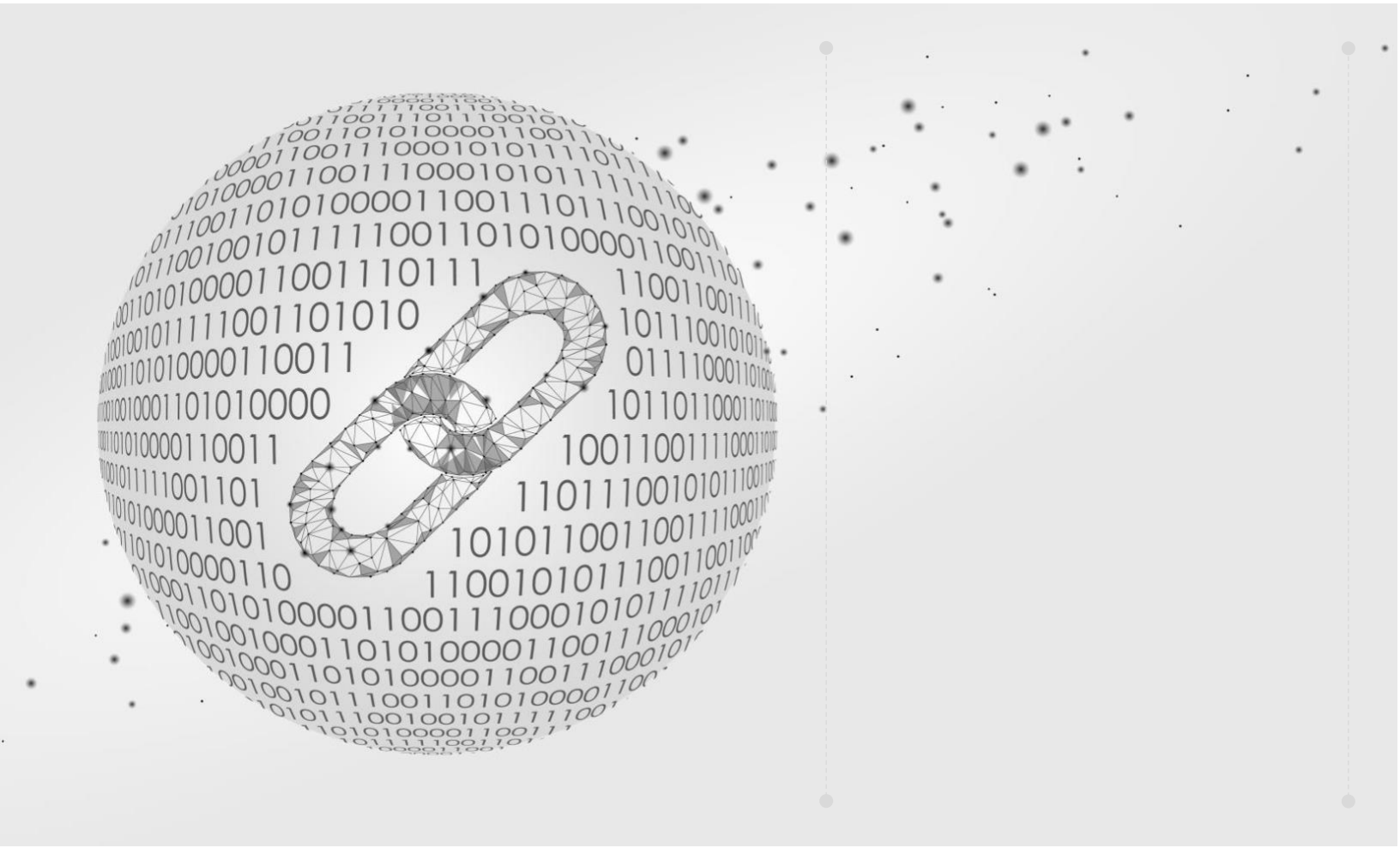
Version: 2.0.1

Dated: 6-OCT-2019

Founded by Silicon Valley veterans, Zebi operates in the entire blockchain ecosystem and is focused on core blockchain and blockchain related technologies



This document is intended to be a high-level business version of the whitepaper, explaining Zebi's vision and how we intend to pursue it.

It covers business problems in the blockchain world that Zebi believes are important and outlines the approach in solving the technology problems that are important in achieving Zebi's vision.

The technical documentation for each of these is intended to be released over time, along with the code libraries.

Table of Contents

Executive Summary

Big data generation is increasing exponentially, driven by continued growth of internet usage, social networks, proliferation of smart phones, as well as the digital initiatives and structural reforms undertaken by the Indian government. At the same time, incidents of data crimes such as data hacks, data leaks, data tampering, identity thefts are on the rise.

High value data like land registry, educational documents, employment, transaction and health records etc. are required by individuals and organizations as part of their routine activities. However, the current mechanism of data exchange is mostly manual, paper based, slow and fraught with risks of tampering, forgery and thefts.

Recognizing the need and opportunity to enable with technology the enforcement of data protection regulations, Zebi has created a Blockchain driven, unique and holistic solution to make high value and sensitive data readily available for legitimate use. Zebi safeguards data against hacking and tampering, while obtaining consent from individuals.

Zebi has stood for Data security and has innovated at all levels in this space. This spans from core infrastructure, private blockchains, public blockchains and applications built on its own infrastructure, called zapps. In the past few years, Zebi has made a considerable mark in not only innovating in the blockchain ecosystem, but also going on ground to understand how these will be deployed to address gaps in all layers of this.

We have also worked on several other blockchain infrastructures to understand what is better than the other. All of this is reflected in the sheer number of monetized projects we have. We have built a culture of evolving our offerings in this brave new world and will continue to do so.

Zebi Public Blockchain Overview

Zebi mainnet is launched with the learnings that we have found to be the real game changers in blockchain adoption, apart from learning what others have done in the ecosystem.

One of the biggest learning outcomes is that it is almost impossible for each and every use case to be fit into a single public blockchain, as the needs of various use cases are different.

The core learnings and philosophies that have impacted the architecture of our mainnet are as follows:

- All data is created equal, but some are more equal than others: There are several types of data and the needs for securing each of them is different.
- Data Quality is in the Eye of the beholder: There are many players in the ecosystem, like creators, users, holders and partners, and their utility of the same type of data is different.
- To each his own, and mainnet for all: The governance around each of the subnets could be private or public, or possibly even hybrid.

Zebi mainnet characteristics:

- One chain to hold them all : The ZPB Mainnet, which holds the core Zebi Tokens
- One chain, for each type of Sub-Ecosystems - Zones, with different business objectives, which Zebi intends to roll out as use cases mature
- Zapps (That's Zebi Dapps), third party apps which reside on this ecosystem of the main and sub chains.
- Apart from this, Zebi has also equally invested into making the platform usable by creating libraries/ modules which can be used by third parties for quick integration, and building meaningful use cases.

Simply put, the eventual goal for ZPB is to operate one chain for speed, one for governance, one built to HIPAA standards and other features.

Zebi has Zebi token, a base utility token which will be used as mode of payment for all Zebi services, including transaction processing and data protection by Zebi platform.

ZPB Design Overview

Zebi intends to handle all data use cases on its platform. However, to achieve this, several technical innovations are required. This outlines the innovations we are currently addressing to achieve the desired goals. Zebi Public blockchain follows design philosophy that includes a modular architecture approach, interoperability, emphasis on high security solutions and development of APIs.

Given that COSMOS has already solved several of the problems that are in the vision of Zebi, ZPB has been forked from COSMOS.

ZPB addresses some of the common issues in public blockchains. In addition to the existing solutions, ZPB has taken unique approaches to tackle the issues in public blockchains, listed below:

Zebi Communication Protocol

The biggest challenge in public blockchains today is how one chain can interact with another. The logical separation of blockchains has been a long-standing problem. This is broadly referred to as the inter blockchain communication problem.

Zebi has taken a different approach to solve this problem. Zebi is currently building a communication protocol using SMTP as an underlying layer to achieve interaction between blockchains. This can be simply thought of as a Decentralized SMTP, on steroids.

This is being designed to not only solve the problem of blockchain interactions with ZPB Hubs and Zones, but eventually address all blockchains – both public and permissioned. A slightly more detailed approach note is in the following section.

Once built, this is slated to be one of the biggest innovations in the blockchain world.

ZAPP Modules

Zebi also believes that a successful project means that developers should be able to quickly build and deploy applications without having to build everything from scratch. Today a lot of third-party developers are apprehensive of choosing a platform due to the non-availability of sample applications, easily deployable modules, etc. This includes everything from libraries, modules, oracles, etc.

ZAPPs are Zebi Decentralized Applications, which are DAPPS of the ZPB ecosystem. ZAPPs don't need to be on mainnet but will be communicating with mainnet. One may compare this to early HTML like approaches to build websites, or a Wordpress like approach.

While this is a continuously evolving ecosystem, a few of these are outlined in the following sections.

Zebi also addresses some of the existing challenges in blockchain, either as a direct adoption of COSMOS or as enhancements to it. Some of the important ones are as follows:

Self-Amendment

Allows ZPB to upgrade itself without having to split ("fork") the network into two different blockchains. Because of self-amendment, coordination and execution, costs for protocol upgrades are reduced and future innovations can be seamlessly implemented.

Governance

All Validators can participate in governing the protocol. The election cycle provides a formal and systematic procedure for stakeholders to reach agreement on proposed protocol amendments. By combining this on-chain mechanism with self-amendment, ZPB can change this initial election process to adopt better governance mechanisms when they are discovered.

Open Innovation

Proposed amendments that are accepted by stakeholders can include rewards to individuals or groups that improve the protocol. This funding mechanism encourages robust participation and decentralizes the maintenance of the network. Fostering an active, open, and diverse developer ecosystem that is incentivized to contribute to the protocol will facilitate ZPB development and adoption.

Proof-of-Stake

Participants ("nodes") in decentralized, peer-to-peer networks provide the necessary computational resources that keep a network up and running. Proof-of-Stake (PoS) is the mechanism by which the various participants in ZPB reach consensus on the state of the blockchain. Unlike other PoS protocols, any stakeholder can participate in the consensus process in ZPB and be rewarded by the protocol itself for contributing to the security and stability of the network. Additionally, PoS is less costly than other consensus mechanisms and lowers the barriers to entry for involvement.

Delegation

In PoS, a security deposit is required to participate in the consensus process and avoid being diluted by inflation. As in proof-of-work, the consensus protocol relies on an honest majority for its security which is incentivized directly by the ZPB protocol by penalizing dishonest behavior and rewarding honest behavior. If a participant behaves dishonestly, they can lose their deposit. Users who do not wish to participate directly in the consensus protocol have the option to delegate their rights to other users to participate on their behalf.

Byzantine Fault Tolerance

Byzantine fault tolerance is another feature that has been built into ZPB through the use of Tendermint BFT, which is part of the COSMOS SDK.

ZPB – Technical Overview

Zebi Public mainnet Blockchain is a 3rd generation public blockchain platform after Bitcoin (1.0) and Ethereum (2.0) that is designed for organizations and enterprises to secure and tamper-proof their sensitive digital assets. It is a multi-asset and multi-chain public platform that links the assets of various organizations and enterprises to securely share, store, tamper-proof, and verify their sensitive digital assets.

Technically, ZPB is built on the COSMOS SDK that in-turn is built on Tendermint core blockchain software. ZPB comprises of in-house built additional modules in the COSMOS SDK that provide several services in the form of Zebi nodes as REST APIs. These services are in turn consumed by the client specific application called ZApps (from the traditional dApps) that can be easily built by any data provider.

ZPB uses the PoS (Proof of Stake) Consensus protocol to allow an individual to become a validator that requires staking in ZEBI tokens. Its in-built governance mechanism ensures true decentralization of blockchains and the associated nodes.

The functional Architecture of ZPB is shown in Figure 1. The layered architecture of ZPB allows for fine grained modular access control and customizations as per the needs of the application requirements right from the base Infrastructure layer to the front end ZApps - (short for Zebi DApps). Tendermint core is software for securely and consistently replicating an application on many machines. It consists of two chief technical components: a blockchain consensus engine and a generic application interface. The consensus engine, called Tendermint Core, ensures that the same transactions are recorded on every machine in the same order. The application interface, called the Application BlockChain Interface (ABCI), enables the transactions to be processed in any programming language. The Application State Machine, forked out of Cosmos-SDK is built on top of Tendermint Core. Cosmos is a decentralized network of independent parallel blockchains, each powered by BFT consensus algorithms like Tendermint consensus. In other words, Cosmos is an ecosystem of blockchains that can scale and interoperate with each other through its Inter Blockchain Communication Protocol (IBC). At its core, the SDK is a boilerplate implementation of the ABCI in GoLang. It comes with a multistore to persist data and a router to handle transactions. Zebid is a Zebi Mainnet node which runs a daemon comprises of this infrastructure layer.

Multi-Chain and Multi-token support in ZPB is envisioned to adapt to real world applications across various verticals.

It is with the creation and adoption of IBC that ZPB will be able to realize its purpose and vision of creating an ecosystem of Data Providers, Data Custodians and Data Requestors. Zebi intends

to apply this concept and technology across many verticals and domains such as Supply Chain, Educational Institutions, Health Care Providers etc. One of the key issues ZPB intends to solve is that of securely storing and sharing of data without compromising at all on Data Privacy and identity theft at scale (with increasing number of nodes in hundreds and even thousands) and with very high performance (throughput in tens of thousands) with minimal resources and cost. Towards this end, couple of approaches will be attempted including Heterogeneous Blocks in a Blockchain that make use of the ZIBP for inter-blockchain communication.

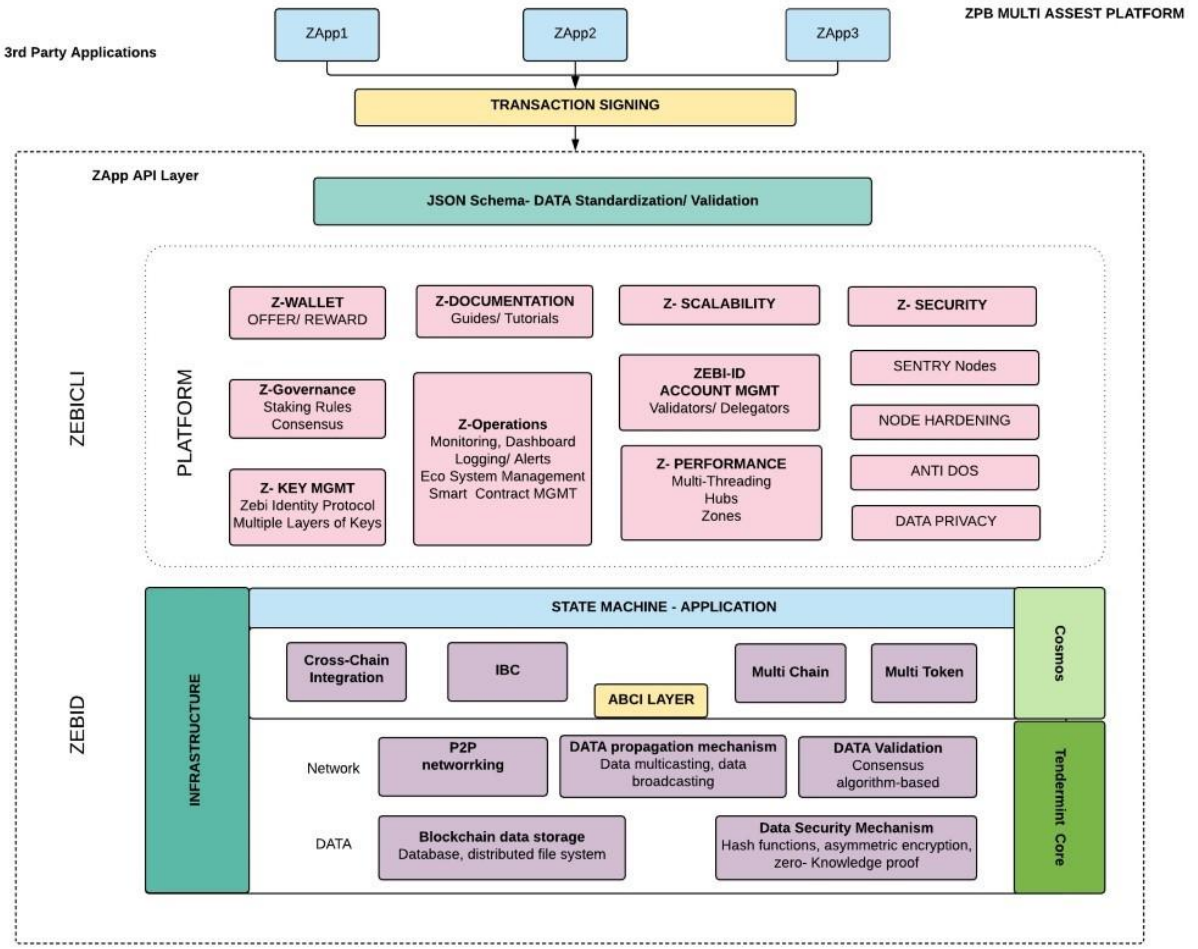


Figure 1. Functional Architecture of Zebi Public Blockchain (ZPB).

ZebiCLI is a Zebi Command Line Interface that also exposes several REST APIs at the Node. This layer supports the various modules that are required for a Public Blockchain,

- Z-Wallet: This is a web-based application that allows account creation in ZPB that comprises of a Public Key, 24-word Mnemonic and a Private key. UserID and Password are

required for 2 factor authentication. The generated Private key can be downloaded and stored as a Keystore file. It is the responsibility of the user to safely store the 24-word Mnemonic which can be used to retrieve the Private key just in case one loses their Private Key. But if Mnemonic itself is lost then Private key can never be recovered and the entire account might be lost or will be unrecoverable. Users can view their transactions, delegate/undelegate/re-delegate their tokens to any listed Validator.

- Z-Governance: This module allows changes to the application through a Proposal and Voting mechanism by all the Active Validators. Anybody can propose a change to the application and send out a proposal. Other Validators have to acknowledge and deposit a few tokens. Proposals are an item to be voted on. It contains the ProposalContent which denotes what this proposal is about, and the other fields, which are the mutable state of the governance process. Proposal Processing Queue is a queue containing all the Proposal IDs of proposals that reached Minimum deposit. At each EndBlock, all the proposals that have reached the end of their voting period are processed. To process a finished proposal, the application tallies the votes, computes the votes of each validator and checks if every validator in the validator set has voted. If the proposal is accepted, deposits are refunded. To prevent spam, proposals must be submitted with a deposit in ZEBI tokens. Voting period will not start as long as the proposal's deposit is smaller than the minimum deposit MinDeposit. When a proposal is submitted, it has to be accompanied by a deposit that must be strictly positive but can be inferior to MinDeposit. Indeed, the submitter need not pay for the entire deposit on its own. If a proposal's deposit is strictly inferior to MinDeposit, other ZEBI token holders can increase the proposal's deposit by sending a TxGovDeposit transaction. Once the proposal's deposit reaches MinDeposit, it enters voting period. If a proposal's deposit does not reach MinDeposit before MaxDepositPeriod, proposal closes and nobody can deposit on it anymore.

- Z-Key Management: This module will make it easy for the users of ZPB to manage their private and Public Keys. If their Private key is compromised or they have lost it, ZPB will provide a hierarchical set of Master Keys. There will be several levels of Keys (5 to begin with in the Order of lowest Level 1 to Level 5 (the highest Level of Master Key). In case Level 1 Key is lost, Level 2 key will override the Level 1 key and it will cease to work by itself. That way if anybody has gained illegal access to Level 1, the Master Key it will immediately cease to work the moment Level 2 key is activated or used. Similarly, if Level2 key is lost then it can be overridden by the next Level 3 key, and so on.

- Z-Operations: This is basically a support module for all Validator nodes that monitors the health of the VMs (CPU, RAM and Disk I/O) on which they are running and sends out timely alerts to keep the Validator node running at all times.

- Z-Security: Validator nodes need to be protected from malicious attacks such as DDoS. Though this can be achieved in multiple ways such as monitoring of the network traffic through 3rd Party subscription, it can also be achieved through the Sentry nodes architecture though it is kind of expensive. In this architecture basically the Validator node sits behind the sentry node

which is a non-validator node and both of them communicate through private network. It is the sentry node which runs on a Public IP. Since the Validator node is never exposed to a public network directly, even in the case of a hack or an attack it's only the sentry node that might be affected but NOT the Validator node.

Challenges addressed

Distributed ledger technologies (DLT) have the potential to disrupt and transform existing markets in multiple industries. ZPB address the problems of existing blockchain by combining best research results and engineering practice in an optimally tuned system. ZPB makes breakthrough in following aspects

The most compelling use cases for DLT require hundreds of thousands of transactions per second, and many require consensus latency measured in seconds. ZPB supports thousands of transactions per second and can have block time on the order of 1 second.

ZPB is secure and has a mechanism to hold its participants accountable for their actions. It is not only fault tolerant, its optimally byzantine fault-tolerant.

ZPB used POS algorithm for instant finality as long as less than 2/3 of validator are malicious.

ZPB is built on Cosmos and its token economics in general follows the rules set by Cosmos. Below table Explains the different parameters involved with ZPB Platform.

Parameter	**ZPB Platform – Zebi Token**
Number of Tokens at launch.	1 Billion, 625 Million Circulating
Target Stake Rate	66% of Circulating Supply
Maximum Number of Validators	Start with 125 Y1, then increase by 13% each year up to a max of 300
Inflation rate	7-20%; Max increase in rate is 13% YoY
Minimum Self Delegation	1 Zebi
Minimum Gas Fee	Set by Validator (Recommend 14 uZEBI)
Transaction Fee	Gas Fee*Gas; Gas fee set by Originator of Transaction
Block Proposer Bonus	5% if 100% votes
Initial Commission Rate	Set by Validator
Maximum Commission Rate	Set by Validator
Maximum Change rate of commission	Set by Validator
Network Tax	2% of txn fee
Slashing	5% for double signing; 1% for Downtime
Unbonding period	21 Days

Zebi Communication Protocol (ZCP)

Zebi Communication Protocol (ZCP) is a crucial protocol for Inter-Blockchain Communication to handle cross chain data transport, authentication and reliability.

Zebi Public Blockchain is built on Cosmos which is a network of many blockchains powered by Tendermint. While most existing public blockchains are based on "single Blockchain" with total global transaction ordering, Cosmos network uses a hub-and-zone model for interoperability where zones (independent blockchains) can transact with other zones by routing through a hub (also an independent blockchain). This protocol is called the IBC (Inter-Blockchain Communication) in Cosmos parlance which is a protocol for sending messages between chains to represent transactions.

The hub manages many independent blockchains called "zones" (sometimes referred to as "shards", in reference to the database scaling technique known as "sharding"). A constant stream of recent block commits from zones posted on the Hub allows the Hub to keep up with the state of each zone. Likewise, each zone keeps up with the state of the Hub (but zones do not keep up with each other except indirectly through the Hub).

IBC, in general is an end-to-end, connection-oriented, stateful protocol for reliable, optionally ordered, authenticated communication between modules on separate machines. IBC implementations are expected to be co-resident with higher-level modules and protocols on the host state machine. It handles authentication, transport, and messages relayed between modules on separate machines. The protocol is defined between modules on two machines, but designed for safe simultaneous use between any number of modules on any number of machines connected in arbitrarily topologies.

Zebi is working on unique and novel way of facilitating two-way communication between hub and zones using the time tested and reliable SMTP like messaging. Combining the Hub-and-zone architecture of Cosmos with the proposed SMTP-like messaging, the ZCP (Zebi Communication Protocol) is as depicted in Figure 1.

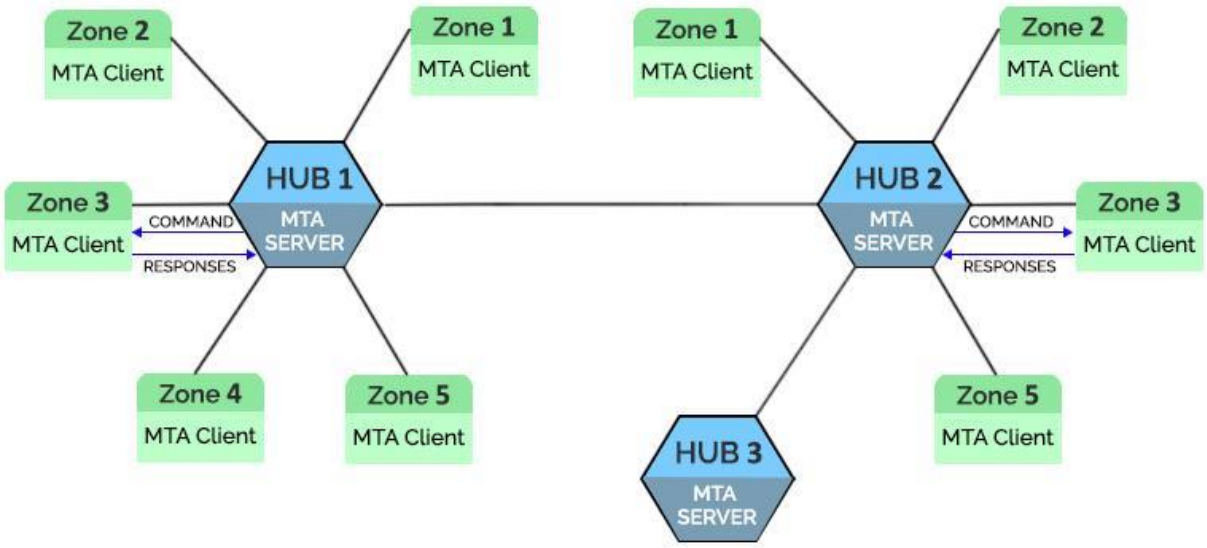


Figure 1. The combined architecture of Hub-Zones of Cosmos and the ZCP using the MTA (Mail Transfer Agent) Client and MTA Server components.

Like in SMTP, Message Transport Agent (MTA) client can be resident on each of the zones. Multiple such MTA Client components communicate with the nearest MTA Server that is resident on nearest Hub. Thus ZCP protocol logic can be suitably modified for the following attributes:

Authentication: Identification of the sender and receiver will be as per the attributes of the specific source Blockchain in a standardized domain specific manner.

- Message Relay: Message relay is built into the SMTP protocol and as long as the sender's and recipient's addresses (in the From: and To: parts of the message header) are defined in a standardized manner, mail relay agents relay the message hopping from one MTA server to another till the nearest domain of the destination To: address is reached.

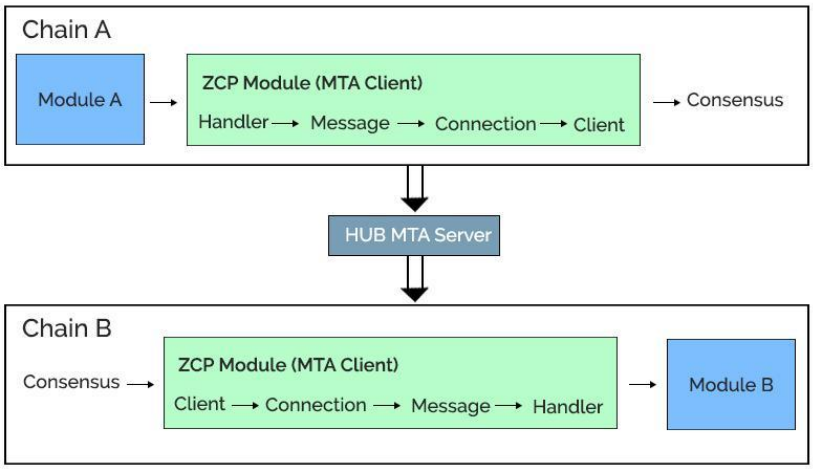
- Data Confidentiality & legibility: Minimum data necessary for correct operation of the ZCP is made available & legible (serialized in a standardized format) through the MDA (Message Delivery Agent) whose job is to receive messages from a local MTA and write them to disk in the proper format and the proper place, depending on the recipient. The relevant data can also be encapsulated in the message envelope's body section even with an attachment.

- Reliability: SMTP is time tested for decades and it is reliable and secure

- Statefulness: MTA client and server architecture is designed to handle multiple connections in a simple protocol that maintains and ensures state information about the blockchain that is embedded in the body of the message is maintained. The handshake

mechanism is well known through command and response exchange protocol between the MTA Client and MTA server (RFC 5321).

- Dataflow: ZCP can be conceptualized as a layered protocol stack through which data embedded in messages flows between two Chains A and B is as shown in Figure 2.



- On Chain A
  - Module (application-specific)
  - Handler
  - Message sent by the Sender
  - Connection with MTA Server
  - MTA Client
  - Consensus (confirms the transaction with the outgoing message)
- Hub
  - MTA Server Relays the message with embedded data
- On Chain B
  - Consensus (confirms the transaction with the incoming message)
  - MTA Client
  - Connection with MTA Server
  - Message Received by the Recipient
  - Handler
  - Module (application-specific)

ZAPP Modules

Zebi has built several IPs that can be directly used along with ZPB for quicker delivery of projects. Some of the modules are listed below. These are called ZAPPs, or Zebi Decentralized Apps, which are Dapps built on the Zebi Ecosystem.

Zero Knowledge Proof based Identity management system

When someone wants to verify the identity of an individual, the blockchain platform is queried with a verifiable claim, which will have the public identifier(such as Zebi ID) of the individual. The verifier gets a safe response verifying the claim. These verification works on zero-knowledge proofs methodology. This module also facilitates the subject of data to permit access to verifier on only specific part of the data.

Zero Knowledge Proof based data verification system

Zero-knowledge proofs let you validate the truth of something without revealing how you know that truth or sharing the content of this truth with the verifier. This principle is based on an algorithm that takes some data as input and returns either ‘true’ or ‘false’. This helps in verifying the data without actually revealing the full data.

MetaHash

One of the biggest challenges with ZKP is the possibility of brute force attacks in the case of formatted data/ metadata, where a prescribed pattern can be used to reverse engineer actual data. MetaHash allows the use of storing data on a chain without exposing these risks.

Proof of Trail

Query capability to get responses based on cross blocks data, unified with precedence rules applied, to return complete and semantically correct information. This query module superimposes various versions of the data in the blockchain, enabling tracking of events of an entity, to provide an immutable proof of trail. For example, this enables tracking asset ownership changes in Land Registry data.

Dynamic schema

Dynamic schema capability lets the platform efficiently store heterogeneous entities’ data that are added, in the transactions of the same block. Queries are enabled that will provide only the responses from the data pertaining to a single entity. The platform stores different structures of data without incurring a data model change. At the same time the solution is privacy preserving as the data is encrypted.

Multi-Tenancy

Multi-tenancy is an architecture in which a single instance of a blockchain network serves multiple customers, Zebi's blockchain platform is built so as to accommodate different clients with different data structures. Since each client's data is encrypted with respective private keys and hashing algorithms, the data cannot be read by other clients.

Key Management

Data in the blockchain is encrypted with state of the art 256bit encryption and stored on the platform. Even an extreme theoretical event like a malicious insider stealing a datafile doesn't cause data breach due to this encryption. There is no human handling of keys or sensitive data at any stage of the entire cycle. The encryption key is never persisted in the blockchain or in any of our systems. It is stored only with the individual. The platform's key management process meets or exceeds OWASP standards. When a data verification request is received, the data owner shall provide consent and key to decrypt and verify the data. As a different key is used for each individual, key shared by one client cannot be used to decrypt another client's data.

Oracles

An important aspect of blockchains and smart contracts is how we can bring data from the outside world into the blockchain. This is broadly referred to as oracles, or gateways/ mechanisms to bring points of truth on chain. Zebi is building several of these oracles to help plug into applications

Business Use Cases

This section provides examples where Zebi blockchain platform has clear and compelling use case.

One of the most valued features of blockchain is data immutability. Once the data is recorded on the Zebi blockchain platform, it cannot be modified or removed, providing integrity to the data. One of its use cases is to store vital document data on to the chain. ZPB allows verified institutions to easily create and publish document data on to the platform to provide data immutability. The Verification of the data happens from unaltered sources through ZPB to ensure authenticity and integrity, and hence non-repudiation of document is guaranteed. Zebi Platform secures the following kinds of records.

ZPB tracks assets as they move from manufacturing to deployment and eventually to disposal. The blockchain records the various life-cycle events of assets and the associated evidence. ZPB integrates directly with existing software allowing to share, audit and exchange information securely in a multi-party consortium. The ledger serves as a transparent system of record between all participants who are involved with the asset, which improves the data quality that traditional solutions struggle with.

A detailed roadmap of products is published from time to time.

Currently Zebi has the following products in the market:

Zebi Edu Chain

Zebi Edu Chain is a digital credential management solution that offers a full suite for storing, retrieving and verifying the data online for both students and universities. It allows people to streamline the workflow by using digital flows.

Zebi Doc Chain

Zebi Doc Chain allows verified institutions to store vital documents data on to the blockchain. It provides a platform for controlled issuance of both physical and digital documents – Digital token for physical document security and blockchain for enhanced digital security. Zebi Doc chain provides a platform to verify the authenticity of vital documents in secured and convenient way.

Zebi Asset Chain

Zebi Asset Chain is a fool-proof blockchain based solution that stores the property details and transaction data, making it immutable and tamper-proof. It Provides an ease to use interface for different stakeholders. It minimizes the ownership disputes, speedup the transaction process and improves buyer-Seller Confidence.

Zebi AI Chain

Zebi AI chain is an effective tracking system for hospitality industry. It is a comprehensive solution to manage the digital identity including the characteristics and persona of the customer. It also helps the government officials to report the criminal activities and maintain law and order.

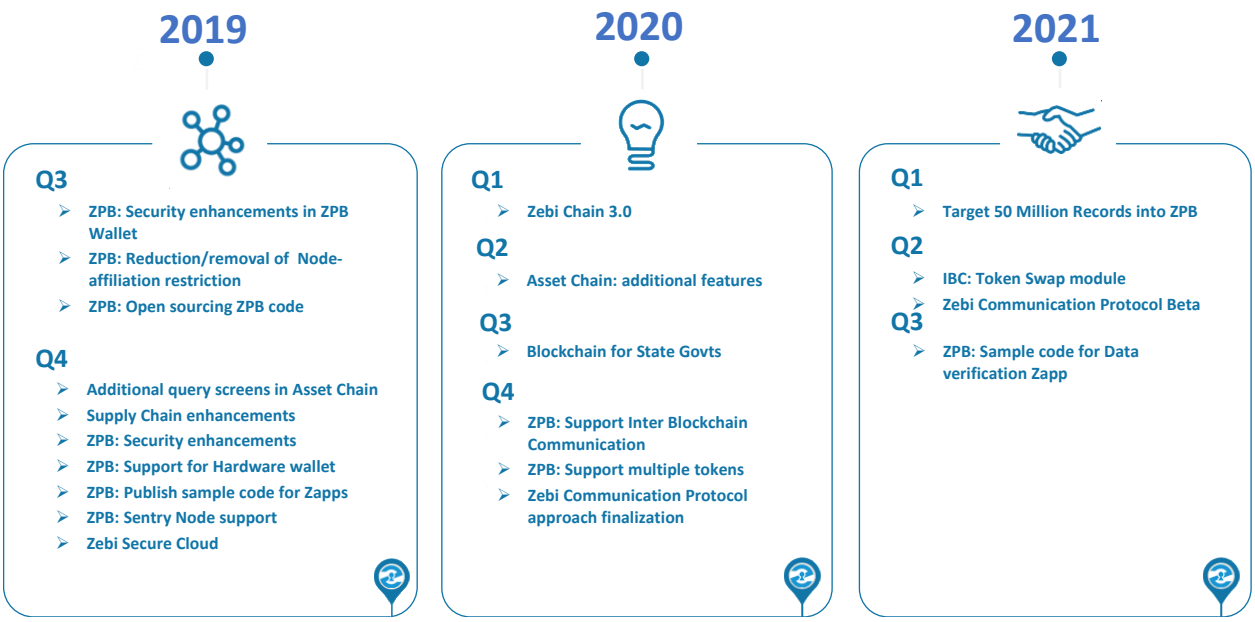
Zebi Secure Cloud

Zebi Secure Cloud is log management, collects logs from different providers and avoid log tampering by storing them cryptographically providing immutable log storage using distributed ledger technology. It Uses Machine learning and predictive analytics for log analysis and flag suspicious activities in real time crucial for fast, effective monitoring and reduce false positives

Zebi Tru Chain

Zebi Tru Chain is an asset tracking and management platform to track and provide transparency and history of the asset. It gathers and share key product information in a secure and trustworthy manner.

Below is the current roadmap for ZPB and its products. Please refer to website for latest and updated roadmaps.



Terms and Conditions

Disclaimer of Liability

To the maximum extent permitted by the applicable laws, regulations and rules, Zebi shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

No Representations and Warranties

Zebi does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, except as specifically set forth under this Whitepaper.

Representations and Warranties by You

This Whitepaper is solely for your information and may not be reproduced, disclosed or distributed to any other person, unless authorized by us. By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), or acting on it, you represent and warrant to Zebi and agree to be bound by the disclaimers, limitations and restrictions described herein, and in addition to the following:

(a) you agree and acknowledge that the ZPB Tokens do not constitute securities in any form in the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder;

(b) you agree and acknowledge that this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities which is registered with the appropriate regulatory authorities in the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder.

(c) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this Whitepaper, no action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules of the jurisdiction of which you are a citizen, resident (tax or otherwise) or green card holder have been complied with.

(d) the distribution or dissemination of this Whitepaper, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Zebi;

(e) you agree and acknowledge that in the case where you wish to purchase any ZPB Tokens, the ZPB Tokens are not to be construed, interpreted, classified or treated as:

(i) any kind of currency other than cryptocurrency;

(ii) debentures, stocks or shares issued by any person or entity

(iii) rights, options or derivatives in respect of such debentures, stocks or shares;

(iv) units in a collective investment scheme;

(v) derivatives of units in a business trust; or

(vi) units in a business trust;

(vii) any other security or class of securities.

(f) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology;

(g) you are fully aware and understand that in the case where you wish to purchase any ZPB Tokens, there are risks associated with Zebi and its business and operations, the ZPB Tokens, the Zebi Token Sale (each as referred to in the Whitepaper);

(h) you agree and acknowledge that neither Zebi is liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you; and rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(i) You are competent to contract i.e. in case of individuals, you are over eighteen (18) years of age, and in case of legal entities, you are duly authorized by such legal entity to act on its behalf.

(j) You are a U.S. “accredited investor” (as defined under the US Securities Act, Rule 501 of regulation D).

(k) all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession this Whitepaper or such part thereof (as the case may be).

No Advice

No information in this Whitepaper should be considered or construed to be business, legal, financial or tax advice regarding Zebi, the ZPB Tokens and the Zebi Token Sale (each as referred to in the Whitepaper). You should consult your own legal, financial, tax or other professional

adviser regarding Zebi and its businesses and operations, the ZPB Tokens, and the Zebi Token Sale (each as referred to in the Whitepaper). You should be aware that you may be required to bear the financial risk of any purchase of ZPB Tokens for an indefinite period of time.

No Further Information or Update

No person has been or is authorised to give any information or representation not contained in this Whitepaper in connection with Zebi and its business and operations, the ZPB Tokens, and the Zebi Token Sale (each as referred to in the Whitepaper) and, if given, such information or representation must not be relied upon as having been authorised by or on behalf of Zebi. The Zebi Token Sale (as referred to in the Whitepaper) shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of Zebi or in any statement of fact or information contained in this Whitepaper since the date hereof.

Restrictions on Distribution and Dissemination

The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to Zebi.

Persons to whom a copy of this Whitepaper has been privately distributed or disseminated, provided access to or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

Data Privacy and Security

Zebi is committed to ensuring that your data is secure. In order to prevent unauthorized access or disclosure, Zebi has put in place suitable physical, electronic, and managerial procedures to safeguard and secure your data.

All the data provided to us is stored in a secure computing environment protected by secure firewalls to prevent unauthorized access. The company controls access so that only people who need to access the purchaser data are granted access. All team members of Zebi are provided security training and are required to adhere to a comprehensive set of security policies, procedures, and standards related to their jobs.

When you use secure areas of the Zebi website, Secure Sockets Layer (SSL) protocol is used with 128-bit encryption. This means that all the information sent between your computers and the

Zebi secure computer environment is encrypted so that it cannot be read it in transit. Secure areas of the site have a time-out feature. If you leave a secure session inactive for some time, the site times- out to prevent unauthorized access.

It is possible that Zebi may be required by law, court order, or other legal process to provide information about our customers to outside parties, including for compliance purposes for regimes, such as the General Data Protection Regulation and the (Indian) Information Technology Act, 2000. It is the company's policy to ensure adherence to the due process of law in all such instances, and if required to provide information under these circumstances, the company will, whenever possible, attempt to inform users whose information has been requested, unless prohibited by law.

Zebi may also retain copies of personal information to comply with legal obligations, pursuant to the company's data retention policies, or for such reasonable period as is required to address potential disputes.

Zebi has developed privacy policies and practices that strive to protect the privacy rights of its users.

Country Specific Disclaimers and Restrictions

The ZPB Tokens are not intended to constitute securities in any jurisdiction. However, in the event a securities regulator were to take a contrary view that the ZPB Tokens constitute securities, this offering is also intended to qualify for exemption from registration in certain jurisdictions where this offer may be made:

United States of America

In the event this Whitepaper is being furnished to you in the United States of America (including Puerto Rico and the U.S. Virgin Islands), it is being furnished on a confidential basis and solely for your information and may not be reproduced, disclosed or distributed to any other person. You acknowledge and agree that the offer of ZPB Tokens in the United States is being made pursuant to Rule 506(c) of Regulation D of the US Securities Act, as amended and participation in the offering is limited to (i) U.S. "accredited investors" (as defined under the US Securities Act, Rule 501 of regulation D) considered "a safe harbour" for the private offering exemption of Section 4(a)(2) of the US Securities Act as amended and (ii) non-"U.S. persons" (as defined in Rule 902) in an offshore transaction in reliance on Regulation S of the US Securities Act. Further, you agree to be bound by the disclaimers, limitations and restrictions described under regulation D of the US Securities Act.

Singapore

In the event this Whitepaper is being furnished to you in Singapore, it is being furnished on a confidential basis and solely for your information and may not be reproduced, disclosed or distributed to any other person. By accepting this document, you (i) represent and warrant that you are either an "institutional investor" (as defined under Section 4A of the Singapore SFA), a

"relevant person" (as defined under Section 305 of the SFA), or persons to whom an offer is being made (as referred to in Section 305(2) of the SFA); and (ii) agree to be bound by the disclaimers, limitations and restrictions described herein.

The purchaser acknowledges that the offer of interests herein is made in reliance on the exemption(s) provided under Section 302B(1), Section 304, and Section 305 of the Singapore Securities and Futures Act (Cap. 289) ("SFA") and is not made in or accompanied by a prospectus that is registered by the Monetary Authority of Singapore and pursuant thereto the purchaser further acknowledges and unconditionally undertakes that the interests offered herein and accepted by the purchaser in accordance with the terms and condition herein shall not be subsequently sold to any person, unless the offer resulting in such subsequent sale is made in compliance with the SFA and/or in reliance on any applicable exemption(s) provided under the SFA.

Risks and Uncertainties

Project Risks

Prospective purchasers of ZPB (as referred to in this Whitepaper) should carefully consider and evaluate all risks and uncertainties associated with Zebi, the Zebi Blockchain Solution, the ZebiCoin and the Zebi Token Sale (each as referred to in the Whitepaper), all information set out in this Whitepaper and the Purchase Agreement prior to any purchase of ZPB. If any of such risks and uncertainties develops into actual events, the inherent utility of the Zebi Blockchain Solution and the ZPB could be materially and adversely affected.

Below are some illustrative risks associated with this Zebi Token Sale. This list is not meant to be exhaustive as the market and regulatory environment are quickly evolving.

Zebi Blockchain Solution Utility Risks

Security Risk

If our security measures are breached, or unauthorized access to data of our clients or their employees is otherwise obtained, our solution may not be perceived as being secure, clients may reduce the use of or stop using our solution adversely affecting the utility of the Zebi Blockchain solution.

Our solution involves the collection, storage and transmission of clients' and their employees' confidential and proprietary information, including personal or identifying information, as well as financial and payroll data. Unauthorized access or security breaches could result in the loss of information and utility, litigation, indemnity obligations and other liability.

Blockchain-based Zapps Market

If the Blockchain-based Zapps market develops more slowly than we expect or declines, our utility may slow or stall, and the Zebi Blockchain Solution could be adversely affected.

The Blockchain-based Zapps market is not as mature as the market for on-premise enterprise software, and it is uncertain whether Blockchain-based Zapps will achieve and sustain high levels of demand and market acceptance.

Blockchain-based solution volatility

Real or perceived errors, failures, or disruptions in the Zebi products and solutions could adversely affect our customers' satisfaction with our solutions and/or our industry reputation and The Zebi Blockchain solution utility could be harmed.

The Zebi products and solutions are very complex and have contained and may contain undetected defects or errors. The Zebi products and solutions are often used in connection with large-scale computing environments with different operating systems, system management software, equipment and networking configurations, which may cause errors or failures of products, or other aspects of the computing environment into which our products are deployed

ZPB

Absence of Rights

ZPB does not grant any rights, explicit or implied, in Zebi. ZPB is not a tool for owning any assets of Zebi.

Refund or Resale

Zebi is not obliged to redeem ZPB, or to otherwise refund their holders, for whatever reason. ZPB's value upon resale is not and will not be guaranteed, including their inherent value. Aside from that, a resale may be limited by laws and regulations that differ from the laws and regulations applicable to the ZPB holder. The resale market for ZPB may not be active.

Blockchain and Software

Processing of Smart Contracts

In the Bitcoin and Ethereum blockchains, block production can occur at arbitrary times, so there is a risk of untimely performance of smart contracts. The holder should be aware of this and consider its probability. The Bitcoin or Ethereum blockchains may not process a transaction at the exact moment the buyer expects it, and the buyer might not receive ZPB on the same day that it completes the necessary action.

Network Overload

The Bitcoin and Ethereum networks are subject to congestion, when transactions can be lost or delayed. Individuals and groups can deliberately congest entire networks, trying to gain an advantage.

Functionality

The Zebi Blockchain Solution may become obsolete or lose relevance due to the fast pace of innovations.

Security

Lost Private Keys

ZPB may be stored in a digital wallet or other storage requiring a digital key (or combination of keys). The loss of keys associated with a digital wallet or storage, will result in the loss of access to their balances. Additionally, a third party may get access to the private keys from the holder's wallet or storage, and, consequently, access to the ZPB Tokens they contain. Zebi is not liable for the losses that this may entail.

Zebi Infrastructure Security

Hackers or other bad actors may try to intervene in a smart contract, or otherwise interfere with aspects of how Zebi functions. These may include malware attacks, denial-of-service attacks, and other digital disruptions.

Connection of Open Cryptographic Keys

In the event that the ZPB holder does not provide access to connect open cryptographic keys to their account, it may cause a third party to incorrectly recognize the holder's ZPB balance in the Ethereum blockchain, while initial balances of a new Zebi blockchain are formed.

Cryptocurrency Wallet Incompatibility

A wallet or cryptocurrency storage system used by the holder must be technically compatible with ZPB. Failure to use a compatible technology may result in the ZPB holder not gaining access to their ZPB.

Zebi Development Third-Party Dependency

In the event that Zebi works with multiple third parties, Zebi exerts no control over the actions of the third parties themselves. The utility of the Zebi Blockchain solution may be severely hampered if there is a failure on the part of the third parties in performing the tasks agreed upon. There is no guarantee that these third parties will do their job properly.

Development Team Dependency

This project exists as the result of effort by the Zebi team, who are responsible for maintaining the competitiveness of the ecosystem overall. To lose members of the management team (or to fail to attract and retain additional staff) could have a significant adverse impact on Zebi and the Zebi Blockchain solution. The competition for staff with relevant experience is high due to the small number of qualified specialists. This shortage of personnel seriously affects the ability to

attract additional qualified management, which may have a significant negative impact on the Zebi Blockchain solution.

Interest in the Zebi Blockchain solution

The success of the Zebi Blockchain solution depends on the continued interest and participation of third parties. Their interest cannot be guaranteed.

Third-Party Projects

The Zebi Blockchain solution can prompt creation of alternative projects promoted by non-affiliated third parties.

Zebi's Activities

Conflict of Interest

Zebi's units may be involved in transactions with affiliated entities. Conflicts of interest may arise within Zebi or between Zebi and affiliated parties. Transactions with related parties may fail to comply with the arm's length principle.

Emerging Markets

Zebi (or its units) can operate in the emerging markets countries subject to high risks, including significant legal, economic and political risks.

Government

Immature Regulatory Framework

Developments in regulations around the world may alter the nature of our utility or restrict the use of blockchain assets or the operation of a blockchain network upon which we rely in a manner that adversely affects the Zebi Blockchain solution's utility

As blockchain networks and blockchain assets have grown in popularity and in market size, federal, state and international agencies have begun to take an interest in, and in some cases, regulate their use and operation. In the case of virtual currencies, regulators have created new frameworks or have published guidance as to how existing regulatory frameworks apply to virtual currencies.

Regulators globally, including, but not limited to, Canada, China, Australia, Brazil, India, Singapore, and South Korea, have issued some form of guidance regarding their position on initial coin offerings and token sales. Our utility and the use of ZPB could be adversely affected by depending on whether and how a given regulatory agency decides to exert authority over a blockchain network.

Zebi may stop distributing coins, developing the Zebi Blockchain solution, or its activities in a specific jurisdiction in the event that such actions are found to be illegal, or legislative changes make them economically impractical.

Licenses and Permissions

Although, as of the date hereof, there are no statutory requirements for Zebi or ZPB holders to obtain any licenses or permissions for operations with digital assets, there is a risk that such requirements will be introduced in the future. Regulatory authorities may establish requirements for cryptocurrency traders, including requirements for compliance with various standards, getting licenses, identification, reporting, and the like. In this case, an exchange trading in ZPB could be suspended for an indefinite period.

State Regulation

Zebi operates in a new industry and may be subject to increased supervision and control. Withdrawal or amendment of regulatory authorizations with respect to all or part of the activities carried on by Zebi or with respect to the fitness and propriety of one or more individuals to perform their current roles (including any of the Directors) might oblige Zebi to cease conducting a particular type of activity, or modify the manner in which it is conducted.

Zebi's property and operations are regulated by various public authorities and are subject to annual inspections. An inspection may conclude that Zebi has violated laws, decrees, or regulations, and cannot refute these findings or rectify the violations in a timely manner.

The failure by Zebi to obtain prior regulatory authorization in a jurisdiction where it has operated or the refusal of a regulator to grant that authorization in a jurisdiction where it may wish to operate could prevent Zebi from maintaining or expanding the Zebi Blockchain solution. Failure to comply with the applicable laws or orders resulting from the inspections can lead to significant penalties, ranging from fines to administrative or criminal prosecution of Zebi's officials.

Actions of Public Authorities

Sometimes public authorities show a high degree of freedom. Under the influence of commercial or political considerations, they act selectively, arbitrarily, without prior notice, or in a manner contrary to the law. This creates risks for Zebi's operations. Furthermore, such conditions allow competitors to gain various privileges and preferences from public authorities, equating to direct competitive advantages.

Privacy Concerns

Privacy concerns and laws or other domestic regulations may drive the adoption of the ZEBI Blockchain solution but at the same time may reduce its effectiveness. Our applications require the storage and transmission of the proprietary and confidential information of our clients and their clients, including personal or identifying information, as well as their financial and payroll data.

A wide variety of domestic and foreign laws and regulations apply to the collection, use, retention, protection, disclosure, transfer, disposal and other processing of personal data. These

data protection and privacy-related laws and regulations are evolving and may result in regulatory and public scrutiny and escalating levels of enforcement and sanctions. In India, there exists no formal data protection laws and is currently governed by specific sections (43A, 65, 69 and 72A) under The (Indian) Information Technology Act, 2000. The regulations surrounding data protection is bound to change with the impending Data Privacy Act to be implemented by the Indian government in the months to come.

In addition to government regulation, privacy advocates and industry groups may propose new and different self-regulatory standards. Because the interpretation and application of privacy and data protection laws are still uncertain, it is possible that these laws may be interpreted and applied in a manner that is inconsistent with our existing data management practices or the features of our solution.

All of these legislative and regulatory initiatives may adversely affect the ability of our clients to process, handle, store, use and transmit demographic and personal information from their employees, which could reduce demand for our applications.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).