Elisia

November 2018

WHITEPAPER
Version 1.3

TABLE OF CONTENTS

LEGAL DISCLAIMER

This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of Token Sale or Initial Coin Offering like the one described in this Whitepaper is prohibited or restricted.

This Whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by Elisia to purchase any ELSA tokens or give any help in any investment decision.

The investor must conduct their own due diligence to ensure that they comply with all local laws regarding cryptocurrency, tax, securities and other regulations in their jurisdiction.

The Elsa Token Sale may in the future be subject to further regulation. Refunds are not permitted. Sales will be final once transacted.

ABSTRACT

A business may have developed a Dapp on a blockchain platform, but instability of that platform or discontinuation of the said blockchain should not be a detrimental factor for the said Dapp.

A business can migrate from one Blockchain platform to another blockchain platform with a single click or few minor adjustments.

We propose a blockchain platform (Elisia), which itself is a Dapp platform having the ability to build a Dapp for any existing blockchains and allow migration of Dapps from one blockchain platform to another with a single click.

This paper outlines the context, vision and software architecture underlying Elisia, which we are building to serve a broad and diverse group of users and blockchains.

EXECUTIVE SUMMARY

In 2018 almost everyone has heard the words Bitcoin, Blockchain or cryptocurrency, but how many people are using Blockchain technology for building solutions for their businesses or personal use? Only a handful people use the real power of blockchain solutions to either build payment solutions or to deploy a Dapp for the purpose of growing their business.

Vast number of businesses are still confused about which blockchain to adopt for building their Dapps? They are either unsure about the transaction fees, sustainability of the blockchain platform, doubts over the team building the blockchain, etc.

At Elisia we propose a blockchain solution, which synchronizes all of the blockchain development platforms in a common platform and provide a unified interface to develop and deploy the blockchain based public and private applications on a master chain (Elisia) or sub chains like other Dapp building platforms with a single click or minor adjustments.

Elisia blockchain is a delegated proof of stake (DPOS) chain with the side chains comprising of different algorithms like proof of stake (POS), proof of work (POW), delegated proof of stake (DPOS), etc.

INTRODUCTION

Elisia is a new cryptocurrency based on its own unique Blockchain technology. Elisia provides lightning fast, free transactions and enables users to easily create free DAPPS and the ability to create their own cryptocurrency with the click of a button!

Elisia has been designed with 4 pillars of strength:

1. Speed
2. Free
3. Security
4. Simplicity

The industry has been waiting for Elisia.

Now the time has come!

FEATURES OF ELISIA

Speed:
Each Elisia transaction reaches itsdestination at lightning speeds!

Free:
Elisia transactions are 100% free for sender and receiver!

DAPPS:
Users can create DAPPS with little to no technical knowledge!

THE ELISIA TEAM

Tony Smith
CEO

Andrey Shypunov
COO

Yogesh Padsala
CTO

Sohailul Alam
Marketing

Mohd Irbaz Hussain
Marketing

ELISIA

The market will always remain competitive for all products/services and blockchains are no exception. There is ever growing competition between blockchains to come out with better solutions either in the form of new project or hard fork of an existing project.

Some projects focus on security, some focus on speed and some focus on the multiple usages of the platform. Different blockchains target different sets of user groups; ie Ripple's main user groups are financial institutions, Tron's main user groups are social/entertainment channel users, Ethereum's main user groups are token builders, etc.

With blockchains, we come to consensus over a block of transactions, such that no transaction conflicts with any other, neither in this block nor prior blocks. However, with the emergence of different blockchain platforms, neither a single blockchain developer nor a blockchain user is arriving at a consensus over using a blockchain platform for building their Dapps. Apart from this existing blockchain platforms are burdened by large fees and limited computational capacity that prevents the widespread blockchain solution adoption by businesses.

Each and every business wants to develop a Dapp on such a platform, which provides the lightning fast transaction speed with security and zero fees along with providing an option to migrate from one block-chain app development platform to another as per their business vision and need.

THE PROBLEM

Every blockchain is plagued by either of two problems:

1. Interaction with Other Blockchain: There are currently 2,000+ different coins and tokens in existence as per the CoinMarketCap data. However, not a single blockchain platform allows migrating of one blockchain to another blockchain as a fully functional sidechain. This problem creates a doubt over the sustainability of a blockchain developed by small group of members or unknown group. It also restricts the blockchain to reach its full value potential. Over the period of a time the blockchain becomes dysfunctional and results in wastage of monetary, infrastructure and other resources.

e.g. Trig token by the Blocksafe Foundation. Trig Blockchain's aim was to resolve the problem around licensing and usage of arms/ammunitions globally. Trig token was listed on only one exchange Binance with a Market cap of $10,400,663. The moment Binance announced the delisting of Token the market value dropped by almost 60% to $3,747,663 in 2-3 trading sessions.

What was the reason behind such a massive fall in price? It was the inability of the Blocksafe Foundation to migrate the Trig token to their separate Blockchain in a given time.

Imagion the situation of a business, who has developed a Dapp on platform like Trig. The instability of their main network, will cost a fortune to the said business and the business will be forced to develop the Dapp from scratch to another blockchain platform.

2. Wide spread adoption: While a number of blockchain platforms have struggled to support functional decentralized applications, application specific blockchains such as the BitShares decentralized exchange and Steem social media platform have become heavily used blockchains with tens of thousands of daily active users. They have achieved this

THE PROBLEM

by increasing performance to thousands of transactions per second, reducing latency to 1.5 seconds, eliminating per-transaction fees, and providing a user experience similar to those currently provided by existing centralized services.

But the real question is how many existing developers have started building their applications using aforesaid blockchain architecture whether for file sharing or for social media or for anything else?

Blockchain is known for its security. Almost everyone understands that a decentralized application cannot be hacked and most of them are equipped with Byzantine fault-tolerant system, still how many cryptocurrency exchanges are decentralized exchanges?

The problem with existing blockchain application development platforms is either they don't allow migration of apps over one blockchain to another platform with a single click or minor fixes or they don't come with a pre-defined tool set to develop an application.

QUANTUM RESISTANCE

While Elisia works on the principal of a DPOS, it is secured against the threat of quantum computing. However, Elisia's sidechain network adopts various kind of protocols like Proof-Of-Stake, Proof-Of Work, etc. which are not secured against the threat of quantum computing.

To protect the Elisia's Main chain from being corrupted by the side chains, for a security measure we have decided to introduce the quantum resistance ledger system.

INTRODUCTION TO WINTERNITZ OTS+ ALGORITHM

Buchmann introduced a variant of the original Winternitz OTS by changing the iterating one-way function to instead be applied to a random number, x, repeatedly but this time parameterized by a key, k, which is generated from the previous iteration of fk(x).

This is strongly unforgeable under adaptive chosen message attacks when using a pseudo random function (PRF) and a security proof can be computed for given parameters. It eliminates the need for a collision resistant hash function family by performing a random walk through the function instead of simple iteration.

Huelsing introduced a further variant W-OTS+, enabling creation of smaller signatures for equivalent bit security through the addition of a bitmask XOR in the iterative chaining function. Another difference between W-OTS(2011 variant)/ W-OTS+ and W-OTS is that the message is parsed log2(w) bits at a time rather than w, decreasing hash function iterations but increasing keys and signature sizes.

Introduction to XMSS

The extended Merkle signature scheme (XMSS) was first reported by Buchmann et al. in 2011 and was published as an IETF draft last year. It is provably forward secure and existentially unforgeable under chosen message attacks with minimal security requirements: a PRF and a second pre-image resistant hash function.

The scheme allows extensions of one-time signatures via a Merkle tree with a major difference being the use of bitmask XOR of the child nodes prior to concatenation of the hashes into the parent node. The use of the bitmask XOR allows the collision resistant hash function family to be replaced.

SECURITY MEASURES

In the design of the ledger it is important that the cryptographic security of the signature scheme is secure against classical and quantum computing attacks both in the present day and also future decades. XMSS using SHA-256, where w = 16, offers 196-bit security with predicted safety against brute force computational attack for hundreds of years.

An extensible stateful asymmetrical hypertree signature scheme composed of chained XMSS trees is proposed. This has the dual benefit of utilizing a validated signature scheme and allowing generation of ledger addresses with the ability to sign transactions avoiding a lengthy precomputation delays seen with giant XMSS constructions. W-OTS+ is the chosen hash-based one-time signature in the scheme for both security and performance reasons.

BLOCKCHAIN PARAMETERS

DPOS System Architecture:

Elisia will launch its main net with 51 block producers authorized to process the transactions. For consensus building the block producers are elected into a round of 51, each producer gets one block per round, and is rewarded for the validation of incoming transactions and production of the block of transactions. A block released by one producer is validated by the next and the next and so forth; if not validated, it is not built upon.

A block that is accepted by a quorum of producers is declared immutable, and the chain of immutable blocks becomes in effect a checkpoint. Like proof of work, producers can censor (ignore) messages, or they can front-run by introducing their own from their superior knowledge of the future.

GOVERNANCE IN ARCHITECTURE:

To provide transparency in block producer selection and their governance over bad acts by producers, each round of producers is continuously elected by the community using proof of stake (PoS).

Block Production:
Bitcoin has a time between blocks of roughly 10 minutes, but with natural variance this can on occasion lead to fairly long periods before the next block is mined. Newer ledger designs such as Ethereum have improved upon this and benefit from a much shorter block-times (15 seconds) without the loss of security or miner centralization from high rates of orphan/stale blocks.

Elisia will have a block production rate of 5 seconds

ELISIA ROAD MAP

KYC (KNOW YOUR CUSTOMER)

The KYC (Know Your Customer) process is very simple. You must submit 2 forms of identification:

1. Photo Identification
2. Address Confirmation

The name must be the same on each document. This is an effort to confirm the identity of investors and to also rule out investors from restriction countries.

WHITE-LISTING

Only white listed addresses will be accepted by our smart contract. This means that only members who have submitted KYC documents and been approved will be able to participate in the Elisia ICO.

Each white listed address is added to the smart contract manually. This will ensure that their is no possibility of an investor from a restricted country or non-verified member participating in the Elisia ICO.

We take our legal obligations seriously!

ELSA TOKEN SALE DETAILS

ICO Start Date:
November 30th 6am GMT

Soft Cap:
5000ETH

Hard Cap:
50000ETH

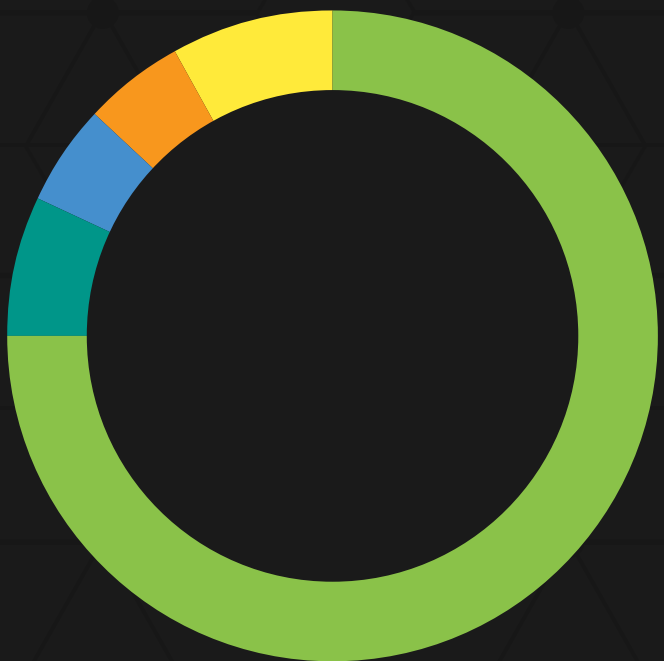
Token Price:
0.0001ETH

TOTAL SUPPLY:
1,000,000,000 ELSA

CONTRACT ADDRESS:
0x96c9126ee53fe08cc28fb08248915c76af3e3568

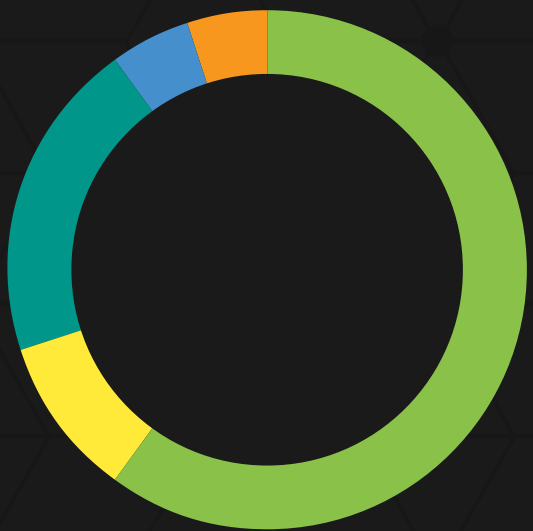
ELSA TOKEN ALLOCATION

- **Token Sale:** 750,000,000 ELSA (75%)
- **TEAM:** 70,000,000 ELSA (7%)
- **AIR DROP:** 50,000,000 ELSA (5%)
- **BOUNTY:** 50,000,000 ELSA (5%)
- **RESERVED:** 80,000,000 ELSA (8%)



ALLOCATION OF RAISED FUNDS

- DEVELOPMENT: 60%
- EXCHANGE LISTINGS: 10%
- MARKETING: 20%
- LEGAL: 5%
- OPERATIONS: 5%



RESTRICTED COUNTRIES

The following countries are restricted. Investors who are citizens of the following countries cannot participate in the Elisia ICO:

China, Bangladesh, Nepal, Macedonia, Ecuador, Pakistan, Algeria, Morocco.

CONCLUSION

Elisia is neither just a cryptocurrency nor a blockchain app development platform. It is a decentralized ecosystem. By building the Elisia platform on top of a highly secure blockchain, integrating the mixture of different technologies, Elisia aims to provide a user-friendly platform to increase user adoption of blockchain technology as a whole.

Blockchain Bridge: To increase the reach of the Elisia platform, Elisia bridges together useful blockchains through the use of our technology and allows the migration of one blockchain based Dapp to another blockchain Dapp platform or Elisia platform with a one click or few minor fixes.

Wide Adoption: Competing with businesses such as eBay, Uber, AirBnB, and Facebook, require blockchain technology capable of handling tens of millions of active daily users. In certain cases, an application may not work unless a critical mass of users is reached and therefore a platform that can handle very large numbers of users is paramount. Elisia aims at resolving this problem by creating a DPOS network on the top of small POS, POW networks.

Free Usage: Application developers need the flexibility to offer users free services; users should not have to pay in order to use the platform or benefit from its services. A blockchain platform that is free to use for users will likely gain more widespread adoption. Elisia is free to use in restrictive terms.

Quantum Resistance: Blockchain technology still uses the same cryptographic building blocks that are at risk to quantum computer assault. More specifically, blockchains rely on ECC – Elliptic Curve Cryptography – for authentication which can be broken by future quantum computers. Elisia's smart hash generation system prevents the quantum computing attacks for hundreds of years into the future!

Elisia is aimed at becoming the game changer for the Blockchain industry and creating a revolutionary application building experience for businesses as well as developers with zero fees.