BIT-BANK

PaaS - (Privacy as a Service)

The Bit-Bank Eco-System Whitepaper

"Arise, you have nothing to lose but your barbed wire fences!"

Tim May - The Crypto Anarchy Manifesto (1992)

Abstract

With the changing world and governance over our lives, COVID-19, government mandates and AML/KYC and data privacy and banking restrictions over the ever changing cryptographic landscape of the digital currency markets and our lives we seek to treat the problems.

Swiss designed with privacy at the heart of what we do, privately connecting users via a hybrid third generation ISO20020 blockchain Ecosystem utilising DeFi Web3 Financial Instruments and creating a private and high speed bridge with a CeFi (Centralised) Banking infrastructure.

We offer Privacy based Ecosystem with DeFi trading instruments such as a decentralised exchange where you can access privacy focused stable coins issued by us on the XDC Xin Fin network and our dApp bridges clients to decentralised contracts such as Investments, Lending, Precious Metals Trading, Hedge Fund Investing, Bonds, Staking, Insurance and more.

Our clients can be safe and sound that your data is safe and sound in the Swiss mountain land with the worlds best privacy laws and protections in place, and that we are actually a Non-Bank, as we do not store your coin we are not required to be adhering to transaction reporting and restrictions.

If our clients do want to bridge to the old centralised Banking world and access IBAN and SWIFT Bank Account, Custody Solutions, Debit Cards etc we have partnered with the worlds leading Digital Bank that currently has over 2Billion under management.

To access Centralised Banking services you will have to be a Certified High Net Worth Individual and we do have a restricted countries list.

Bit-Bank is your cryptographic decentralised digital Swiss numbered bank account!

This paper contains a description of the Bit-Bank network protocols and ecosystem, our team has designed the best financial set of technologies and encryption with security and privacy at the core of our principles and focus.

We have taken the most useful of Web3 and blockchain technologies and built our dApp on top of them as we have designed our products to be user friendly, private, and secure without having a single central point of data or vulnerability.

With such a mixture we are very pleased to be presenting to the public the Bit-Bank Ecosystem.

Social Use

The world has gone through great changes and fundamental challenges since the unprecedented Covid-19 attack, whether the governments control on our movements, the gap between the elite and the essential workers, QR Codes and restrictions on cash this has uniquely brought a new challenge for people to be able to live their lives as they once did – peacefully.
Trends like home working and home schooling have forced households to embrace the digital world.

The world has moved into what some are calling the forth industrial revolution, like all in the world there are good forces and bad forces at play. We like to keep ourselves neutral but our love for privacy, security and freedom has presented us with innovational opportunities; on the dark side we have Bankers, Social Media and other Media outlets all trafficking in our data and collaborating with the authorities to bring us under a one world system and control…… although we these we feel really are a problem of the old Web 2.0 System!

Crypto, Web 3.0, DeFi and dApps

Peoples need to keep privacy, security, freedom and control over their finances have led to the incredible creation first of Bitcoin and now of Web 3.0.

Web 3.0 is completely erasing the boundaries between online and offline, the web will become a decluttered, authentic, and immutable record of smart contracts. The ordered chaos created by the small activities of billions of people, is going to make people work better, work faster and work smarter than ever before.

DeFi (Decentralised Finance) offers financial instruments without relying on intermediaries such as brokerages, exchanges, or banks by using smart contracts on a blockchain. dApps use Web3 to build on top of DeFi to create dApps giving the user a friendly interface.

Lack of Privacy on the Blockchain

Blockchains are generally not designed to have any privacy features. Privacy, in this case, means that the sender, receiver and the amount being sent should not be visible to any entity on the blockchain except for those who have a financial interest in the transaction. However, in bitcoin, and most blockchains out there, all the previously mentioned information is visible.

Anyone viewing the blockchain could see the destination addresses of every transaction, the amounts being sent to these addresses, and since every address has only one private-key that it comes from, we know that the owner of that address is the signer of that transaction.

To make things worse; with statistical analysis and machine-learning, addresses can be linked together and it is even possible to find their ultimate owner. Additionally, there are companies that have taken the initiative in providing services of linking addresses and revealing information about the users of a blockchain; an example is Chainanalysis.

It also provides it as a service for governments. This is particularly negative for people who live in countries with oppressive authorities, where this information can be freely used to invade civil rights.

In other words, even though addresses are pseudonymous and do not reveal the owner by name, it is practical to follow the senders and receivers of transactions, up to an exchange, where the user submitted his personal information to follow KYC and AML laws, which will ultimately reveal the owner. Not only that, but this also endangers the state of fungibility of cryptocurrency coins.

Enhanced Security

Public/Private Blockchain

Hybrid interoperable EVM compatible ISO20020 Public and Private blockchain XDC is what we have chosen as the optimal partnership and blockchain for our project.

The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data. Bitcoin has demonstrated in the financial space that trusted, auditable computing is possible using a decentralised network of peers accompanied by a public ledger. In this paper, we describe a decentralised personal data management system that ensures users own and control their data.

We implement a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. Unlike Bitcoin, transactions in our system are not strictly financial – they are used to carry instructions, such as storing, querying and sharing data.

Finally, we discuss possible future extensions to blockchains that could harness them into a well-rounded solution for trusted computing problems in society.

The amount of data in our world is rapidly increasing. According to a recent report, it is estimated that 20% of the world's data has been collected in the past couple of years.

Facebook, the largest online social-network, collected 300 petabytes of personal data since its inception – a hundred times the amount the American Library of Congress has collected in over 200 years. In the Big Data era, data is constantly being collected and analysed, leading to innovation and economic growth.

Companies and organisations use the data they collect to personalise services, optimise the corporate decision making process, predict future trends and more. Today, data is a valuable asset in our economy. While we all reap the benefits of a data-driven society, there is a growing public concern about user privacy. Centralised organisations – both public and private, amass large quantities of personal and sensitive information. Individuals have little or no control over the data that is stored about them and how it is used. In recent years, public media has repeatedly covered controversial incidents related to privacy.

Among the better known examples is the story about government surveillance, and Facebook's large-scale scientific experiment that was apparently conducted without explicitly informing participants.

In recent years, a new class of accountable systems emerged. The first such system was Bitcoin, which allows users to transfer currency (bitcoins) securely without a centralised regulator, using a publicly verifiable open ledger (or blockchain). Since then, other projects such as ours (collectively referred to as Web 3.0) demonstrated how these blockchains can serve other functions requiring trusted computing and audibility.

On Chain Technology

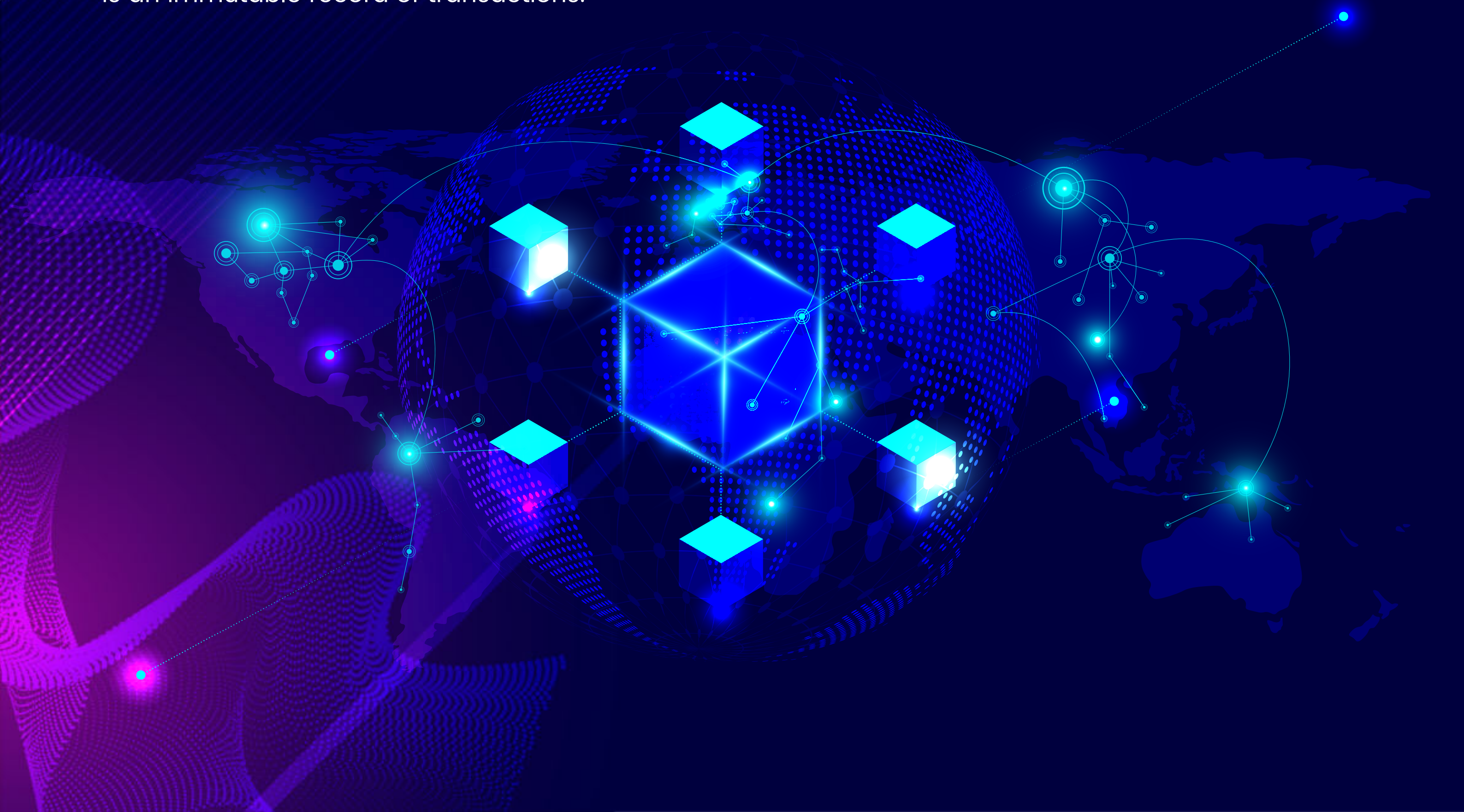
Hybrid Network Architecture - Hybrid Network: Public and Private

The XDC blockchain is built upon the paradigm of consortium blockchains. The architecture differs from conventional private/permission blockchains as well as public blockchains. Built upon the Ethereum codebase, the XDC blockchain also deals with the system state rather than blocks of transactions.

There are two different kinds of networks that can exist within the XDC ecosystem. Firstly, the public network that all constituents are part of and a private/permission network that restricts participation. And secondly, the private network state is maintained in its respective network but a record (hash) of transactions and smart contracts is stored on the public state of the blockchain.

As depicted in Figure 1, various institutions will have different relationships with other participants. The public state of the XDC blockchain is shared by all participating nodes that are owned by different kinds of constituents. Groups of nodes can further form fully permission networks with their own private state that is accessible only to authorised members.

For instance let us assume that a private marketplace for goods and services is set up in Network 1. The specifics of the trade between parties is not accessible to Network 2. But the record of individual trades are stored as hashes on the public state that is shared by all such that even in the private network there is an immutable record of transactions.



The Bit-Bank XDC & J.P Morgan Quorum Forking

The XDC blockchain is built upon Quorum, a private/permissioned blockchain developed by J.P. Morgan. Quorum has been developed as a layer upon the Go implementation of the Ethereum protocol. There are few but significant changes made to the protocol. The consensus mechanism has been entirely reworked, replacing proof of work with a consensus mechanism called QuorumChain. This new consensus mechanism allows for new blocks be created in a two-step process. In the first step, the transactions to be included in the new block are voted upon by all participating nodes. In the second step, one node is selected as the leader or block maker randomly. The block maker node then creates the new block.

The XDC blockchain is forked from Quorum. There are a number of reasons behind this decision. Firstly, the powerful smart contract functionality that exists in the Ethereum protocol is easily accessible through in Quorum. Secondly, the consensus mechanism is implemented as a smart contract in QuorumChain. Additional changes to this method of achieving consensus are easy to implement. Thirdly, the hybrid nature of the Quorum blockchain is ideal for a large number of enterprise use-cases. Fourthly, the fairly high throughput compared to public blockchains is essential for any scaling needs for high volume businesses. Finally, the ability to reuse the substantial development dedicated to the Ethereum protocol makes the choice of Quorum as our base implementation very appropriate.

In addition to the above, our fork includes a number of improvements to the Quorum protocol. The throughput of transactions is significantly increased in our test environment. We've developed a smart contract manager that allows for interoperability between the XDC blockchain and public blockchains. We've added punitive smart contracts that connect to the QuorumChain consensus smart contracts to ensure those who stake the XDCs to run network infrastructure remain honest. We're also in the process of developing a light client built for the Quorum protocol that would connect natively with the XDC ecosystem.

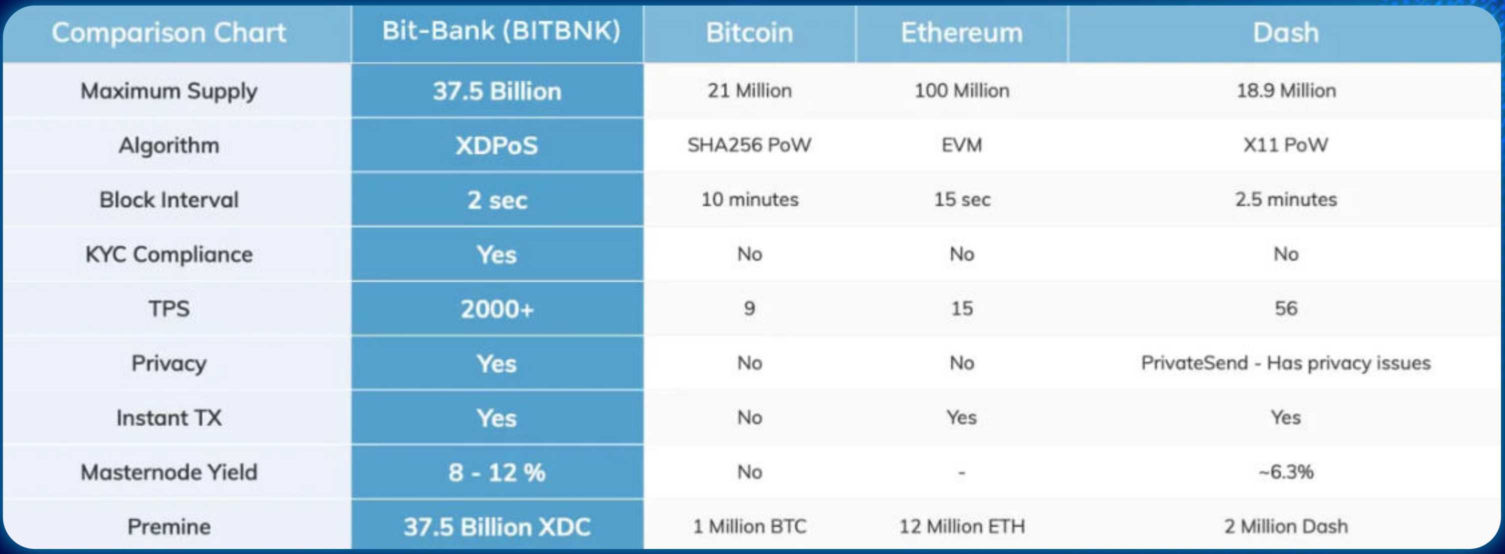
Tokens Technology

The XDC token is built upon the ERC20 token standard. This design decision was taken to ensure a fundamental compatibility with the multitude of emerging Ethereum Dapps. With a view at future interoperability with the Ethereum blockchain, the choice of using the ERC20 standard was straightforward. This compatibility extends to smart contracts written for the Ethereum blockchain.

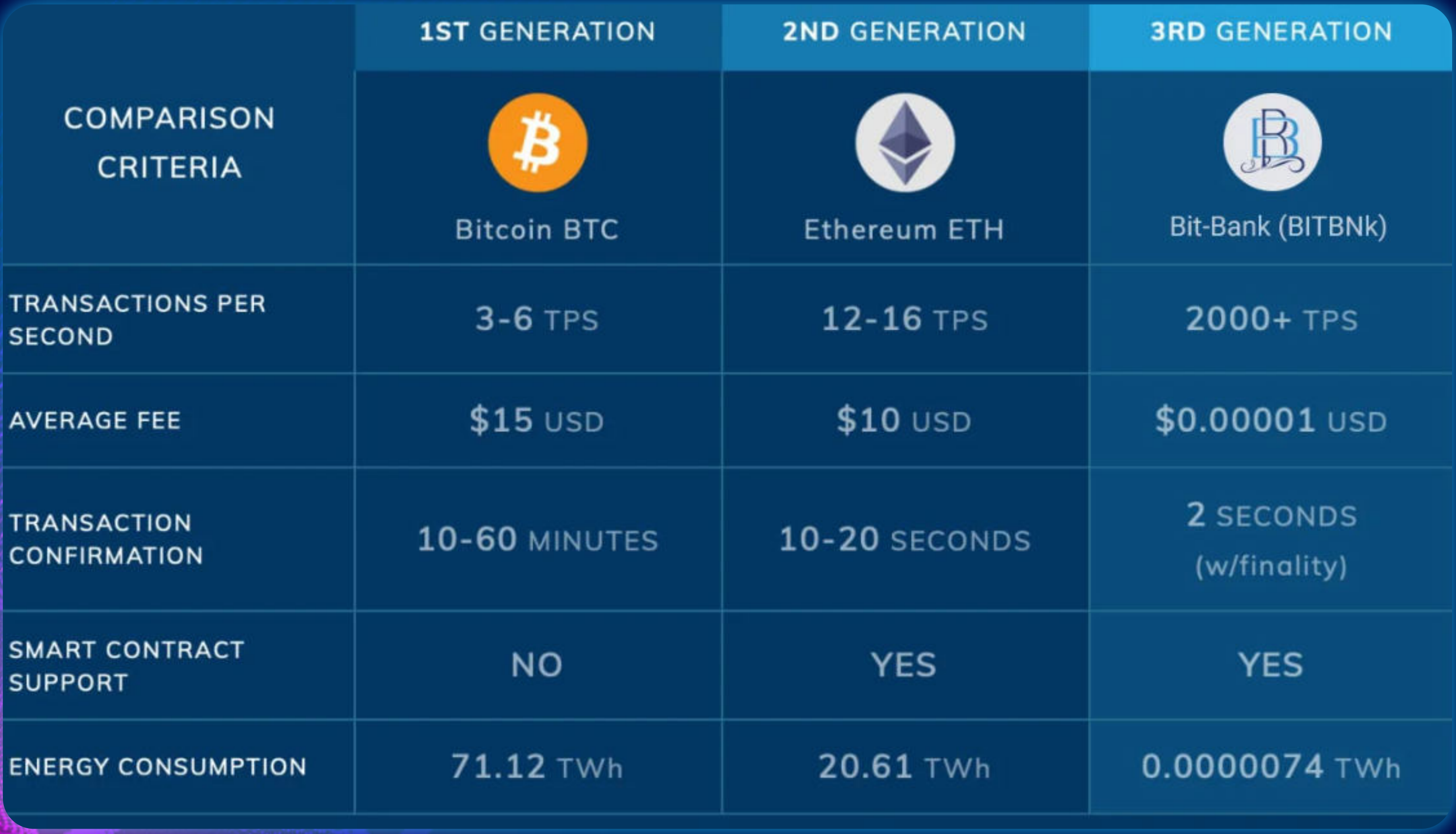
Centralised exchanges

While we all claim to be proud participants in a movement for decentralisation, we are tied to centralised exchanges. True decentralisation will evade the blockchain ecosystem till there is meaningful interoperability. Our design choice was also taken with this perspective in mind. We envision a future where all kinds of tokens can be exchanged and smart contracts are not limited to the architecture of individual organisations.

The Bit-Bank Ecosystem

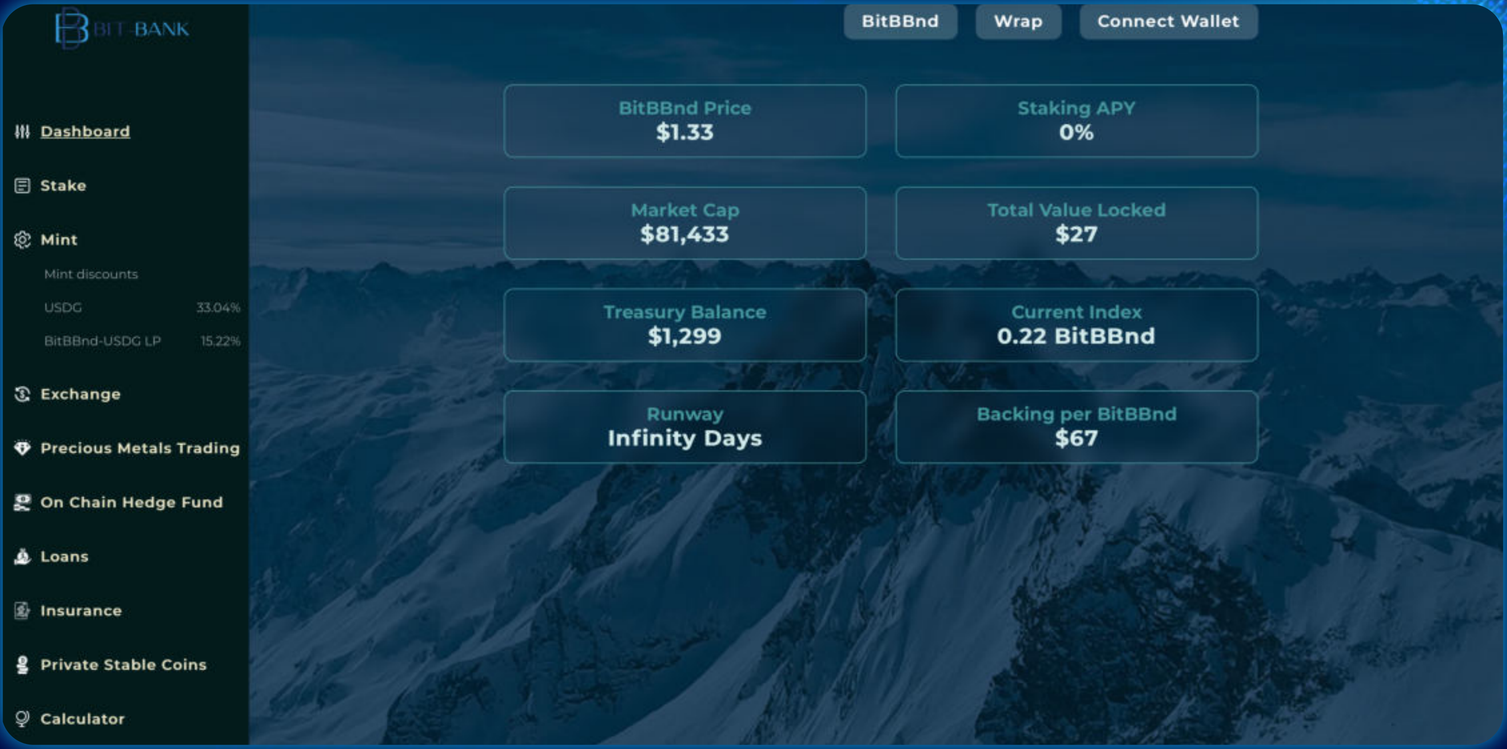


Comparison Chart	Bit-Bank (BITBNK)	Bitcoin	Ethereum	Dash
Maximum Supply	37.5 Billion	21 Million	100 Million	18.9 Million
Algorithm	XDPoS	SHA256 PoW	EVM	X11 PoW
Block Interval	2 sec	10 minutes	15 sec	2.5 minutes
KYC Compliance	Yes	No	No	No
TPS	2000+	9	15	56
Privacy	Yes	No	No	PrivateSend - Has privacy issues
Instant TX	Yes	No	Yes	Yes
Masternode Yield	8 - 12 %	No	-	~6.3%
Premine	37.5 Billion XDC	1 Million BTC	12 Million ETH	2 Million Dash



COMPARISON CRITERIA	1ST GENERATION	2ND GENERATION	3RD GENERATION
	Bitcoin BTC	Ethereum ETH	Bit-Bank (BITBNk)
TRANSACTIONS PER SECOND	3-6 TPS	12-16 TPS	2000+ TPS
AVERAGE FEE	$15 USD	$10 USD	$0.00001 USD
TRANSACTION CONFIRMATION	10-60 MINUTES	10-20 SECONDS	2 SECONDS (w/finality)
SMART CONTRACT SUPPORT	NO	YES	YES
ENERGY CONSUMPTION	71.12 TWh	20.61 TWh	0.0000074 TWh

The dApp



BIT BANK

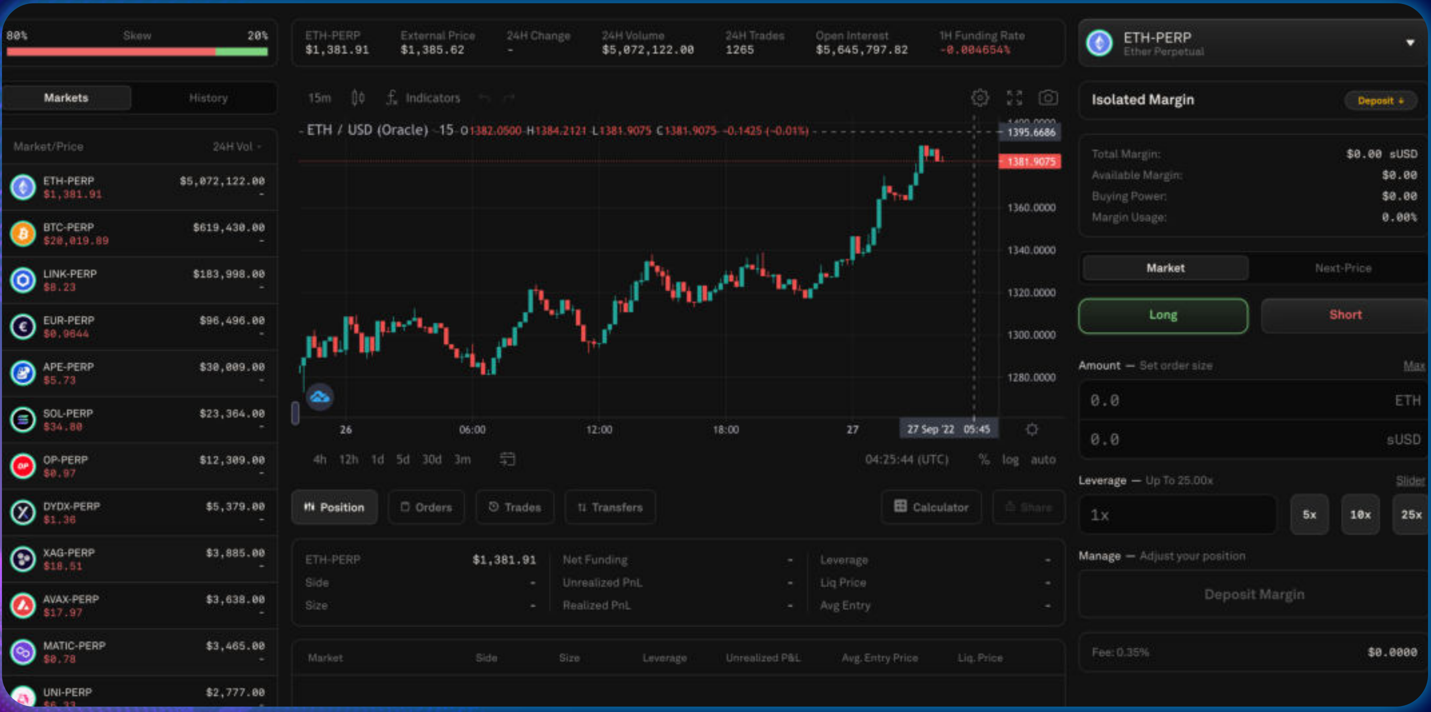
BitBBnd | Wrap | Connect Wallet

- Dashboard
- Stake
- Mint
  - Mint discounts
  - USDG 33.04%
  - BitBBnd-USDG LP 15.22%
- Exchange
- Precious Metals Trading
- On Chain Hedge Fund
- Loans
- Insurance
- Private Stable Coins
- Calculator

BitBBnd Price $1.33	Staking APY 0%
Market Cap $81,433	Total Value Locked $27
Treasury Balance $1,299	Current Index 0.22 BitBBnd
Runway Infinity Days	Backing per BitBBnd $67

Giving clients a user friendly control panel and interface for the EcoSystem connecting DeFi contracts across our platform.

Our DEX



80% Skew 20%

Markets | History

Market/Price	24H Vol
ETH-PERP $1,381.91	$5,072,122.00 -
BTC-PERP $20,019.89	$619,430.00 -
LINK-PERP $8.23	$183,998.00 -
EUR-PERP $0.9644	$96,496.00 -
APE-PERP $5.73	$30,009.00 -
SOL-PERP $34.80	$23,364.00 -
OP-PERP $0.97	$12,309.00 -
DYDX-PERP $1.36	$5,379.00 -
XAG-PERP $18.51	$3,885.00 -
AVAX-PERP $17.97	$3,638.00 -
MATIC-PERP $0.78	$3,465.00 -
UNI-PERP $6.33	$2,777.00

ETH-PERP	External Price	24H Change	24H Volume	24H Trades	Open Interest	1H Funding Rate
$1,381.91	$1,385.62	-	$5,072,122.00	1265	$5,645,797.82	-0.004654%

15m Indicators

ETH / USD (Oracle) · 15 · O1382.0500 H1384.2121 L1381.9075 C1381.9075 -0.1425 (-0.01%)

4h 12h 1d 5d 30d 3m

04:25:44 (UTC) % log auto

Position | Orders | Trades | Transfers | Calculator | Share

ETH-PERP	$1,381.91	Net Funding	-	Leverage	-
Side	-	Unrealized PnL	-	Liq Price	-
Size	-	Realized PnL	-	Avg Entry	-

Market	Side	Size	Leverage	Unrealized P&L	Avg. Entry Price	Liq. Price

ETH-PERP
Ether Perpetual

Isolated Margin Deposit +

Total Margin:	$0.00 sUSD
Available Margin:	$0.00
Buying Power:	$0.00
Margin Usage:	0.00%

Market | Next-Price

Long | Short

Amount — Set order size Max

0.0 ETH

0.0 sUSD

Leverage — Up To 25.00x Slider

1x | 5x | 10x | 25x

Manage — Adjust your position

Deposit Margin

Fee: 0.35% $0.0000

TOKENS

BIT-BANK EXCHANGE TOKEN
XDC:BITBNK

BIT-BANK DAO BOND TOKEN
XDC:BITBNKBND

TOKENOMICS

BIT-BANKS´ Private Protocol Stable Coins

EUR

GBP

USD

CHF

GOLD

SILVER

XBNK - BIT-BANKS' EXCHANGE TOKEN

We have created XBNK Tokens to match along with the original Bitcoins Core guidance of fixing a problem, so we have set at the national said currency reserves at 20 Trillion with an additional 8 decimal places.
The XBNK Token will burn every coin that is used after transfer for security purposes, thus also increasing in user value for long term speculation and rewards for being part of the Privacy as a Service revolution.

XBNK is a Hybrid Private Blockchain advanced XDPoS Algorithm, transacting at 2000 Transactions per Second, giving users Instant Private Transactions with ISO KYC Compliance and with Smart Contract capabilities.

XBNK allows the user to access the Web3 Private Decentralised Encrypted Exchange, which is found hosted at https://app.bit-bank.io, which enables you to access decentralised Financial Instruments and Privacy Stable Coins. (The Exchange may also be accessed via our Privacy Enabled Stable Coins or other Privacy Coins such as Monero, zCash, Dash)

The XBNK Token will also be able to work as a bridge for assets between our CeFi Financial Services.

✓ Lower Exchange Fees for token holders.

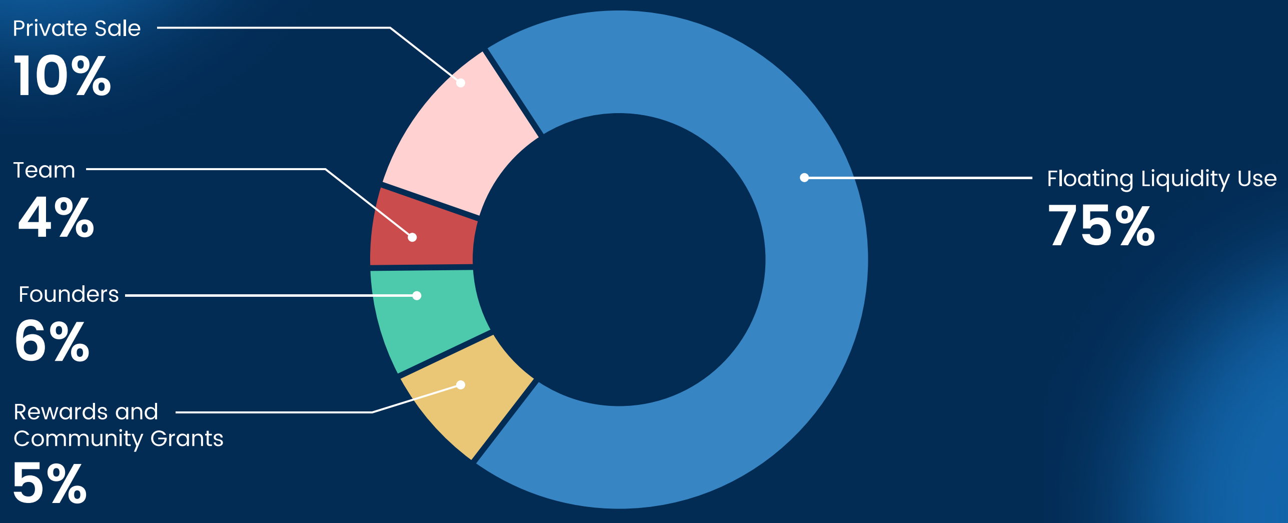
✓ Privacy Enabled Blockchain

✓ Low Fees

✓ ISO20022 Complaint

✓ Secure Transaction and Burn Feature

✓ 3rd Generation Speed Block Intervals, Algorithms and Transactions Per Second.

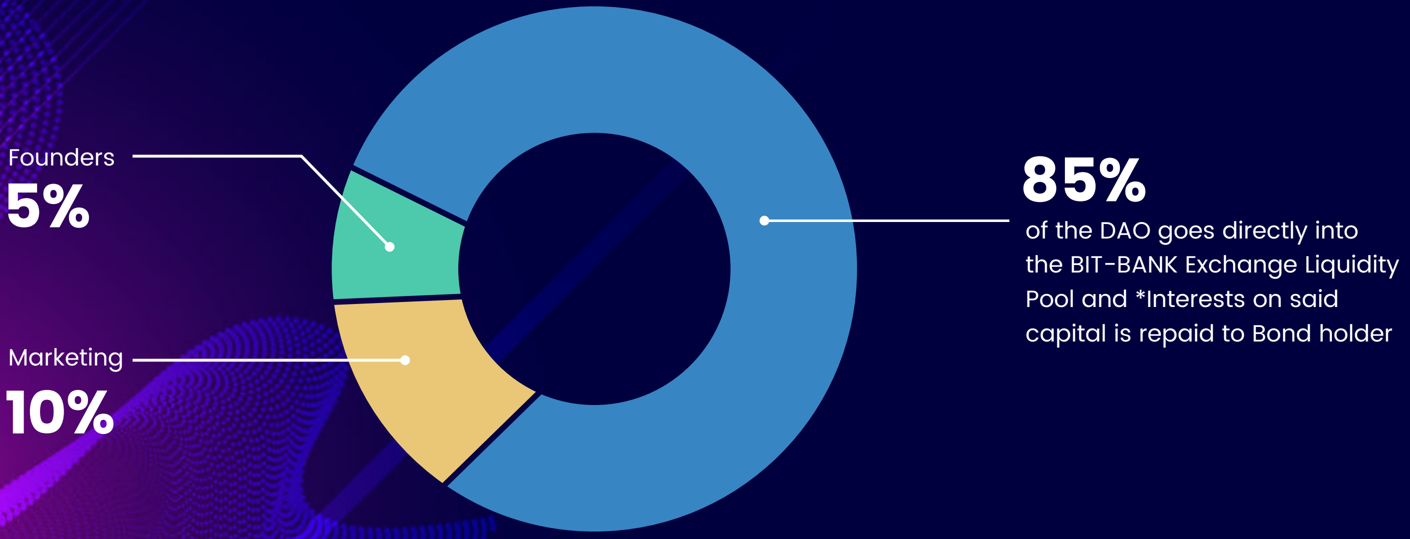


BITBBND - BIT-BANK'S BONDS

Our Company has taken the step to become a fully Decentralised Autonomous Organization (DAO). We felt that in order to make our business fully compliant yet privacy and security based for our Clients, Founders and Team this was the best way in securing our future success by giving the business back to its community and developers.

The Bit-Bank Ecosystem and COMMUNITY GOVERNANCE

By using the latest in cryptographic technology we have been able to divide the business and harness the real use case for angel investors and investors alike to be part of a revolutionary future.
Using our Business Model of a dAPP onto of a Web3 infrastructure bridging between additional Financial Services and keeping everything Private! We have been able to do all the work, launch all the code and sign all the contracts and we have managed to keep our anonymity and maintain high standard of relationships with banks and financial institutions understanding our remit and business.
We have given the business back to the community where investors can purchase Bond contracts from us that provide liquidity to our other clients wishing to exchange or other financial services and share the benefits with the liquidity holders. Our bonds are Monthly, Quarterly or Yearly.



Discreet Custody Service

We offer our clients a discreet and private Crypto Custodian Service, served from Switzerlands Fort Knox data centre we give clients the finest in privacy, security and discretion.

24-7 Zero Access Custody - The Private Key is completely Air gapped to minimise attack possibilities, we do not have or own keys to your holdings, which means our clients control their private keys and sign their transactions, we are locked out of your holdings. The cold wallets are completely air-gapped and authorised by the client.

Our data centre is known as the Swiss Fort Knox, it is Europes safest data centre, protected and situated in the heart of the Swiss Alps, we host our data in an ex Swiss Military Bunker, the buildings have excellent structural and sturdy design which makes them resistant to Military and Civilian Threats. There is also a runway and customs for private jet/plane and helicopter access to the bunker, we have full protection against NSA Prism snooping. Encoding of all of our data using the 256 AES encryption standard.

Three factor authentication, Multi Party Authorisation, and RSA signatures are required for moving funds from the Custodian account, our blockchain and coins hosted in our data centre are our Stable Coins, Exchange Tokens and DAO Bonds which are all privacy enabled cryptocurrencies on the XDC blockchain.

We also implement Onion servers in between our clients three factor signing transactions and back to our data centres.

Keybackups, Security and Insurance are available, we do also offer Regulated Custodian solutions with our FINMA regulated banking partner.

Security features

Security features

The key lifecycle is entirely air-gapped to minimize the attack surface.

Transaction Signing

Customers must initialize all transactions to be processed.

Entropy & Client Account Segregation

Client accounts are segregated at the root entropy level. No shared omnibus.

Strict Process Isolation

All servers and customer terminals boot into a secure environment.

Partitioning & Physical Segregation

Each root key in a customer's multisig scheme is handled by a distinct physical device in a distinct data center behind a distinct firewall.

Data Storage & Encryption

Most sensitive secrets are stored on Knox Secure Modules and cannot be retrieved.

Client Account Backups

Encrypted wallet key backups are using Shamir's Secret Sharing Scheme.

Key Backup Storage & Retrieval

A security and logistics firm is responsible for storage and retrieval of backups.

Client Authentication

All Knox clients are required to use three-factor authentication.

swiss safety center ISO 27001 certified system

MADE IN EUROPE INNOVATIVE PRODUCT

SWISS ACCREDITATION sas.admin.ch SCESm 0073

EMshield
an Albatross Projects company

Partners

Degussa
GOLD UND SILBER.

Securitas

MOUNT10
SWISS DATA BACKUP

Eth Capital Asset
Management & Hedge LLC

ARGOR · HERAEUS SA ·
AH

Tor

X

Additional Services

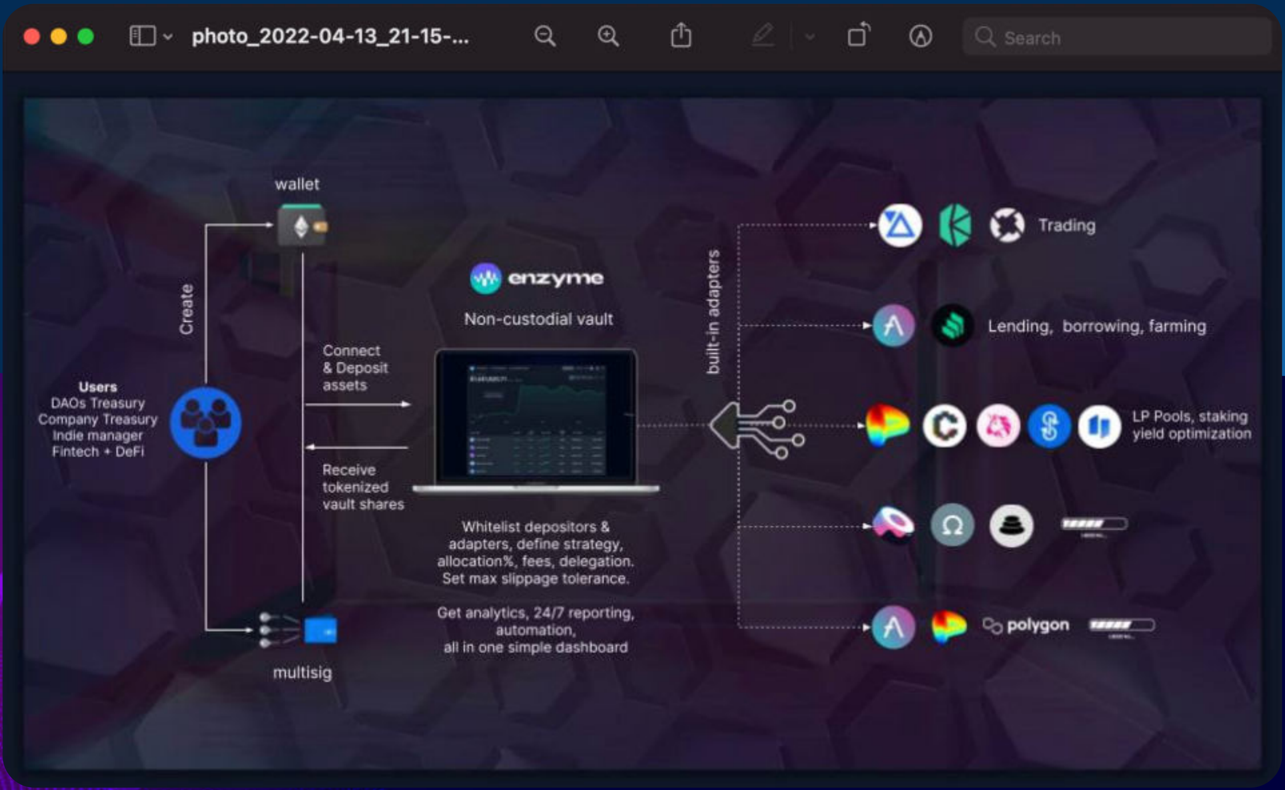
Precious Metals Trading – Digital or Physical Precious Metals Trading.
Pegged 1 for 1 with our stable coins.
either in vault or you can send us an encrypted Memo using PGP - SHA - encrypted messaging with address for physical delivery.

Lending

Excellent LTV lombard loan rates against your assets for liquidty.

On Chain Hedge Funds

Hedge Fund Investing – On Chain Asset Management, led by the markets best Hedge Fund Managers www.ethcapital.co.uk using the Enzyme Ethereum Protocol with over 300Million under Asset Management.



Whitelist depositors & adapters, define strategy, allocation%, fees, delegation. Set max slippage tolerance.

Get analytics, 24/7 reporting, automation, all in one simple dashboard

Staking

VPN,VPS + TOR Clusters

Secure private Virtual Private Servers and VPNs on our intranet, only can access certain services when fully connected to the VPN. We do not keep logs, we do not share data with anyone. This is a privacy service.

Black OS Secure USB

Secure Cold Wallet and Security Configured Mobile devices

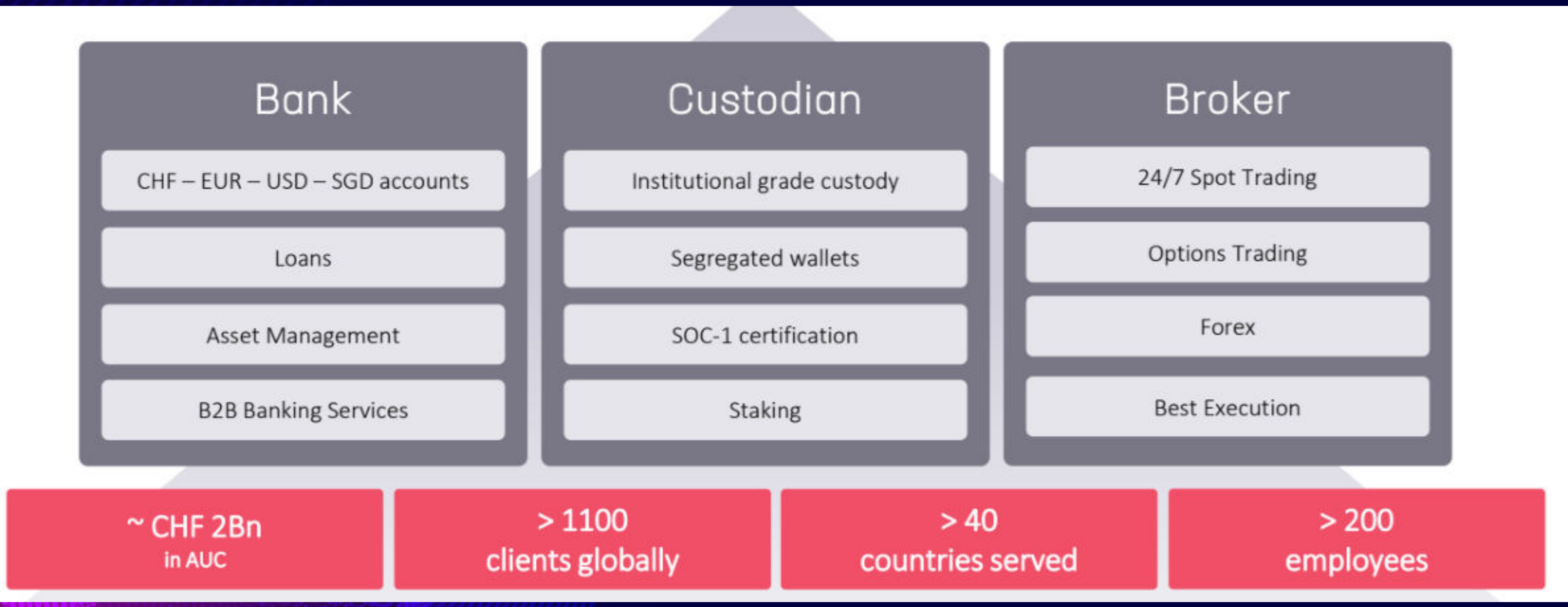
Centralised Financial Services

Trade: Access our universe of supported assets thanks to our institutional brokerage desk connected to the leading institutional liquidity pools in the space to help them manage their clients' positions with the highest liquidity.

We help to Securely store clients' digital assets under a fully regulated environment with our banking-grade custody solution that follows the highest security standards and counts with the certification of PwC

Manage clients market exposure with derivatives, professionally managed investment products and loans.

All this **directly settled with the traditional banking system,** with fiat accounts in CHF, EUR, USD, SGD.



Bank	Custodian	Broker
CHF – EUR – USD – SGD accounts	Institutional grade custody	24/7 Spot Trading
Loans	Segregated wallets	Options Trading
Asset Management	SOC-1 certification	Forex
B2B Banking Services	Staking	Best Execution

~ CHF 2Bn in AUC

> 1100 clients globally

> 40 countries served

> 200 employees

Seamlessly integrated digital asset banking

We offer a banking-grade compliant, integrated solution to securely issue, store, trade and manage digital assets.

Brokerage

Trade your digital assets securely and seamlessly 24/7

Sygnum's technology and operations are set up for highly secure and seamless trading of digital assets, allowing clients to focus on what is truly important – their investment decisions

Tokenization

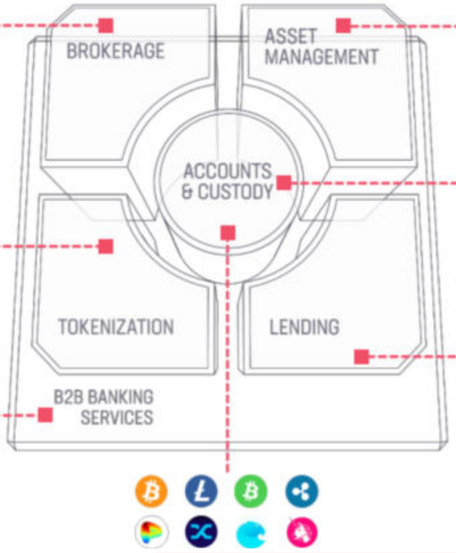
Create added value for both issuers and investors through tokenization of new and existing assets

Sygnum's tokenization solution is built to improve the life-cycle management of securities issuance and investment, enabling issuers, such as SMEs, to reduce cost and time spent on raising capital and managing corporate actions

B2B Banking Services

Add regulated digital asset banking service to your business

Sygnum partners with existing financial institutions to enable them to provide regulated digital asset products and services to their own clients through white-label B2B banking services



Asset Management

Diversify your investment portfolio with digital assets

Sygnum provides high-quality digital asset investment products, providing diversified exposure to an emerging megatrend

Accounts and Custody

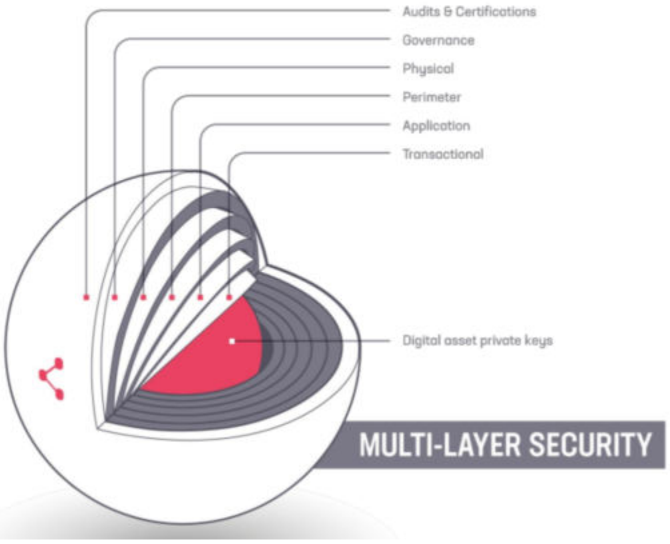
Store your digital assets with institutional-grade trust

Sygnum's custody infrastructure, co-developed with Swisscom, is built with a multi-layer security approach enabling clients to invest in digital assets with complete trust

Lending

Increase your liquidity with digital asset Lombard loans

Sygnum Bank`s Lombard loans are designed to increase fiat liquidity against digital assets such as Bitcoin and Ethereum on Sygnum`s banking platform



Six security levels

Audits & Certifications

- Transaction signature process audited by PwC (ISAE 3000) ongoing audit of transaction environment (ISAE 3402) by PwC
- HSMs fully compliant with industry leading security standard (FIPS-140.2 Level 3)

Governance

- Processes and organizational structures ensure that no team or single employee can independently access your private keys
- Critical transactions must be approved by several delegated individuals in your organization

Physical

- HSMs located in Switzerland in Tier 4 data centers (highest security level)
- Data centers are run by Swisscom, the largest banking infrastructure provider in Switzerland

Perimeter

- Multi-factor authentication for critical transactions
- Suspicious/ off-pattern transactions monitoring in terms of time, volume or geography

Application

- No single point of failure in the system architecture
- Segregated accounts

Cross-Asset Trading Services

Best prices

Fast execution

Fast settlement

Bank-grade settlement

24/7 spot trading of digital assets

- Instantaneous settlement 24/7
- Automated and commoditized product
- Best price execution
- Different order types: market, stop limit*, stop loss*
- Wide variety of coins

Options

- European style put and call options
- Offered on BTC/USD and ETH/USD (others on request)
- Long and short positioning possible
- Profit from market volatility in crypto space

Forex

- Swaps, forwards, spot, liquidity management
- Wide range of currency pairs
- Competitive spreads

Upcoming products

- Futures and forwards on BTC and ETH
- Leveraged trading
- Structured products: reverse convertibles, tailored, new coins
- Algorithmic orders

Double Validation (DV) XinFin DV Technique and Technicals

With XinFin's DV technique, the likelihood of having garbage blocks in the blockchain is significantly reduced. In this case let's assume that M1 and M2 are the block creator and block verifier of block100, respectively.

If block100 is invalid and M2 is honest (see Fig. 3 [a]), the next block creator M3, when creating block101, notes that block100 doesn't have the required number of signatures (two signatures in XinFin's case), and thus, rejects block100 and creates another block100 next to block99. In the event that M2 is also an attacker pairing/handshaking with M1 (see Fig. 3 [b]), M2 signs block100 despite its invalidity. Worth noting is that XinFin's block verifiers or M2 are randomly selected, therefore there is little chance of successfully pairing M1 and M2. This limits the possibility of invalid blocks being added to the blockchain.

Next, even after M3 verifies that block100 has two valid signatures, M3 still rejects it because block100 is invalidated by M3 that will create another valid block100. To break the stability and consistency of XinFin's blockchain, in this case, M3 should be an attacker together with M1 and M2. This scenario has a low probability of occurring since block verifiers are randomly selected. That said, DV strengthens the consistency of the blockchain and makes it hard to disrupt.

Fig. 3. Double Validation (DV): (a) DV with block creator as an attacker and (b) DV with both block creator and block verifiers as attackers

Randomization for Block Verifiers for Double Validation

The First masternode or Block Creator: Within a given epoch, the first masternode/block creator(v1) is selected by a round-turn game and it can be formally defined as an array.6 The array's formula is as follows:

(equation: 1)

Random Matrix and Smart Contract

To select random verifiers for a subsequent epoch (e+1), 3 (three) steps are followed. To understand the three steps explained below, let m be the number of masternodes, n be the number of slots in an epoch.

Step 1: Random Numbers Generation and Commitment Phase

First, at the beginning of epoch e, each masternode Vi creates an array of n + 1 special random numbers Recommendi = [ri.1, ri.2, ..., ri. n, θi], where ri. k ⊠ [1, ..., m] indicates the recommendation of an ordered list of block verifiers for the next epoch of Vi, and θi ⊠ {-1, 0, 1} is used for increasing the unpredictability of the random numbers.

Second, each masternode Vi has to encrypt the array Recommendi using a secret key SKi, say Secreti = Encrypt (Recommendi, SKi) as the encrypted array. Next, each masternode forms a "lock" message that contains encrypted array Secreti, signs off this message with its blockchain's private key through the Elliptic Curve Digital Signature Algorithm (ECDSA) scheme that's currently used in Ethereum and Bitcoin along with the corresponding epoch index and its public key generated from its private key. After forming a "lock" message and signing off the message via the ECDSA verifiable key, every masternode can check who created this lock message through ECDSA verification scheme and which epoch it relates to. Thereafter, each node Vi sends their lock message with its signature and public key to a Smart Contract stored in the blockchain. The process enables each masternode to collect and know the locks from all other masternodes.7

Step 2: Recovery Phase

The recovery phase is for every node to reveal its previous lock message so other nodes can get to know the secret array it has sent before. A masternode only starts revealing its lock message if all masternodes have sent their lock messages to the smart contract or a certain timeout event occurs. Each masternode then opens its lock message by sending an "unlock" message to the smart contract for other masternodes to open the corresponding lock. Let's imagine a commitment-like scheme, in this case, where a lock message is a commitment message locking its contained recommendation array Recommended so that no one can open or guess the contained array, and the unlock message gives the key for other masternodes to decrypt the box and retrieve the values of Recommended. Eventually, a masternode has both locks and unlocks to other masternodes. If some elector is an adversary which might publish its lock but not intend to send the corresponding unlock, other masternodes can ignore the adversary's lock and set all its random values be 1, by default. The idea is simple: the network can keep working successfully even if some masternodes are adversaries.

Step 3: Assembled Matrix and Computation Phase

At the point of the slot nth of the epoch e, the secret arrays Secreti in the smart contract will be decrypted by each masternode and return the plain version of Recommendi. Each tuple of the first n numbers of each Vi will be assembled as the ith column of an n × m matrix. All the last number θi forms a m × 1 matrix. Then each node will compute the block verifiers ordered list by some mathematical operations as explained below. The resulting output is a matrix n × 1 indicating the order of block verifiers for the next epoch e + 1.
For the second masternode or block verifier, each node computes the common array v2 for the order of the block verifiers by the following steps as in Equation 1.

(equation: 2)

Then, v2 is obtained by modulo operation of element values of v 0 2 as in Equation 2:

Finality Analysis

A standard definition of "total economic finality": A phenomenon occurring when 3/4 (three quarters) of all masternodes make maximum-odds bets that a given block or state will be finalized. This condition offers very strong incentives for masternodes to never attempt colluding to revert a block. When masternodes make such a maximum odds bet, in any blockchain where that block or state is not present, the masternodes lose their entire deposit.8

XinFin Network maintains this standardization in the design so that one block is considered as irreversible if it collects up to three-quarters of the signatures of all members in the masternodes committee. The time-line of the blockchain creation process, checking finality, and marking the block as immutable are described in Figure 4 below.

Fig. 4. Timeline of Blockchain Making Process

D. Consensus Protocol: Formalization

Basic Concepts & Protocol Description

To provide a solid educational foundation and to prove that the XinFin Network can achieve its claims, in the following section, we will present a preliminary examination of the concepts discussed in our yellow paper and an overview of XinFin Delegated Proof of Stake (XDPoS). To start, we will provide a presentation of XinFin's proof of stake consensus algorithm. The formalization follows that of notable tokens, such as Cardano and Thunder, in recent literature. More specifically, XinFin places emphasis on the following concepts and definitions that were presented in literature for Cardano and Thunder tokens and adapts them to the context of XinFin Network.

Time, Slots, Epoch

Ideally, each epoch is divided into 900 block times. Each of these block times is referred to as a block slot. Only one block can be created in a slot. The main assumption is that there is a roughly synchronized clock that allows for masternodes to learn the current slot. This simplification effectively permits masternodes to execute the signing and validation process of the XDPoS consensus, where each masternode must collectively create a block to the current slot. Simplified further, each slot SLR is accessed by an integer r ⊠ {1, 2, ...}, and is supposed that the real-time window that corresponds to each slot has the following properties, which are similar to what is specified in Cardano.6

1. Everymasternodecandeterminetheindexofthecurrentslotbasedonthecurrent time. And, any discrepancies between parties' local time are insignificant in comparison with the length of time represented by a slot.

2. Theamountofaslottimeissufficienttoguaranteethatanymessagetransmittedby an honest party at the beginning of the time window will be received by any other honest party by the end of that time window. While similar to Cardono's assumption,

the XinFin Network adopts the assumption to ensure that block creators seamlessly propagate their created blocks to the corresponding block verifiers. This guarantees a block is signed by both the masternodes before the next block creator builds another block on top of it.

As mentioned in Section II-A, in XinFin's setting, it's assumed that the fixed set of m (150) masternodes V1, V2, ..., Vm interacts throughout the protocol to reach the consensus. For each Vi, a public/private key pair (PKI, ski) for a prescribed signature scheme, ideally ECDSA, is generated.

Additionally, XinFin's protocol adopts the assumption that the public keys pk1, ..., pkm of the masternodes are distributed and known by all masternodes in the protocol (that means a masternode knows all public keys of all other nodes). Some notable definitions of the blockchain concepts are defined following the notation.

Definition 1 (State):

A state is an encoded string st ⊠ {0, 1}

Definition 2 (Block):

A block B generated at a slot sli contains the current state st ⊠ {0, 1} λ, data d ⊠ {0, 1} ⊠, the slot number i and a signature Σ = Signski (st, d, sli) computed under ski corresponding to the masternode Vi generating the block

Algorithm 1: The algorithm illustrated the consensus protocol

Input: m - Number of masternodes, n number of slots in an epoch Output: The complete ledger of the blockchain C

To create the complete ledger for block C, several steps must be completed. These are as follows: (a) Creating the empty blockchain (stack) C (b) Commencing an Initial Coin Offering (ICO) to raise funds to support the provision of cryptocurrencies and blockchain-related products and services (c) Issuance of tokens/coins to holders. These tokens do not provide equity stake, rather they deliver their owners some stake in a product or service created by the company and (d) Voting for the masternode committee (masternodes) VC ⊠ {V1; V2; ..., Vm}.

Thereafter, (e) Initiate the first epoch e1 ⊠ {sl1, sl2, ..., sln};(f) Randomly generate the array of second masternodes for the first epoch SV1 ⊠ [v 1 2.1, v1 2.2, ..., v1 2. n]; (g) Create the genesis block B0; (h) Update the blockchain C ⊠ C. push(B0); while true do while j is less than n to create block Bj by the first masternode; Update the blockchain C ⊠ C. push (Bj);

Then, step (i) validate the block Bj by the second masternode; (j) broadcast and validate the block Bj by VCi; if Bj has more than 3/4 masternode committee members' signature then FINALITY(Bj .ID) = true; if j = n then j ⊠ 1; else j++; if len(C) mod n = 0 then doCheckpoint(); Voting for the masternode committee for the next epoch VC ⊠ {V1; V2; ..., Vm}; Random generate the array of verifier masternodes for the next epoch (i + 1)th; SVi+1 ⊠ [v i+1 2.1 , vi+1 2.2 , ..., vi+1 2.n]; ei+1 ⊠ i ⊠ n ⊠ 2 + e1; i++;
Here's a pictorial summary of the process:

Definition 3 (Blockchain):

A blockchain C is a sequence of blocks B1, ..., Bn associated with a strictly increasing sequence of slots for which the state sti of Bi is equal to H(Bi-1), where H is a collision-resistant cryptography hash function. To add, a blockchain has a number of properties, including the length of a chain len(C) = n, which is its number of blocks, and the block Bn is the head of the chain, denoted head(C).

As mentioned earlier, in the XinFin Network model, each time slot sli is set as 2 seconds and an epoch is a set as R of 900 slots {sl1, sl2, ..., sl900}. The duration of an epoch equals 1800 seconds. In summary, the consensus protocol of XinFin Network consensus can be formalized in Algorithm 1. Algorithm 1 is simulated and explained as a process shown in Fig. 5

Fig. 5. Randomization of Block Verifiers, Creating and Validating Blocks in Each Epoch

SECURITY ANALYSIS

A. Nothing-at-stake

Nothing-at-stake is a well-known problem in PoS-based blockchain, just like the 51% attack in PoW algorithms. For PoW-based miners, it’s mandatory to have CapEx (capital expenditures) for buying mining equipment such as ASICs. Similarly, there's a need for OpEx (operation expenditures) such as electricity to solve mathematical puzzles securing the network. That means, there is always an intrinsic cost for miners in mining regardless of its success. In case of a fork, miners therefore always allocate their resource (equipment) to the chain that they believe is correct in order to get incentives for compensating the intrinsic costs in mining.

On the contrary, PoS-based systems don't rely on mining. During an ideal execution creating a fork, the only costs incurred relate to block validation and signing. That is because masternodes do not incur intrinsic costs. In this case, there’s an inherent problem of the masternode having no downside to staking both forks. Therefore, there are actually two issues in the original design of PoS. On one hand, for any masternode, the optimal strategy is to validate every chain/fork, so that the masternode receives its rewards no matter which fork wins. On the other hand, for attackers/malicious masternodes, they can easily create a fork for double spending.

The XinFin Network handles these two problems exceptionally. (Note: Through the XinFin Network consensus protocol, the XinFin Network maintains a certain order of masternodes in creating and sealing blocks during each epoch).

For the first issue, random/arbitrary forks never happen because block creation by the masternodes is predetermined in each epoch. For the second issue, the Double Validation mechanism ensures that only one block can be validated by the second randomly selected masternode. That’s even when one malicious masternode creates two blocks at its turn.

B. Long-rangeattack

Within the XinFin Network, a block is valid only if it collects Double Validation and is finalized once 3/4 of masternodes verify. Therefore, as long as the number of attackers or malicious nodes and/or fail-stop nodes is less than or equal to 1/4 the number of masternodes, the number of masternodes signing a block is at least 3/4 the total number of masternodes, which makes the block finalized.

Thus, there is no chance for one malicious masternode to create a longer valid chain on the XinFin Network because other masternodes will reject the new block.

C. CensorshipAttack

In the event that there are more than 3/4 malicious masternodes in the XinFin Network, censorship attacks may occur. For example, if the malicious masternodes refuse valid blocks or simply become inactive, the chain is stuck. To avoid censorship attacks, masternodes are paid for their effort of correctly working so that the chain is actively updated in a consistent manner.

More importantly, becoming a masternode means a certain number of coins is locked —10,000,000 XDC in this case. Therefore, to control more than 3/4 masternodes, attackers must hold a considerable amount of XDC and gain substantial support from coin-holders. Given the inhibiting cost, the attackers do not have incentives to engage in any malicious activity that could harm the chain

However, in the worst-case scenario, XinFin Network can conduct a soft fork to reduce the number of masternodes, keeping the chain running and figuring out slasher mechanisms to weed out the malicious masternodes.

D. RelayAttack

The XinFin Network supports EIP155. The EIP-155 provides unique identifiers to a blockchain helping it overcome relay attacks. With EIP-155, two conditions are met: (a) definition of an integer for Chain-id for a blockchain and (b) signing of a chain-id into a transaction data. This prompts attackers to send the same transaction to different blockchains. With specifications in the EIP-155, blockchains have to define a chain-id and register the chain-id in a public repository.9

9 Zoltu, Micah. "Ethereum/EIPs." GitHub, September 29, 2020. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-155.md.

A challenge for using an integer for chain-id is that it's not broad enough to cover all blockchains and it doesn't prevent the use of the same chain-id by different blockchains. Furthermore, using an integer fails to address issues introduced by two forked blockchains having the same chain-id. In this context, the XinFin Network has adopted a more robust blockchain identifier that overcomes these drawbacks, especially for cross chain operations where multiple chains are involved thus providing extensive protection against relay attacks. With the XinFin Network, the process through which a transaction id is made unique is as illustrated with the following example:

Consider a transaction with: **nonce = 9, gas price = 20 * 10**9, start gas = 21000, to = xdc3535353535353535353535353535353535353535, value = 10**18, data='' (empty).**

Once signed the “signing data" becomes:

Lorem Ipsum

0xec098504a817c800825208943535353535353535353535353535353535353535880de0b6b3a7640000 80018 080

And, the "signing hash" becomes:

0xdaf5a779ae972f972197303d7b574746c7ef83eadac0f2791ad23db92e4c8e53

In the event that a transaction within the XinFin Network is signed with a private key like **0x4646464646464646464646464646464646464646464646464646464646464646,** then the v, r, s values would be:

(37, 18515461264373351373200002665853028612451056578545711640558177340181847433846, 46948507304638947509940763649030358759909902576025900602547168820602576006531)

With the use of 37 instead 27 in the v, r, s values, the signed Tx would become:

0xf86c098504a817c800825208943535353535353535353535353535353535353535880de0b6b3a76400008025a028ef61340bd939bc2195fe537567866003e1a15d3c71ff63e1590620aa636276a067cbe9d8997f761aecb7033 04b3800ccf555c9f3dc64214b297fb1966a3b6d83

Within the XinFin Network, a cross chain-id can be used to present a relay attack. Notably, applications handling cross chain transactions can verify cross chain-id via their block hash and decide whether the transaction is valid or not. Transactions without a verifiable cross chain-id are rejected. In effect, EIP-155 specifications provide a robust approach to preventing relay attacks.

Table 1 shows chains and chain-ids recognized on the network.

CHAINS AND CHAIN_ID

1	Ethereum mainnet	61	Ethereum Classic mainnet
2	Morden (disused), Expanse mainnet	62	Ethereum Classic testnet
3	Ropsten	1337	Geth private chains (default)
4	Rinkeby	77	Sokol, the public POA Network testnet
30	Rootstock mainnet	99	Core, the public POA Network main network
31	Rockstock testnet	50	XinFin Mainnet
42	Kovan	51	XinFin Testnet

E. SafetyandLiveness

A consensus protocol is considered live if it can eventually propagate and make valid transactions onto the blockchain. A liveness fault occurs when transaction omission, information withholding, or message reordering, among a number of violations are observed. This type of fault is unlikely to happen in XinFin Network because the block creation masternodes list is ordered in a predetermined way for each epoch, thus if even an attacking masternode omits some transactions, the latter will be processed and validated by the next honest masternode in the next block.

Furthermore, safety implies having a single agreed upon chain where there are not two or more competing chains with valid transactions in either chain. As such, consensus protocols are safe when blocks have settlement finality, or else probabilistic finality. The XinFin Network provides safety because it has a settlement finality.

To note, XinFin Network has implemented the Istanbul Byzantine Fault Tolerant (IBFT) consensus mechanism. The IBFT consensus mechanism ensures instant finality, higher throughput, manageable validator set, and a high Transaction Per Second (TPS) rate.[10]

With the IBFT consensus mechanism, the XinFin Network introduces several benefits guaranteeing the network's safety and liveness. First, the XinFin Network—via the IBFT—guarantees immediate block finality. That is because only 1 block is proposed at a specific chain height. Thus, the single chain removes forking, prevents uncle blocks, and the risks that a transaction may be “undone” once on the chain at a later date. It’s worth noting that XinFin’s MyContract—a next generation smart-contract platform—will be IBFT compliant, enabling the consensus to scale up to 2500 TPS.

Second, the IBFT consensus mechanism reduces times between blocks. This occurs by effectively reducing efforts needed to construct and validate blocks, increasing the throughput of the network. Third, with the IBFT consensus, the XinFin Network ensures high data integrity and fault tolerance. To clarify, the IBFT employs a group of validators to ensure the integrity of each block being proposed. Plus, a super majority (66%) of the validators are required to sign a block Byzantine, which is inserted to the chain, making block forgery very difficult. Thirdly, the IBFT consensus mechanism guarantees operational flexibility. Notably, the ‘leadership’ of the network's validators rotates over time, preventing faulty nodes from exerting long-term influence over the chain, introducing undesirable liveness and safety issues.[11]

[10] Yutelin. “Istanbul Byzantine Fault Tolerance · Issue #650 · Ethereum/EIPs.” GitHub, June 22, 2017. https://github.com/ethereum/EIPs/issues/650

F. DDOS Attack

Distributed denial of service (DDoS) attacks occur when malicious characters overwhelm the target or the related infrastructure with malicious traffic. Employing networks of malware compromised computers, bots, and other devices, an attacker remotely controls the target infrastructure. DDOS adversary affects the bandwidth and connectivity leading to the disruption of services on a network. To add, cloud-based ecosystems suffer significant losses since DDOS causes service degradation and in some cases complete service denial.

Lorem Ipsum

11Yutelin. "Istanbul Byzantine Fault Tolerance · Issue #650 · Ethereum/EIPs."

Fig.6.Distributed denial of service (DDoS) attack.12

In the context of the XinFin Network, masternodes are required to run on reputable public cloud providers like AWS, Microsoft Azure or Google Cloud, which provide multiple DDOS prevention mechanisms. When some nodes are attacked or fail-stop, the network still operates correctly as long as the number of failing and/or attacked nodes remains less than 1/4 of the number of masternodes.

G. SpamAttack

XinFin Network keeps the same transaction fee mechanism as Ethereum which employs gas prices.13(-Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network).14 However, the XinFin Network supports a minimum transaction fee (1 wei--approx. 1/100 the gas price of Ethereum). Concerns have been raised on the likelihood of spamming given that attackers try to broadcast a huge amount of low fee transactions to the system. To deter spamming attacks, however, the XinFin Network's masternodes always sort transactions and pick up only high fee transactions into the proposing block. Thus, spammers have little chance of harming the system.

BIT-BANK

"Privacy Empowering The World Block By Block, The Future Is Decentralised Be Part Of It!"

BIT-BANK – (2017)