at the most basic level and work will be carried out in this area to provide all the functionality mentioned. The integrated wallet & chat system will be available for the desktop, ios and android platforms.

Social Media Integration

As well as our own brand of encrypted chat we will provide a more limited and restricted set of plugins to well known popular chat platforms such as Slack, Discord, Telegram, Facebook and Gitter. Plugins for these platforms will require a user to login into their wallet securely via an authentication dApp in a process similar to OAuth before gaining access to wallet functionality within the respective chat systems.

This will make it very easy to send and receive SUSHI and custom tokens on all the major social media applications. This will also act as a gateway into the SushiChain platform allowing integration between social media and dApps. Allowing social media focused dApps to evolve in a safe and secure way will offer many opportunities to innovate within the crowded space.

Crypto Exchange

SushiChain allows developers to create their own custom tokens and send and receive these as well as use them in dApps. Therefore we would like to provide a means of exchanging these custom tokens with the default SUSHI token.

We will create our own crypto exchange that focuses on giving a great user experience when trading both SUSHI and custom tokens created on the SushiChain platform. This will also make it very attractive for projects to create custom tokens on the SushiChain platform and be able to list them without the huge listing fees that many existing exchanges currently charge.

It will also greatly simplify the process of creating and listing a custom token. The exchange will also be integrated into our wallet and chat applications running in ios, android and on the desktop. This will provide a very tailored experience for trading on the SushiChain platform.

We plan to launch our cryptocurrency exchange in several phases:

1. Exchange custom tokens with SUSHI
2. Exchange custom tokens with other custom tokens
3. Exchange custom tokens and SUSHI with fiat
4. Buy SUSHI and custom tokens with fiat

In this way users will have access to send each other SUSHI and other custom tokens as well as buy, sell and trade right within the integrated chat and wallet system. A future evolution of the exchange would be to allow trading with other cryptocurrencies using SUSHI as the base pair.

Payments Hub

Once the SushiChain platform starts to evolve and developers start building dApps we would like to provide a way to pay for things online and within dApps. To do this we will build a payment gateway which will allow developers and tech savvy users to add shopping baskets, stores and simple payment plugins that support paying for things in SUSHI and custom tokens.

As part of this work we will also define a stable token which can be used for payments as well as providing functionality that auto adjusts SUSHI and other custom tokens within the payment gateway to a range of fiat prices.

The Core Blockchain

SushiChain is an original custom blockchain implementation. It is not a fork or clone of any current existing blockchain project. SushiChain takes inspiration from Bitcoin and Ethereum and to some degree other existing blockchains. SushiChain is implemented in the Crystal programming language.

Crystal was chosen because it has many similarities to the Ruby programming language and shares the same kind of language syntax but with the added benefit of the executions speeds to the C programming language. Crystal is also statically typed and has a vibrant community.

The main features of SushiChain are:

1. An original blockchain with streamlined and simplified core components
2. A plugin style architecture for building decentralised applications with off chain logic
3. Full public REST API for building dApps in any programming language
4. Built in human readable addresses
5. Proof of Work consensus
6. CPU only mining using the award winning Argon2d hashing algorithm

There are 3 main command line programs which provide access to the SushiChain platform:

1. Sushi - the command line client
2. Sushid - the command line node
3. Sushim - the command line miner

User will mostly use the miner and the Sushi client to interact with a node. Most users will connect with the mainnet nodes or mining pool nodes. There is also a cross platform Electron wallet which will become the main interface for interacting with the platform.

As previously discussed there will also be a range of other supporting clients and plugins for various social media integrations that will provide a gateway into the platforms functionality.

The Blockchain platform itself has a plugin style architecture and the internal components are implemented in a similar way as user defined external components which we call dApps.

SushiChain implements the core blockchain concepts such as:

1. An immutable ledger which is stored on disk in a sqlite3 in-memory database.
2. Cryptography based on the SECP256K1 elliptic curve
3. OpenSSL ECDSA based wallet with private and public key pairs with address
4. Encrypted wallets using blowfish encryption
5. Peer to peer networking for nodes using the Chord networking pattern
6. Merkle tree hashing of blocks and transactions
7. Transactions and transaction and block validation
8. Built in default token SUSHI and the ability to create custom tokens for use in dApps
9. Rejected transaction handling
10. Transaction fees system
11. Human readable addresses
12. Real time peer to peer communications system capable of token transfer and messaging

There are many additional features that will be added to the base platform such as support for asset management, hierarchical deterministic wallets and two factor authentication. See the coin specification below for more information about the default token SUSHI.

As previously mentioned one of the main features of SushiChain is that it is CPU only mining. Proof of work is still the most proven consensus mechanism but things have gotten a little crazy with specialised rigs, ASIC chips, GPU mining and massive mining operations.

Limiting mining to the CPU is the most eco-friendly form of proof of work mining since CPU's require much less energy. This also allows for a more equally distributed participation in the mining process since anyone with a CPU can get involved using regular consumer hardware and without the need to spend thousands on expensive hardware and mining rigs.

SushiChain also features much faster block times between 10 seconds and 40 seconds which is a lot faster than Bitcoins 10 minute block rate and the 4 minute block rate of Ethereum. Also with super low fees this makes SushiChain very cheap and attractive for building dApps.

SushiChain also has a limited supply of the default SUSHI token which is set at 20 million and as such will help retain the coin's market value over time as the supply is reduced and the focus shifts to transaction fees and trading.

Smart Assets

SushiChain will feature a smart assets system. Assets can be registered on the blockchain with a set of properties that can be used to define the asset. An asset can also optionally contain bytecode compiled from a special smart asset language called Taro.

In this way you can write smart asset code which can mutate the properties of the asset. Assets can be queried to retrieve their data at a node via an asset API. Asset code can be invoked via transaction calls which execute the public asset functions that have been coded into the asset.

A practical example is when storing game assets in the blockchain that have mutable characteristics such as storing a sword asset which has properties such as strength, attack, magic buffs etc which can be mutated through usage or upgrades. In this case an asset function could be called to increase the strength of the sword asset as it gets levelled up.

The asset code could also apply additional logic to enforce limits or trigger the mutation of other properties. Asset code will only be able to interact with the assets own properties and will not be able to operate on a wallet or send token transfer transactions of any kind. However assets will be allowed to query data from other assets and call functions on other assets.

The Taro language will include many easy to use constructs for working with assets and there will also be a supporting asset test framework to help with the development of smart assets.

Smart assets will cost a fee to execute based on execution time and charged per millisecond from the wallet of the invoker. If the invoker runs out of Sushi the execution will stop.

The node will execute the smart asset code and charge the wallet supplied in the transaction that was used to invoke the asset. Of course the transaction will go through the same validity and signature checks as every other transaction to ensure security is maintained.

The smart asset bytecode is included in the transaction hash so once created cannot be changed. It can however be programmed to self destruct and also can have execution and visibility permissions set to specific wallets.

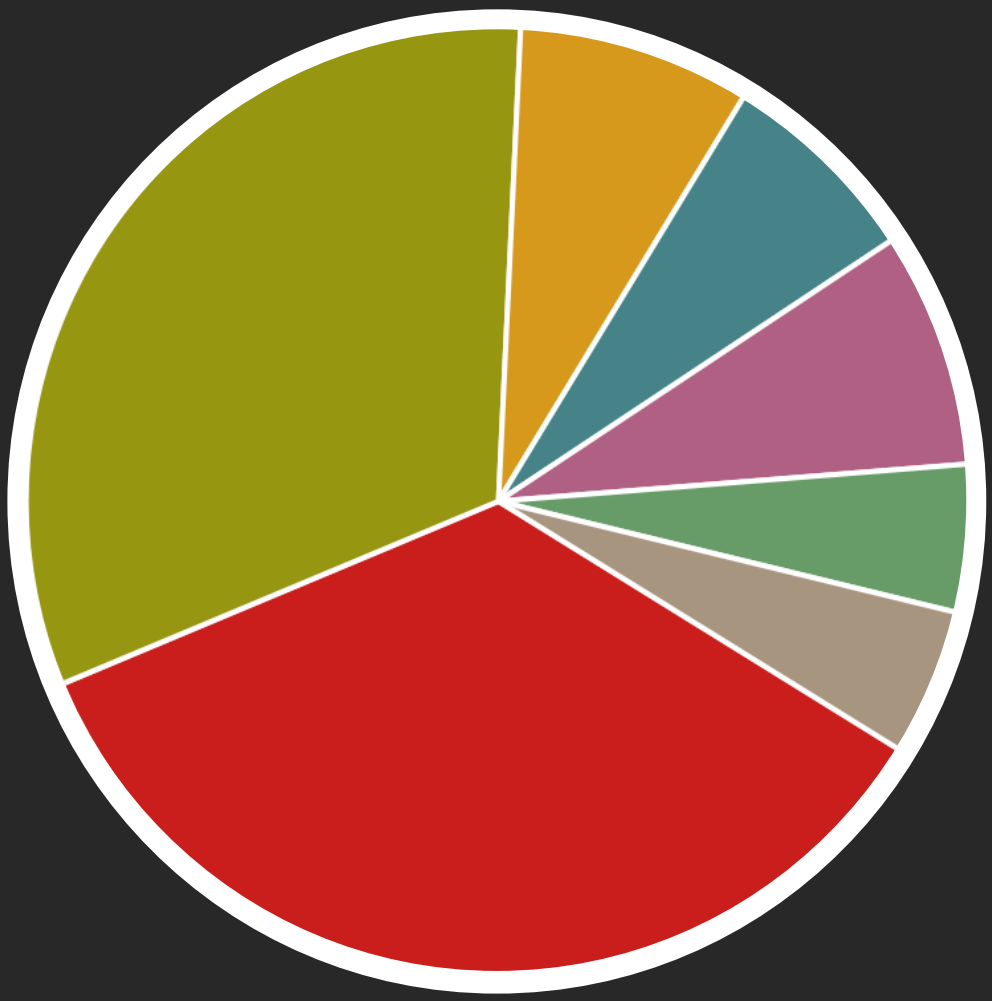
Pre-Mine

SushiChain will operate on a 10% pre-mine system. Pre-mining is very good for the development team so that they can use the coins to strengthen the community and pay for marketing, bounties, promotions as well as paying for related development such as graphic design, tools and hosting.

Below is an approximate guide to how the pre-mine coins would be used. The lead developer team amount is intended to help the lead developers pay for costs that occur now and into the future. The lead developer team will also receive 50% of the block rewards from the mainnet nodes in order to support ongoing development.

The remaining 50% of the block rewards from the mainnet nodes will be held in reserve following regular planning sessions to decide what the coin should be used for. All decisions about the expenditure of pre-mine and mainnet nodes will be publicly documented and reviewed regularly.

Usage	Amount (SUSHI)
Lead developer team	700,000
Exchange costs	640,000
Mainnet operation	160,000
External development	140,000
Community team	160,000
Airdrops	100,000
Future use	100,000
Total	2,000,000



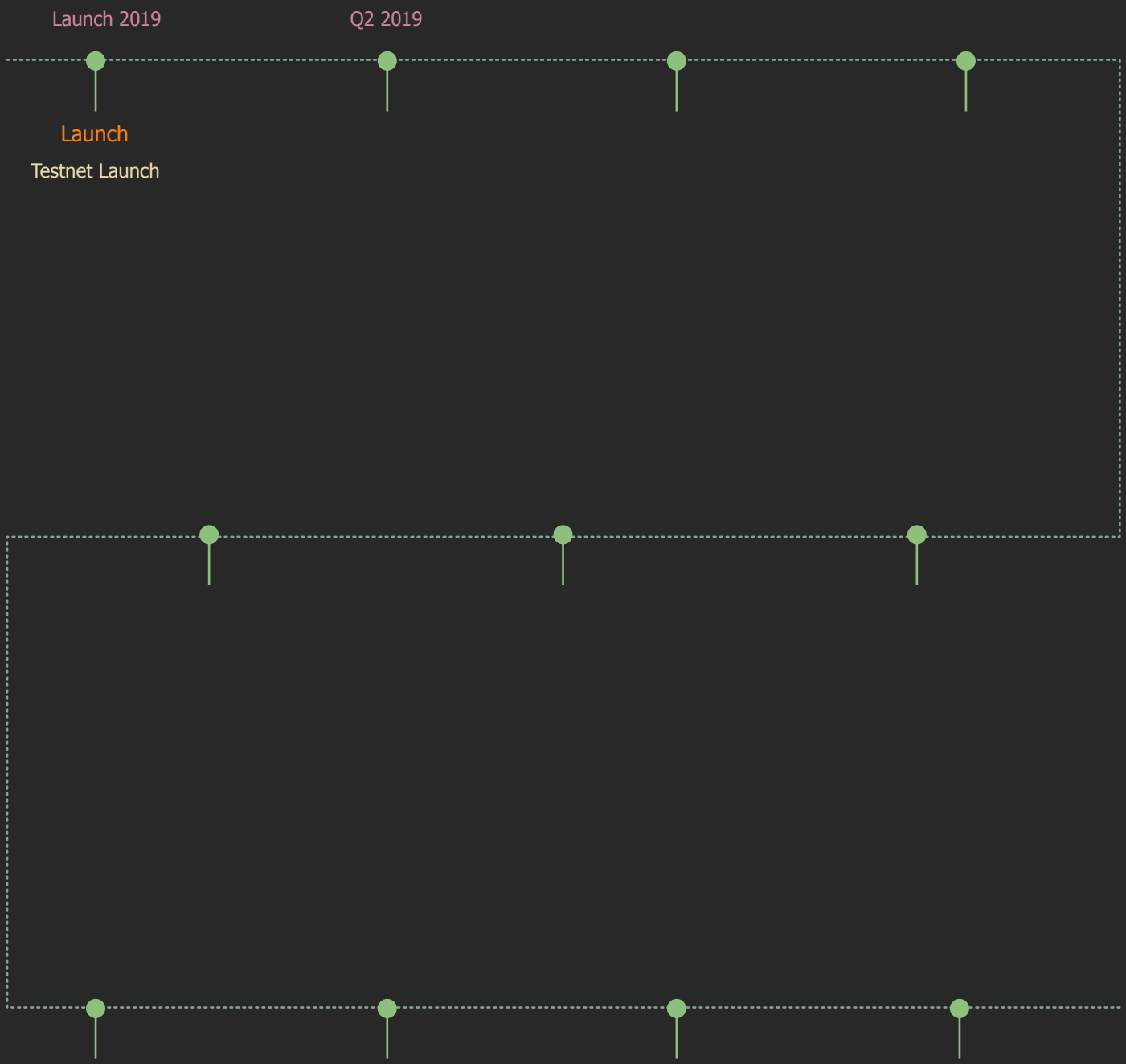
Planned dApps

The SushiChain team also plan to release several of our own dApps which will run on the SushiChain platform. The first dApp we plan to release is a trading card game called Guardian of Axum. You can find out more about Guardians of Axum at www.guardiansofaxum.com.

Guardians of Axum

Guardians of Axum is an online competitive turn based trading card game. Players buy decks of collectible cards and battle them out against each other in tournaments.

Road Map



Team Information

Kingsley Hendrickse
Lead Developer / Founder

Kingsley is an agile software developer and technology enthusiast. He is very interested in blockchain and cryptocurrency technologies. He also loves to eat Sushi - which is one of the main reasons he loves working on SushiChain!

Minesh Patel
Product Owner

Minesh is an agile business analyst with a passion for solving problems through technology. Takes ideas from conception to launch. Excited about how Blockchain will reinvigorate the internet as we know it. Often found savouring sashimi!

Tim Tennant
Advisor

Hands on leader of software design and development teams with over 20 years of experience with brands such as Barclays, UBS, Credit Suisse, Citibank, Sky, Vodafone and Mars as well as many smaller businesses. Currently he is CTO of Nivo Solutions, which is a fintech startup providing an instant messaging platform with bank standard authentication, ID&V and encryption built in.

Coin Specification

Coin name	Sushi
Coin ticker	SUSHI
Consensus	PoW
Block reward	0.5 SUSHI
Miner reward	Prorated on contribution
Block spacing	10 to 40 seconds
Pre-mine	2,000,000 SUSHI (10%)
Total supply	20,000,000 SUSHI
Maturity	20 Blocks
Minimum tx fee	0.0001
PoW mining algorithm	Argon2d
Port	3000

Each miner that is mining against a node which mints a new block receives a prorated amount of SUSHI based on their contribution to finding hashes. The total block reward is 0.5 SUSHI from which miners and the node itself receive their rewards.

The block spacing is determined using a custom algorithm that ensures a new block is minted between 10 and 40 seconds. Initially the block spacing is calculated on a per block basis until 720 blocks are reached after which the spacing is determined by the average elapsed time across the 720 blocks.