BHOLDUS

DEFI FOR THE REAL WORLD.

Whitepaper / 2021

Abstract

BHoldus Chain is a blockchain dedicated to decentralized financial (**DeFi**) applications and non-fungible tokens (**NFTs**). Our chain not only offers unprecedented high transaction throughput, reduced risk of errors but also provides intelligent feature creation explicitly for the fulfillment of financial services for both fungible token and non-fungible token (**NFT**) by exploiting the unique features of the blockchain

Business overview

SMEs' challenges in getting funding

Globally, SMEs face challenges in getting financing. The problem is even more so in emerging markets such as Southeast Asia, as a lack of banking infrastructure makes it harder for SMEs to access credits from the banks.

Some features of the BHoldus blockchain network

- BHoldus token (BHO) will be a digital asset that stores values, generates yield (interest), and provides access to an open lending network.

- The digital asset BHO (BHoldus) represents its owner's voting rights over economic factors such as inflation and deflation levels. A blockchain network protocol named Black Hole will determine the voting rights of BHO token owners based on different metrics. Black Hole will create values for BHO token owners via various incentivizing systems and business models.

- BHoldus pools - BHoldus provides a seamless user interface that allows anyone to deposit their digital assets to earn yields. Through the BHoldus staking algorithm, investors will have the privilege and priority in capturing attractive yields and participate in the BHoldus ecosystem, which interconnects with other blockchain networks in the market such as Binance, Ethereum, Bitcoin, Polkadot, amongst others.

- High speed and low fees - BHoldus will provide native stable coins in BHoldus Network for low transaction fees and fast settlement.

More on BHoldus financial infrastructure

What is the BHoldus blockchain network?

BHoldus is interoperable, cross chained with various digital asset economies with direct integration with the other Defi networks such as Binance, Ethereum, and Polkadot. In addition, BHoldus also acts

as a hybrid model to accelerate traditional finance, allowing network players to record their real-world assets on-chain with NFTs.

What is NFT?

NFTs are unique, non-replicable cryptographic tokens that exist on a blockchain. NFTs can represent real-world tangible assets such as artworks or real estate, allowing them to be bought, sold, and traded more efficiently while reducing the probability of fraud. NFTs can also be used to represent personal identities, property rights, amongst others.

How NFTs work on BHoldus network

BHoldus uses NFTs to represent real-world assets and evidence for creditworthiness, such as audited financial statements, invoices, or audited mortgages.
Issuing NFTs to represent these assets and information helps open doors for individuals and businesses to access new financing channels on DeFi space.

BHoldus Chain & Its Smart contract

BHoldus allows on-chain borrowing against various collateralized assets managed by trustless smart contracts. BHoldus will gradually become a fully decentralized financial exchange protocol interoperable with multiple blockchain networks in the market.
Smart contracts will help

- Maintain identities in a similar format to the BNB or DOT standard,
- Anchor state commitments
- Minting NFTs from off-chain BHoldus documents

BHoldus Token (BHO)

1. The intrinsic value of the BHO token

BHoldus token (BHO) incentivizes desired behaviors on the BHoldus interoperable blockchain network. Owning BHO tokens provides users a stake in the BHoldus network. Participants use BHO to pay for transaction fees, stake as validators, and participate in BHoldus on-chain governance. In addition, the BHO token helps ensure chain security by rewarding BHO holders in the Parachain loan offering and by distributing a block reward to Validators and Nominators.

As the ecosystem of BHoldus token owners grows, the BHO token will capture the increasing value provided to token owners via each of its utilities.

The total supply of the BHO tokens will be minted at the launch of the main net and kept in the BHO reserve Pool for distribution amongst investors, contributors, and participants to the network.

2. The benefit of owning and using BHO token

Users can benefit from the BHO token by

- Staking BHO tokens to earn attractive Yields
- Borrowing or paying back loans via BHO tokens
- Submitting & voting on different programs that help grow the BHO Ecosystem.
- Participating in the Black Hole decentralized pools for lending, staking, borrowing, swapping
- Referring new users to grow the community
- Receiving grants by participating in the BHO governance structure
- Access staking reward, higher interest rates, loyalty programs, amongst others.

Community Driven Organization

BHoldus DAO

A BHoldus Decentralised Autonomous Organization (BHoldus DAO) is a blockchain-based organization that enables individuals and businesses to coordinate and govern themselves via a set of self-executing rules deployed on a public blockchain. Members of BHoldus DAOs use BHO tokens to vote on the rules that govern the decentralized system.

General Foundation and Expertise Councils

The overall BHoldus network governance operates via a general foundation and expertise councils. Expertise councils would govern specific areas of the network. For example, the Financial Council would handle the financial and compliance management of the network, and the BHoldus Council would oversee the BHoldus protocol.

The BHoldus Council or public BHO token owners can raise requests. In a decentralized way, the community will make decisions to approve or reject them through a predetermined process and framework.

Any network update would be under the governance of the general foundation. BHO token holders are eligible to govern BHoldus core technologies requests through the BHoldus council. The general foundation would have oversight of the BHoldus council to ensure the efficiency and productivity of

the BHoldus blockchain network. BHO token owners can participate in voting for or against BHoldus protocol-related request programs.

BHoldus's governance responsibilities are as follows:

- Determine which digital assets should be listed in centralized or decentralized exchanges
- Execute emergency shutdown of BHoldus Orderbook and oversee its actions
- Oversees the expenditure of BHoldus Treasury Funds to grow the ecosystem
- Fund innovative projects built on top of the BHoldus blockchain network.
- Manage inflation of BHoldus (BHO) token
- Advance economic models
- Advance Black Hole Pool reserve and its infrastructure
- Update staking strategies and implementation.
- Amongst others

Staking

Strategies and execution

Besides staking BHO tokens for validating or nominating within the BHoldus network, the BHoldus Protocol would also aggregate the supply of each user and allow them to participate in staking collectively. For example, BNBs supplied to the staking pool are represented as BHO_BNB account balance, which entitles the owner to an increased quantity of underlying assets. The BNBs being used to stake would earn block reward and be subject to slashing (punishment) in cases of misbehavior (e.g., when a validator fails to maintain required uptime).

The balance of the two is the profit/loss that would increase/decrease the amount of the underlying asset of BHO-BNB. Hence, earning a staking reward is as simple as holding an BHO_BNB token, while BHO-BNB is cross-chain capable and can be used to participate in other network activities.

Non-custodial and custodial staking services

BHoldus plans to support non-custodial staking in the near-to-mid-term and add custodial staking-as-a-service for other PoS assets, such as ETH 2.0. The rules will vary by the chain and by the assets. The

BHO governance can allow for voting to determine the staking fee structure for specific DPoS assets.

Understand the Black Hole Pool

1. Black Hole Pool overview

Black Hole Pool is an open, smart contract-based infrastructure of different digital asset pools bringing together Assets Originators and Defi investors who seek to utilize the full potential of Decentralised Finance. Black Hole will become a fully decentralized financing protocol that interoperates with different blockchains and leverages various funding sources. Through multiple Black Hole Pools, Businesses or Asset Originators will have opportunities to access DeFi financing using real-world assets such as audited invoices, mortgages, audited financial statements, et cetera. They do this by tokenizing their financial assets into Non-Fungible Tokens (NFTs) and use these NFTs as collateral in their Black Hole Pool.

2. The functionality of the Black Hole Pools

For every Black Hole Pool, Defi investors can invest with different digital assets in the form of tokens such as BHO, BTC, BNB, ETH, DOT, and the other valuable crypto assets accepted by the governance structure.

Every Asset Originator has an opportunity to establish a Black Hole Pool for their assets.

Black Hole Pools are "revolving" or open-ended pools where Defi investors can join and leave at any time, and the provided funds can be on-going deployed by the Asset Originator unless the investors redeem it.

3. Revolving Black Hole pools - Continuous liquidity

Revolving Black Hole Pool contains different valuable digital assets that allow Defi Investors to invest/redeem independently at any time. A decentralized algorithm under the BHoldus blockchain network matches investments and redemptions. It ensures that certain requirements are considered, such as redemption requests and the pool's risk metrics. Assets Originators should have regular liquidity resources while Defi investors can have the flexibility to invest and redeem.

4. Investing in Black Hole Pool

Investors are required to complete their KYC process. To invest, BHO investors lock their investments in different digital assets such as BTC, ETH, USDT, et cetera, into Black Hole Pools during an Epoch. Investment and Redemptions automatically execute at the end of an epoch with advance notice to the investors. A decentralized algorithm calculates the rules for investment and redemptions, ensuring the pool's proper risk control.

Lending

- In Phase 1, we'll build cross-chain bridges to existing open-source DeFi lending protocols to offer our users access to lending interests.

- In Phase 2, we'll use third-party lending providers to provide access to high-interest savings options and stable coin loans. This platform-agnostic approach allows us to cooperate with industry leaders across multiple blockchains and protocols, giving users access to a full suite of services within a single, easy-to-use interface. We will take a reasonable spread on these integrated products.

- In Phase 3, we'll be developing a proprietary lending algorithm & stablecoin system, but with cross-chain collateralized assets rather than single-chain ones. Using tokenized derivatives, such as BHO_BNB, as collateral, we'll allow users to generate staking rewards even while taking out stablecoin loans.

Black Hole Stablecoin

Black Hole USD is the native stablecoin of the BHoldus infrastructure. Similar to DAI stablecoin in MakerDAO, Black Hole USD is generated through Collateralized Debt positions (CDPs) in an over collateralized manner and pegged 1:1 with US Dollar. While DAI uses ERC-20 Ethereum-based assets to back it, Black Hole USD can use various crypto currencies supported by the BHoldus ecosystem and its cross-chain network. It may be BNB, ETH, DOT, BTC, ADA, or ERC-20 based tokens.

Tokenizing and financing a real-world asset or a digital asset

The Asset Originator can utilize digital asset funding provided by Defi investors. To facilitate this, the user locks an NFT representing a "Real World Asset" into a set of smart contracts as collateral. The NFT is minted based on audited documents created and shared via the BHO BHoldus blockchain network. Auditing providers will determine the structure of these financing offers through an on-chain "Pricing Oracles." Upon repayment, the NFT is unlocked and transferred back into the Asset Originator's wallet.

Custody

As BHoldus will be dealing with hundreds of millions of dollars worth of digital assets, the security of our users' assets is the most crucial factor. BHoldus DAO will have an opportunity to integrate with both non-custodial and custodial wallet's existing solutions depending on the specific service offerings. We will select the most prominent digital asset firms such as Coinbase Custody or similar enterprise-grade security solutions to provide the most robust encryption technology solution. In the long term, BHoldus DAO will focus on delivering non-custodial services for the initial staking business line through

Delegated Proof of Stake (DPOS) token. This significantly reduces the risk as users' tokens remain at all times in the users' custody.

Our community

We use several growing social media platforms to communicate and collaborate with the public and core team members. The channels include but not limited to

- Telegram Chat
- Telegram Announcements
- Forum
- Discord
- Slack
- Facebook
- Twitter
- Newsletter

You can take a more active role in the BHoldus community by

- Invest in BHoldus
- Originate Assets
- Hold BHoldus tokens (BHO)
- Become a validator
- Get funded for a project

Technological background

A. Blockchain

A blockchain is a decentralized ledger that records the provenance of digital assets across a peer-to-peer network. It is ideal for the delivery of such information since it provides immediate, shared, and completely transparent information that can only be accessed by permitted network members on a ledger. Participants can confirm transactions without a central clearing authority.

A blockchain includes the following key elements:

- **Distributed ledger technology**: The distributed ledger and its immutable transaction records are available to all network participants. Transactions are recorded only once when using a shared ledger, helping eliminate the duplication of effort that is common in traditional business networks.

- **Immutable records**: After recorded in a shared ledger, the transaction cannot be modified or tampered by any participant. If a transaction record includes an error, it must be reversed by adding a new transaction, and both transactions will be visible.

- **Smart contracts**: A set of rules, known as a smart contract, is stored on the blockchain to speed up transactions. When a set of predefined conditions are fulfilled, the agreements are automatically executed and the involved parties can immediately see the outcome, without any intermediary's involvement or delay. Additionally, when certain conditions are met, subsequent actions are automatically triggered which make the entire workflow automated.

B. Decentralized Exchanges (DEXs)

With centralized exchanges (CEXs), people can deposit their money (i.e., fiat or cryptocurrency). However, when they deposit their crypto, they also give up the control over it. Not in terms of usability, as people can still trade or withdraw it, but from a technical perspective: they can no longer do anything else on the blockchain. They don't have access to their private keys to the funds, so they must ask the exchange to sign the transactions on their behalf when making the withdrawals. Transactions do not occur on-chains when people are trading – instead, the exchange allocates balances to them in its own database. This comes at the cost of independence: they have to trust the exchanges. In this way, people face certain counterparty risks (e.g., crashing the system by hackers).

In theory, any peer-to-peer swapping could be considered as a decentralized trade. With Decentralized Exchanges (**DEXs**), transactions are executed on-chain (with smart contracts). You do not sacrifice custody of their funds at any point and do not need to trust the exchange.

- **On-chain Transactions**: Transactions will be considered valid if the transactions on the distributed public ledger are reflected in the blockchain. This requires authentication and validation by a certain number of participants of a transaction. The different details of a transaction are recorded on the block and distributed to the entire blockchain making the transaction irreversible because it cannot be changed. On-chain transactions take longer due to the various steps that have to happen before a transaction is considered successful. Furthermore, the potentially high cost of a transaction may deter some of the members in the network.

- **Off-chain Transactions**: These are transactions that deal with values outside of the blockchain and also use a payment mechanism based on the code. The participant purchases redeemable codes here to exchange them with the crypto assets. They then pass the codes to a third party who redeems them. Depending on the service provider of a code, the third party may choose to redeem the codes in the same crypto assets or others. In comparison to on-chain transactions that may have significant delays depending on the number of transactions waiting to happen on the same network as well as the network load and the transactions on the queue not confirmed, off-chain transactions are performed instantly.

- **Automated Market Makers** (**AMMs**): By using liquidity pools rather than a traditional market of buyers and sellers, AMMs allow digital assets to be traded in a permissionless and automatic way. AMM users provide liquidity pools with crypto tokens, the prices are determined by a constant mathematical formula. Liquidity pools can be optimized for various purposes and are an important tool of DeFi.

Here are the comparisons between DEXs and CEXs

	CEXs	DEXs
KYC/AML (Know Your Customer and Anti-Money Laundering)	Yes	No
No counterparty risk	No	Yes
Unlisted tokens	No	Yes

Usability	• Friendly • Real-time trade • More forgiving experience (e.g., forget your password, it is simple to reset)	• Not nearly as user-friendly as traditional exchanges • Need to custodial cryptocurrency wallets • Losing seed phrase or private key means that you also lose control of your wallet and your money.
Trading volumes and liquidity	• Greater liquidity: easy to buy or sell assets at a reasonable price	• Still relatively niche: not always supply or demand for the crypto assets wishing to trade. • Assets might not be able to trade if no trading pair is found.
Fees	Fixed	Not always higher, but when congested, the network charges hundreds of dollars for a single transaction

Theoretically, DEXs are ideal exchanges. All rights and ownership are delegated to the community, and all processes are entirely carried out by smart contracts. Furthermore, their non-custodial aspect provides a safe space for fervorous crypto enthusiasts.

In a perfect world, DEXs will be the only kinds of trading platforms available in not only crypto but also other markets. However, their limitations prevent them from becoming a dominant force.

C. Web3.0 and Polkadot

Web3.0 will bring us a more equitable internet by allowing the individual to be a sovereign. Web3.0's decentralized blockchain protocol will enable everyone's control over all their personal values in the digital world, such as their data, identity, and assets. It eclipses an exploitative and unjust web, where giant, centralized repositories own and profit from their information. Finally, it will bring a truly transparent and credible internet economic model to the world.

Polkadot was founded by Gavin Wood, co-founder and former CTO of Ethereum, to realize the vision of Web3.0 and solve the current problem of "data islands" in the blockchain. It is dedicated to developing a network protocol similar to the Internet TCP/IP protocol by defining and developing a set of fragmented

multi-chain structures of parallel chains and relay chains. Allow all blockchains connected to this architecture to better complete the information interaction between each other, and finally, realize the "all chain interconnection."

D. Substrate

Polkadot has revolutionized the Substrate development framework for blockchain developers worldwide. Instead of wasting time and effort, all teams create a new blockchain that must implement the entire network and consensus code from scratch (not to mention the cryptographers, security researchers, etc); the Substrate framework modularized the basic low-layer design of the blockchain, allowing developers to call it with one click, reducing the original complicated workload.

The blockchain gains unprecedented features thanks to the Substrate framework:

- Scalability: An isolated blockchain can only handle a limited amount of traffic. But with Substrate, it supports multiple blockchains via a parachain/parathread mechanism, allowing transactions to be processed efficiently and in parallel.

- Interoperability: The interoperability design and compatibility between chains allow different blockchains and applications to share information and functions.

- For-free Upgrade: It can be upgraded without time consuming and split hard forks. New features can be added without transforming the network completely.

- Specialization: Each parachain can be customized based on particular use cases or applications.

- Autonomy: Polkadot's community can manage its network according to its own wishes, and it has transparent rights and interests in the governance of the entire Polkadot network in the future. The team can customize and optimize its governance to meet specific requirements, experiment with new ideas, or deploy pre-built modules for faster deployment.

Our technology - The proposed solution

A. System architecture

1. Digital assets

Besides the native token (BHO), BHoldus blockchain can issue new assets on-demand to facilitate different business use cases and purposes. BHoldus plans to build not only a solid but also flexible asset system with the following capabilities:

- New assets issuance (minting) can be done in both permissioned and permissionless manners
- Assets can be easily moved between holders
- System administrators (special privileged accounts) have the ability to freeze account balances as well as mint and burn (destroy) assets
- And many more to be added in the future

The above features are supported natively and out-of-the-box throughout the BHoldus ecosystem.

2. Accounts

Users interact with the BHoldus chain using their blockchain key pairs. Within BHoldus, an account is identified by the public key and authorized by the corresponding private key.

Public key is the address on-chain, which is applied SS58 address encoding format [(1)] (e.g, 5Gv8YYFu8H1btvmrJy9FjjAWfb99wrhV3uhPFoNEr918utyR). A balance on each address can be sent to any other address.

Users can sign Transaction Requests using their private key and submit them to the BHoldus chain using Substrate Extrinsics [(2)].

BHoldus plans to build a user hot wallet that can keep users' key pairs so that those key pairs can be used for activity authorization within the BHoldus chain. Since the wallet provided is a hot wallet, the keys are kept in an online device which puts the security at higher risk compared to cold wallets. A typical hot wallet would generate a new deposit address for each new user by generating a new key pair. However, this approach seems to make managing those keys tedious in the long run. BHoldus chooses to follow another approach introduced by Parity to build a more scalable and secure wallet [(3)]. The hot wallet comprised of 3 main parts:

- **Multisig Accounts:** in some other blockchain networks, multisig works in a way that multiple keys must be used to sign a single transaction off-chain before submitting the transaction on-chain. BHoldus multisig accounts follow a different approach: an account ID which is used to uniquely identify an account (it can either be the public key corresponding to a private key or simply a 32-byte number) is generated based on a pre-processed set of information including the individual accounts involved in the multisig and the requisite threshold needed to dispatch from the generated account.

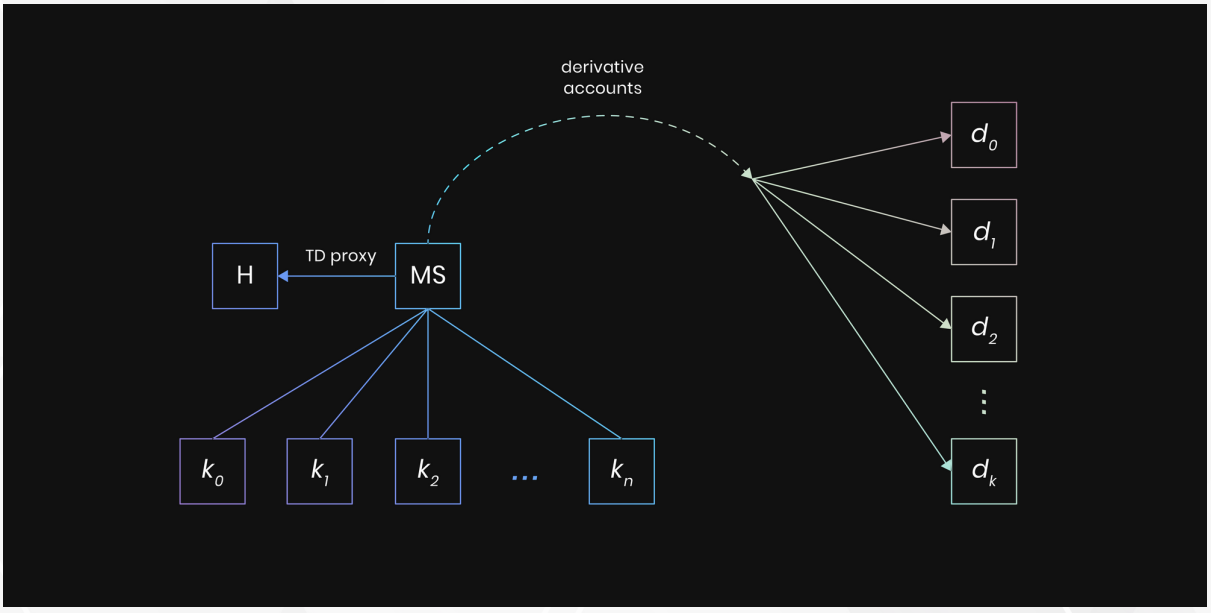
[(1)] https://github.com/paritytech/substrate/wiki/External-Address-Format-(SS58)
[(2)] https://substrate.dev/docs/en/knowledgebase/learn-substrate/extrinsics
[(3)] https://www.parity.io/building-a-hot-wallet-with-substrate-primitives

The created account intuitively does not have a corresponding private key. So in order to authorize a transaction originating from the newly created account, the members of the multisig "must mutually agree" on the function that the multisig account will make. By leveraging hash functions, such process follows a manner where only one account needs to submit a transaction on-chain with the actual function while other members submit the hash of that function without submitting the same transaction again. By doing this, the space occupied on the chain could significantly reduce.

- **Proxy Accounts:** by introducing a new concept, proxy account, multisig address now has the ability to delegate authority to another account. This means, a proxy account can give some privileges from one account to another to make function calls on its behalf. The given authorities can be specific and tailored depending on the use cases. The functions dispatched are then marked with origin being the proxied account after the chain verifies that the proxy has the right to make the function calls. To achieve a higher security level, a time delay is added to the proxy where the actual function call only happens after the time delay is over. Prior to the delay, the proxied account's owner can optionally reject the function call by submitting a transaction before the time delay is over.

- **Derivative Accounts:** each account can have its own set of derivative accounts. Again, by leveraging hash functions, a derivative account ID can be created based on the combination of calling account ID, derivative account index and some other special information such as derivative prefix. Deposit address for each new user can then be generated for effective and clear accounting. To access the funds of these accounts, proxy accounts come into play.

The following image shows the BHoldus hot wallet built up from the above listed components:



3. Governance

BHoldus aims to build a decentralized network that will be governed by a widely distributed set of token holders, including BHoldus core team, users, collators, and other contributors. Our ecosystem will facilitate the engagement of these stakeholders throughout the launching and developing phases of the network. Any network upgrade decision should be administered by active token holders and collators.

4. Consensus

Consensus protocol is an essential part of every blockchain network. Consensus protocol allows every participant in the distributed network to coordinate and agree on the state of the system. With a robust consensus mechanism, one network can achieve overall system reliability in the presence of a number of faulty actors. Consensus protocol can be broken down into two main parts: Block authoring and Finality.

Disclaimer: Most people often mistake Proof of Work (**PoW**), Proof of Stake (**PoS**) as a shorthand to refer to the consensus mechanism but they are actually just a part of the complete consensus protocol. For example, PoW is the method for agreeing on a block authority and part of the fuller Nakamoto consensus that also encompasses a chain selection algorithm (longest chain rule in Bitcoin). Similarly, PoS is a set of rules for selecting the validator set and does not specify a chain selection rule or how a chain might reach finality.

In the PoS blockchain network, participants holding native tokens (stakeholders) of the network can become maintainers of the network called validators forming a validator set. The chance users are selected is proportional to the number of tokens they hold. PoS have several benefits over traditional PoW:

- **Less energy consumption:** In a PoW system, all participants compete with each other to solve the puzzle but only winners are allowed to produce a block and receive the reward. While in a PoS network, only predetermined validators need to produce blocks at a time.

- **Lower risk of network attack in the long term:** In a PoW system, when there is little or no reward for miners, the network is highly vulnerable to 51% attack since users don't have incentives to become miners. While in a PoS system, the attackers need to hold 51% stake of the network which is expensive. Also, attackers will be disadvantageous in attacking the network where they hold a large stake of it since they also attack themselves.

- **Higher transaction throughput:** With PoS systems, since there is no puzzle to solve, blocks are produced much faster than PoW networks.

At BHoldus, we use an extension of PoS called Nominated Proof of Stake (NPoS).

In NPoS, the following roles are highlighted:

- **Nominators:** Stakeholders of network
- **Validators:** A set of participants responsible for maintaining the network and nominated by Nominators
- We decide to support NPoS instead of PoS because of following improvements:
- **Higher security:** Since validators are not selected proportionally to the amount of stake they hold and more participants are involved in network governance, there is less chance for attackers to act.
- **Higher performance:** Too many validators has a side effect of underperformance, since the network cost of gossipping can be overwhelmed (Gossipping is the communication between nodes in the network. The network cost of this includes the time and data size. The more nodes the more time and data size it takes to deliver to all the nodes). The NPoS system has the number of validators bound resulting in higher network performance.

While some blockchains couple the block production with finality, i.e to produce block N+1, block N must be finalized, BHoldus uses Hybrid Consensus. Hybrid consensus separates finality gadget from block authoring mechanism.
Hybrid consensus has both the benefits of:

- **Probabilistic finality of Block Authoring:** Ability to always produce new blocks
- **Provable finality of Finality Gadget:** Having a universal agreement on canonical chain with no chance for reversion

By combining these mechanisms, BHoldus allows slower universal finality to happen while high block production, high transaction throughput is guaranteed.

BHoldus uses **BABE** (Blind Assignment for Blockchain Extension) as Block Authoring Protocol and **GRANDPA** (GHOST-based Recursive ANcestor Deriving Prefix Agreement) as Finality Gadget.

5. Staking

Staking is a process of locking users' funds for specific purposes. At BHoldus, we currently support staking for governance of the network such as nominating or becoming validators.

Basically, an account in a blockchain network comprises a private key and a public key derived from the private key, or shorthand, a key pair (keys). In Staking, BHoldus supports various types of keys to minimize the security risks for users:

- Account Keys: Their purpose is to manage funds

    ⌑ **Stash Account Keys**: A Stash Account is a cold wallet, whose private key is stored safely and entirely offline on a hardware device. This is where users can safely store a large amount of funds. Think of it as "Saving Bank Accounts"

    ⌑ **Controller Account Keys**: A Controller Account is a semi hot wallet, whose private key is stored in a device connected to the internet. Controller Keys are usually used to interact with the network. In the context of Staking, Controller keys signal non-spending decisions on behalf of Stash Keys. Only small amount of funds should be allocated to Controllers Keys to pay transaction fees

- Session Keys: Used in signing consensus messages between validators. To create session keys, controller keys must sign generated session keys to create a certificate which is published to the network. Therefore, Session Keys act as a link between users and their validator nodes.

Disclaimer: Account Keys and Session Keys actually use the same cryptography techniques. They are differently classified based on their specific uses.

In order to participate in network maintenance, a user must go through a process of bonding. In the bonding process, the user's stash keys are paired with the user's controller keys and become a staker. The purpose of this process is to protect users from revealing their Stash Keys where large funds are stored and use Controller Keys to interact with the network instead. After becoming a staker, users can stake their funds to nominate or to become a validator. In return, BHoldus will reward validators and nominators with native tokens for correctly playing their roles and punish them when malicious behavior is detected.

Slashing is reducing stash accounts funds due to their invalid behavior when maintaining a network as a punishment. Controller Keys can't spend funds from Stash Keys but attackers can leverage it and open a slashing attack since Controller Keys are used in most Staking operations. Therefore, it is recommended for users to keep Controller Keys as secure as possible and rotate it frequently.

6. Smart Contract

In general, smart contracts are simply a collection of code and data stored in the blockchain that run when certain conditions are met. They simulate real world contracts where a set of rules and actions that

have been mutually agreed between parties are included and guaranteed to execute when predefined conditions are fulfilled and verified by the blockchain. Smart contracts have the advantages of automated execution without any intermediary's involvement and the involved parties can immediately see the outcomes without any delay. Once smart contracts are completely executed, permanent changes are made to the blockchain state and thus makes all transactions happening on the blockchain irreversible and transparent. Records of smart contracts are stored in a distributed and decentralized blockchain network where the contracts' information and results are shared across participants of the network. Given those characteristics, modern blockchain smart contracts have benefits of speed, efficiency, accuracy, trust and transparency while saving significant time and costs involved.

BHoldus blockchain has built-in, performance efficient runtime smart contracts thanks to the powerful and highly customizable Substrate framework. BHoldus smart contracts run directly in its blockchain to serve specific business logics and purposes.

In addition, community blockchain players and developers can also build smart contracts on top of BHoldus blockchain. Since BHoldus is built using Substrate and Substrate supports WebAssembly smart contracts, any language that can compile to Wasm can be used to write smart contracts.

ink! which is a Rust-based embedded domain-specific language provided by Parity can be used to build Wasm smart contracts. By being built based on Rust, a programming language that has gained significant popularity and continues to mature over the past few years, ink! has benefits of type safety, memory safety, small binaries, protection against underflow/overflow and many other good characteristics and supports available from Rust ecosystem. Furthermore, as Rust continues to grow, ink! developers and users can automatically gain access to new updates for free.

Contracts written by community developers and users are put under some essential safeguards to prevent malicious, bad actors as well as inexperienced developers. The followings are some safeguard examples:

- **Fees**: fees are charged upon usage of computer resources such as memory and storage to prevent bad behaviors and uncontrolled implementations.

- **Sandbox**: the contracts only have the ability to modify its own state, but not other contracts as well as the blockchain's storage. Besides, to provide additional safety to the blockchain state, safeguards support revertible transactions when they fail by rolling back any state changes that have not completed successfully.

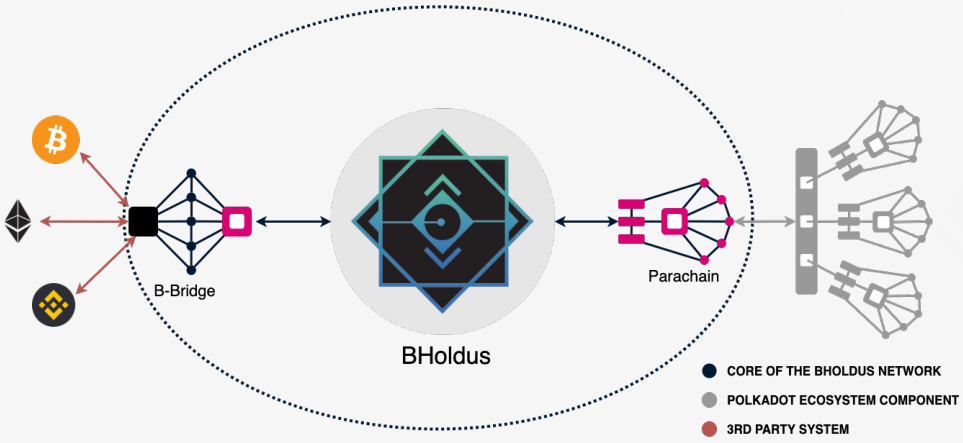
- **State rent**: a contract is charged for using space on the blockchain. This prevents the users from taking advantage of free storage on the blockchain.

Since BHoldus smart contracts run in the runtime of the blockchain itself, it intuitively has better performance and more flexible customizability compared to contracts written by the community, which run in the layer above the runtime and have extra safeguard overheads.

Disclaimer: there are clear different sets of business logics and use cases that can only be solved by only one of the above two approaches or by either of them. Depending on the requirements, scalability and many other aspects, a suitable approach will be chosen. The following table can give a brief overview on which approach should be used on different scenarios:

Built-in, runtime logics	Smart contract	Either
• Business-use case-tailored fee tokens • Decentralized Exchange (DEX) • Stable coins	• Multisig user wallet	• dApp ⌑ Small scale (smart contract) ⌑ Large scale (runtime) • Decentralized Autonomous Organizations (DAO) ⌑ Community driven (smart contract) ⌑ Protocol driven (runtime) • Treasury ⌑ Community driven (smart contract) ⌑ Protocol driven (runtime)

7. Cross chain



Cross-chain communication is communication between a network and another network through messages (events). There are several ways to enable cross-chain communication

a. Bridge

One approach to enable cross-chain communication is through a bridge.

One-way communication is communication that a source network (source chain) sends messages (events) to a target network (target chain). BHoldus tackles two-way communication by switching the roles of source chain and target chain and applying one-way communication

BHoldus uses Substrate Framework to build our blockchain network and also our bridge, therefore, any Substrate-based cross-chain integration with BHoldus should be seamless. However, this doesn't mean BHoldus only limits bridging to Substrate-based networks, any integration with other blockchain technologies like Bitcoin, Ethereum, Binance Smart Chain also works in the same manner.

Unlike communication between centralized systems where trust is established, a bridge between distributed networks must be a trustless bridge. Trustless bridge must come up with a consensus protocol for events to ensure the target chain receives events that really happened on the source chain, in other words, the source chain must give the target chain a Proof of Event to verify.

Our bridge is composed of these layers:

- Trust layer: A layer where consensus protocol on events takes place. Specifically, we have a pallet for target chain to verify GRANDPA finality on source chain (BHoldus) and a Relayer sitting in the middle of two chains and act as a messenger forwarding finality synchronization events.
- Message layer: This layer is built on top of the Trust layer and handles message queueing, delivery

and doesn't care about specific message format. BHoldus currently supports both sequential and parallel message delivery and acknowledgement

- Dispatch layer: This layer is built on top of the Message layer and its job is to decode the message into expected format and dispatch a side effect corresponding to the decoded message. Usually, the message is decoded into the extrinsic calls of target chain

- Application layer: This layer is built on top of the Dispatch layer. All specialized business logic is added in this layer. This layer helps to hide all the complexity of lower layers and streamline the application development process.

b. Parachain

Polkadot's cross-chain composability allows any type of data or asset to be sent between parachains. Polkadot's parachain model was designed with the belief that the internet of the future will have many different types of blockchains working together.

For this reason, Polkadot places no criteria on the design of the parachain other than it must be an application-specific data structure (usually in the form of a blockchain) that is globally coherent and validatable by the validators of the Relay Chain (Polkadot validators). Polkadot's cross-chain composability also has the flexibility meaning that each parachain can have its own design, token and governance process, optimized for its specific use case(s).

The name "parachain" derives from the concept of parallelized chains that run parallel to the Relay Chain. Thanks to their parallel and flexible nature, they are able to parallelize transaction processing so as to achieve scalability of the system.

Parachains are maintained by a network maintainer known as a collator whose role is to maintain a full-node of the parachain, retaining all necessary information of the parachain, and producing new block candidates to pass to the Relay Chain validators for verification and inclusion in the shared state of Polkadot.

Polkadot's cross-chain composability allows communities to have full control and sovereignty over their own blockchain, while being able to engage in free trade with other parachains and external networks. Therefore, users now can do the exchange of not only tokens, but also any type of data, including smart contracts calls, verifiable credentials, and off-chain information from oracles such as stock market price feeds.

Because Polkadot only supports a limited number of parachains, currently estimated to be about 100. In order to run as a parachain on Polkadot, Beholdus is planning to win a parachain slot auction to lease a slot on the Relay Chain for a minimum of six months to a maximum of two years.

c. Parathread

Parathreads are an idea for parachains to temporarily participate in Polkadot security without the need to lease a dedicated parachain slot, thereby also known as pay-as-you-go Parachains.

By lowering the barrier to gaining the benefits of shared security and connectivity, Polkadot is now even more accessible to projects that may not have the capital to secure a dedicated parachain slot.

Although dedicated parachain slots offer high throughput, it requires a large bond for up to two years, which also means the capital to set aside upwards of 20,000 DOTs for two years. With the minimal bond of only 50-100 DOTs, parathreads allow chains to submit a block to the relay chain whenever they have a full batch of transactions, while reaping the full security and connectivity benefits.

In particular, parathreads are ideal for three types of applications:

- Applications seeking an on-ramp to Polkadot
- Applications worried about losing parachain slots, and
- Applications that have more reads than writes.

Moreover, Polkadot allows switching between being parachains and parathreads effortlessly depending on the needs as well as the capabilities of maintaining a parachain slot. Therefore, parathread seems to be an appropriate choice in BHoldus' early stage.

B. Economic model

1. BHO Token:

BHO is the native token of the BHoldus ecosystem. The main features of the BHO tokens are:

- **Reward for farming**: There will be many pools for farming like other DeFi platforms. The amount of BHO earned by liquidity providers will be proportional to the total amount of liquidity added.
- **Governance**: BHO holders have the rights including voting, proposing referenda, electing council members, et cetera.

- **Operations**: Paying for network transaction fees and supporting the gas metering of smart contract execution.

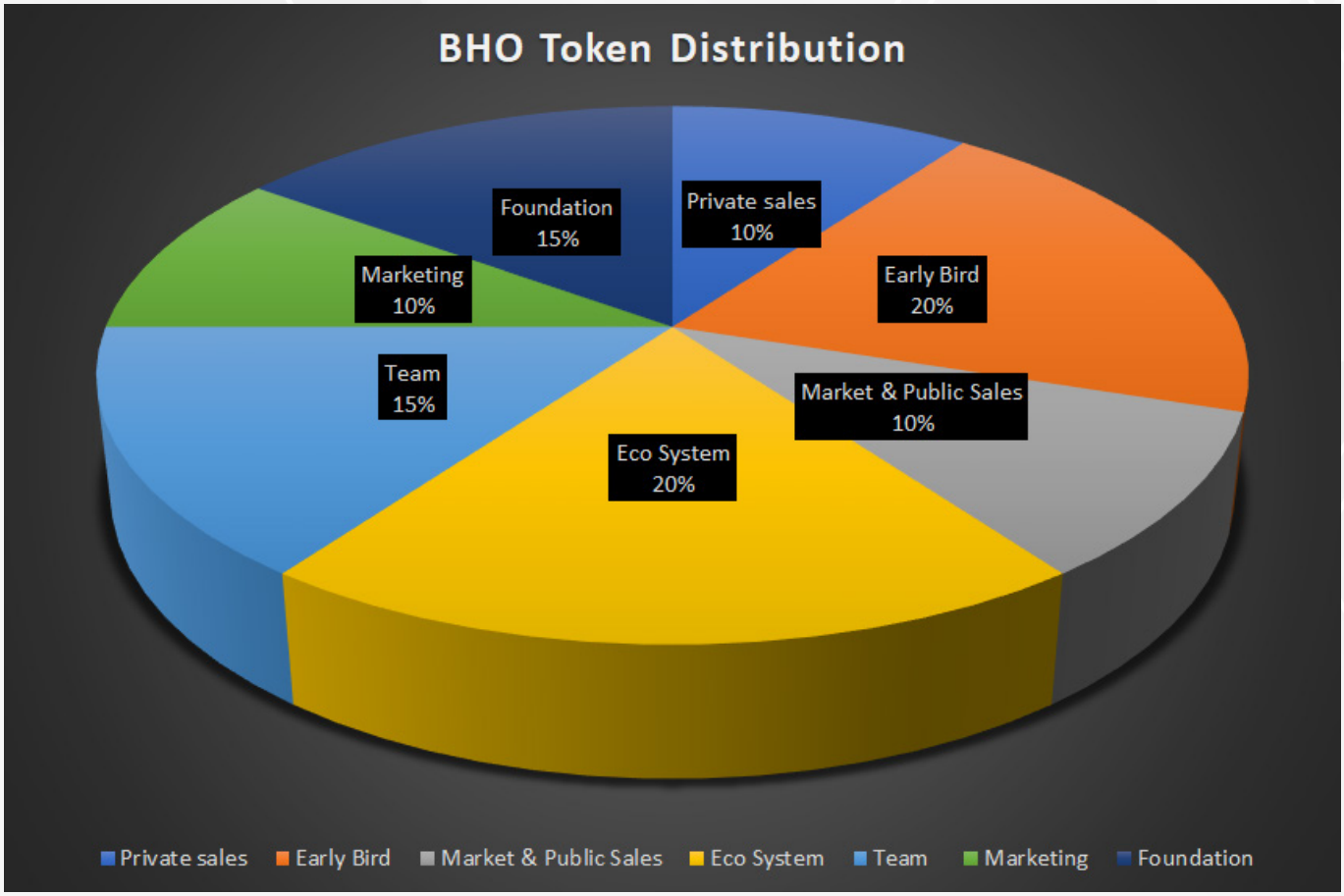
- **Lending fee**: Using BHO for fees to borrow on BHoldus Lending, the user will receive a 50% discount, and the remaining 50% will be burned to support the deflationary token mechanism.

- **Launchpad**: To participate in future projects on BHoldus LaunchPad.

Moreover, BHO will also play a major role in further developing and expanding the BHoldus ecosystem. Marketing strategies, bounties, listing exchanges, and more will all use BHO as rewards and fees.

2. Distribution and release

Total supply will be 10,000,000,000 (10B) BHO. The token allocation details are as follows:



Roadmap & Milestone

Q1 2021	• May: Whitepaper
Q2 2021	• Launch BHoldus Testnet • End of June: ⌗ Launch BHoldus Mainnet ⌗ Publish website
Q3 2021	• July: ⌗ Website supports airdrop ⌗ Mobile Wallets' Integration ⌗ Testnet: Digital Assets • Aug: ⌗ Testnet: Staking native asset ⌗ Listing BHO on decentralized exchanges • Sep: ⌗ Testnet: Cross-chain BSC, ETH ⌗ Security Audit (Round 1) ⌗ Mainnet: Staking native asset ⌗ Listing BHO on top tier centralized exchanges ⌗ Parachain Auction Plan

Q4 2021	• Oct ⌑ Testnet Cross-chain TRX and BTC ⌑ Testnet Staking Synthetic Assets ⌑ Tokenomics & business model audit • Nov: MainNet Cross-chain ETH and BSC • Dec: Tools ⌑ BHoldus mobile app ⌑ Improve Browser Extension
Q1 2022	• Implement DEX (Jan - Mar 2022) • Audit parachain slot & implement parachain (Feb - Mar) • MainNet: ⌑ Cross-chain: BTC (Jan); ETH (Jan); BNB (Jan); TRX (Feb) ⌑ Staking Synthetic Assets (Jan) • Release BHoldus mobile app Testflight & BHoldus extension (Feb)
Q2 2022	• TestNet: ⌑ Launch DEX (May-Apr) ⌑ Parachain Rococo (Apr) ⌑ Implement smart contracts (May-June) ⌑ Launch Stablecoin, Staking Derivative & Multiple Pools (May) • Release BHoldus app on AppStore & publish extension(May)
Q3 2022	• MainNet: ⌑ Launch DEX (July) ⌑ Publish smart contracts (Aug) ⌑ Launch Stablecoin, Staking Derivative & Multiple Pools (July-Sep)

Competitive Analysis

	BHO	BTC	ETH	EOS
Types	Public Chain	Public chain	Public chain	Public chain
Tamper-proof	✓	✓	✓	✓
Auditable	✓	✓	✓	✓
Safe	✓	✓	✓	✓
Consensus Algorithm	NPoS	PoW	PoW	DPoS
Transaction Per Second	Up to 3000	5	16	2000+
Block Creation	3 seconds	10 mins	16 seconds	0.5 second
Provable Finality	✓	✗	✗	✓
Smart Contract authoring language	Ink! , Solidity	Bitcoin script	Solidity	Java C++
Platform Tokens	BHO	BTC	ETH	EOS

Team

Leadership

Ronald Le

Global Business Chief

Tech entrepreneur. Fintech business leader. Founded Hawking, Polariis, Chino-Rino Visual Lab. Singapore.

linkedin.com/in/ronaldle

Nhat Phan

Vietnam CEO

Financial/Investment Advisor. Co-founder VNbot - Capital Management System. Experienced in CryptoCurrency, Social Media, Game Online MMORPG. Vietnam.

linkedin.com/in/NhatPhan

K. N.

Managing partner, Strategy & Operation

Entrepreneur; Edtech leader; Fintech strategist. Experienced in strategy, planning, process innovation. Built highly scalable operations and teams across multiple markets. Singapore.

linkedin.com/in/kelsienguyen

Duong Le

Core Developer

Co-founded Hawking Network, Snr AI engineer, co-founded Guu, MegaDrupal, Polariis. Experienced in building tech products from scratch. USA.

linkedin.com/in/duongld87

Engineering & Design

Nhi Tran

Snr Engineer

5-year experience in Backend development

Singapore

Khoa Nguyen

Engineer

Top 5 CS graduate,

University of Science

Vinh Nguyen
Engineer

Top 5 CS graduate

University of Science

Dung Lam
Engineer

Valedictorian, Computer Science; University of Science

Thomas Nguyen

UI/UX

UI/UX Designer at Etsy

Research Assistant at Parson School of Design. USA

Hai Minh
UI/UX

UI/UX designer

Eco Moblie

Compliance & Internal Control

Toàn Nguyễn

Compliance partner,

Lawyer

Former KPMG

Tho Nguyễn

Finance & Internal Control Partner

Finance manager with 8 years experience in banking and investment.

Master in Finance & Accounting, UK

Community and Marketing Communication

Duong Vi Khoa
Advisor

Vice President of VIRESA,

Microsoft Most Valuable Professional. Over 25 years building IT, Games, tech communities.

Lily Cam
Head of Digital Marketing

10 years of Martech/Digital Transformation. Experienced in Technology, Telco, Media Groups in Vietnam and Asia

Ha Tran
Head of Communication

Entrepreneur. Specialised in Human Behavior & Psychology; Formerly Top50 Amazon Ecommerce Merchant based in Australia

Lan Vo
Vietnam

Larry Nghiem
US

Trang Tran
US

Quang Vu
Vietnam

Advisors

Ramon Tisaire
US Chief Strategy Partner

Extensive startup experience. Fintech connector. UChicago board governor.

linkedin.com/in/ramontisaire/

Becky Vo
Board Advisor

CO SAL4 AP Regional Director

Bosch BT

linkedin.com/in/BeckyVo/

Disclaimers

Licenses and approvals may NOT be obtained in all jurisdictions. Regardless, BHOLDUS DAO intends to operate in full compliance with applicable laws and regulations.

Third-Party Data: This whitepaper contains data and references obtained from third-party sources. While the management believes that the data is accurate and reliable, they have not been subject to independent audit, verification, or analysis by any professional legal, accounting, engineering, or financial advisor. There is no assurance as to the accuracy, reliability, or completeness of the data.
Translations: This whitepaper and related materials are in English. Any translation is for reference purposes only and is not certified by any person. We can make no assurance as to the accuracy and completeness of any translation. If there is any inconsistency between a translation and the English version of this whitepaper, the English version prevails.

Views of BHoldus DAO: The views and opinions expressed in this whitepaper are those of BHoldus DAO. They do not reflect any government's official policy or position, quasi-government, authority, or public body (including but not limited to any regulatory body of any jurisdiction) in any jurisdiction. This whitepaper has not been reviewed by any regulatory authority.

References

1. https://academy.binance.com/en/articles/what-is-a-decentralized-exchange-dex
2. https://www.linkedin.com/pulse/defi-good-small-medium-sized-enterprises-smes-david-shin/?trk=public_profile_article_view
3. https://en.wikipedia.org/wiki/Decentralized_finance
4. https://substrate.dev/docs/en/
5. https://policyreview.info/glossary/DAO