SETOKEN

Social Environment Technology

SETOKEN WHITEPAPER

www.SETOKEN.eu – decentralized blockchain-based identity storage

SETOKEN

Legal considerations, Risks and Disclaimer

YOU MAY LOSE ALL MONIES THAT YOU SPEND PURCHASING SET TOKENS.
In the event that you purchase Tokens, your purchase cannot be refunded or exchanged.

THERE IS NO GUARANTEE THAT THE UTILITY OF THE SETOKEN PLATFORM OR THE PROJECT ENVISAGED IN THIS WHITE PAPER WILL ACTUALLY BE DELIVERED OR REALISED.
THE TOKENS YOU PURCHASE DO NOT ENTITLE YOU TO ANY OWNERSHIP OR OTHER INTEREST IN SETOKEN. THEY ARE MERELY A MEANS BY WHICH YOU MAY BE ABLE TO USE OUR SETOKEN PLATFORM THAT IS YET TO BE DEVELOPED. THERE IS NO GUARANTEE THAT THE SETOKEN PLATFORM WILL ACTUALLY BE DEVELOPED.
YOU ARE WAIVING YOUR RIGHTS BY AGREEING TO THESE TERMS AND CONDITIONS AND PARTICIPATING IN THE SETOKEN TOKEN-SALE. BY PARTICIPATING IN THE SETOKEN TOKEN-SALE YOU AGREE TO HAVE NO RECOURSE, CLAIM, ACTION, JUDGEMENT OR REMEDY AGAINST SOCIAL ENVIRONMENT TECHNOLOGY AND SETOKEN IF THE UTILITY OF THE SETOKEN PLATFORM OR THE PROJECT DESCRIBED IN THIS WHITE PAPER IS NOT DELIVERED OR REALISED.
IF YOU ARE UNCERTAIN AS TO ANYTHING IN THIS WHITE PAPER OR YOU ARE NOT PREPARED TO LOSE ALL MONIES THAT YOU SPEND PURCHASING SET TOKENS, WE STRONGLY URGE YOU NOT TO PURCHASE ANY SET TOKENS.

SETOKEN

INTRODUCTION

We, Social Environment Technology - SETOKEN, are believing in our vision to store your personal identifier data decentralized and secure on the Blockchain technology – encrypted in form of digital lockboxes.

Have you ever been the victim of identity theft? It is an ugly experience. Calling up credit card companies to change all your cards and dispute charges. Resetting passwords to all of your applications. Always worrying whether someone may call up your cell phone provider with your leaked information to commit a SIM porting hack, meaning they would have access to all of your text messages. Once someone has access to your texts this is the gateway to getting into many online services, even if you were being diligent and using two factor authentications.

Our user names, passwords, and personal information are being stored on centralized corporate servers, many of which remain ripe for the picking, despite the attention on this class of problems over the last several years. Once your personally identifying information genie is loose, it's extraordinarily difficult to put it back in the bottle.

Ideally the only risk you should have when it comes to managing your digital identity is whether or not your personal systems have been compromised, instead of worrying about every corporation you've ever dealt with in the past. In the offline world, you update your proof of identity every few years, receiving a driver's license, ID card, or maybe a passport if you travel internationally. When you go to a club, they check your age on your ID.

So how do we get from an insecure, centralized information model to a decentralized authentication model like how we interact in the real world? The answer is a combination of cryptographic hashing and blockchain technology.

This is where our Proof of Identity protocol-based platform comes to save you.

The decentralized and secure platform with authentication model stores your personal identifier data and there is one person who gives permission to access: YOU.

SETOKEN

CONTENT TABLE

SETOKEN

1. Key facts

For most of us, giving out personal information like our home telephone number or driver's license number is an everyday occurrence. Something we do with every check we write or online order we place. But do we really know what happens to that information once it leaves our hands? This paper provides a discussion on theexpansion of a crime that feeds on the inability of consumers to control who has access to sensitive informations and how it is safeguarded: identity theft.

It's time to keep an eagle eye on your finances.

Some 15.4 million consumers were victims of identity theft or fraud last year, according to a new report from Javelin Strategy & Research. That's up 16 percent from 2015, and the highest figure recorded since the firm began tracking fraud instances in 2004.

"All of the underlying types of fraud we measure are up," said Al Pascual, a senior vice president and research director for Javelin.

Card-not-present fraud — transactions made online or via phone where the cardholder does not need to present the physical card to complete the purchase — jumped the most, increasing 40 percent compared to 2015. Account takeover fraud — where thieves used stolen login information to access a consumer's accounts — rose 31 percent, and instances where fraudsters opened new accounts in a consumer's name were up 20 percent.

In all, thieves stole $16 billion, the report found — nearly $1 billion more than in 2015.

What is Identity Theft, anyway?

“Identity theft and identity fraud...refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data...”

- US Department of Justice, Criminal Division, Fraud Section report.

Identity theft is when someone takes your personal information like your name, address, social security number and mother’s maiden name — and uses it to establish unauthorized credit and charge items in your name. And finding someone’s personal information has never been easier.

SETOKEN

2.0 BLOCKCHAIN TECHNOLOGY

Where did blockchain come from?

Although blockchain technology has only been effectively employed in the past decade, its roots can be traced back far further. A 1976 paper on New Directions of Cryptocurrency discussed the idea of a mutual distributed ledger, which is what the blockchain effectively acts as. That was later built upon in the 1990s with a paper entitled "How to Time-Stamp a Digital Document". It would take another few decades and the combination of powerful modern computers, with the clever implementation with a cryptocurrency to make these ideas viable.

In order to validate the blocks in the same manner as a traditional private ledger, the blockchain employs complicated calculations. That, in turn, requires powerful computers, which are expensive to own, operate, and keep cool. That's part of the reason that bitcoin acted as such a great starting point for the introduction of blockchain technology, because it could reward those taking part in the process with something of financial value.

Bitcoin ultimately made its first appearance in 2009, bringing together the classic idea of the mutual distributed ledger, the blockchain, with an entirely digital currency that wasn't controlled by any one individual or organization. Developed by the still effectively anonymous "Satoshi Nakamoto", the cryptocurrency allowed for a method of conducting transactions while protecting them from interference by the use of the blockchain.

How do cryptocurrencies use the blockchain?

Although bitcoin and the alternative currencies all utilize blockchain technology, they do so in differing manners. Since bitcoin was first invented it has undergone a few changes at the behest of its core developers and the wider community, and other alt-coins have been created to improve upon bitcoin, operating in slightly different ways.

In the case of bitcoin, a new block in its blockchain is created roughly every ten minutes. That block verifies and records, or "certifies" new transactions that have taken place. In order for that to happen, "miners" utilize powerful computing hardware to provide a proof-of-work — a calculation that effectively creates a number which verifies the block and the transactions it contains. Several of those confirmations must be received before a bitcoin transaction can be considered effectively complete, even if technically the actual bitcoin is transferred near-instantaneously.

This is where bitcoin has run into problems in recent months. As the number of bitcoin transactions increases, the relatively-hard 10-minute block creation time means that it can take longer to confirm all of the transactions and backlogs can occur.

With certain alt-coins, that's a little different. With Litecoin it's more like two and a half minutes, while with Ethereum the block time is just 10-20 seconds, so confirmations tend to happen far faster. There are obvious benefits of such a change, though by having blocks generate at a faster rate there is a greater chance of errors occurring. If 51 percent of computers working on the blockchain record an error, it becomes near-permanent, and generating faster blocks means fewer systems working on them.

2.1 BLOCKCHAIN SOLUTION FOR IDENTITY MANAGEMENT

As cybersecurity threats become increasingly prevalent and sophisticated, the case for blockchain technology as a way to secure and improve identity management grows stronger.

Blockchain can give people more proactive control over their data and make it more difficult for unauthorized users to exploit it.

Blockchain startups are exploring more decentralized data management systems by, in some cases, teaming up with financial services, technology, and government organizations to mitigate the risks of large-scale cyber-attacks and identity fraud.
They're also finding ways to give individuals, including the underserved, access to services that require valid identification and they're able to do that much more efficiently than current know your customer processes.

The blockchain is currently being tested in several use cases.

Blockchain as an identity management solution is still nascent when viewed broadly though a general technology perspective.

When viewed strictly in a blockchain context, identity management is one of the most immediate use cases.

It provides a promising opportunity to mitigate identity theft and fraud, and reduce costs and time spent on KYC processes.
At the same time, it also provides opportunities for refugees to start fresh, with access to jobs, banking, and other services.
Digital identity holders will be able to access services more efficiently and control how much of their data is shared.

While cybersecurity concerns are a real concern still, improved technology will build trust in this new way for people around the world to manage their identity.

3.0 DIGITAL IDENTITY

A digital identity is the body of information about an individual, organization or electronic device that exists online.

Unique identifiers and use patterns make it possible to detect individuals or their devices. This information is often used by website owners and advertisers to identify and track users for personalization and to serve them targeted content and advertising.

A digital identity arises organically from the use of personal information on the web and from the shadow data created by the individual's actions online. A digital identity may be a pseudonymous profile linked to the device's IP address, for example, or a randomly-generated unique ID. Digital identities are seen as contextual in nature since a user gives selective information when providing authentication information.

Examples of data points that can help form a digital identity include:

- Username and password
- Purchasing behavior or history
- Date of birth
- Social security number
- Online search activities, such as electronic transactions
- Medical history

Because a profile often includes aspects of a person's actual identity, digital identities come with privacy and security risks, including identity theft.

Pseudonymous profiles can also yield an individual's identity through cross-site data analysis.
While passports and licenses identify users in real life, the inclusion of such personally identifying information (PII) online may pose more risks than benefits for the user.

Several authentication and authorization systems have been explored, but there is still no standardized and verified system to identify digital identities.

SETOKEN

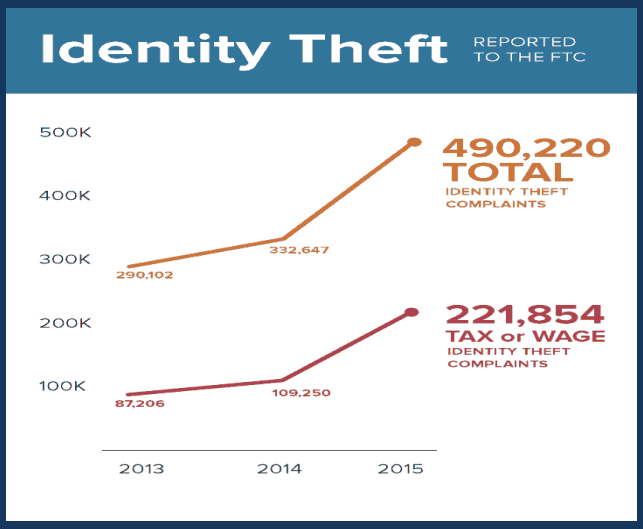
4.0 PREVENT IDENTITY THEFT / IDENTITY FRAUD

One of the most important aspects of personal security is identity theft protection. Just as you might take steps to protect your life, your home, your family, and personal property, you must also take steps to ensure that the only person who is using your identity is, in fact, you.

There is a lack of transparency in the type of protection that is advertised. First and foremost, identity protection must be transparent.

You might have seen advertisements for protection from identity theft, but you also assume that identity theft would never happen to you.

Unfortunately, this is the case. We are all subject to becoming a victim of identity theft.



Once identity theft occurs, it is extremely difficult to recover the information that cybercriminals have stolen.

Many times, you aren't even aware of how or when it happened.

That's why it's always better to take proactive security measures, that will prevent fraudsters from stealing your personal details and information.

It's easier to play it safe instead of only react once the damage is done and it's too late to keep it under control.

Blockchain enables the individual to gain greater security regarding their personal information without losing their privacy and paying further fees. Creating a distributed ledger containing everyone's identity distributes trust from a single central point towards the whole system.

A sovereign identity enables the individual to keep personal information under their control and share only when required. Individuals can choose to revoke the information after some time. The individual is now independent of a third party or government organization. Individuals can keep their privacy without risking identity theft.

In the past, to file for a loan, an individual would need to fill out personal information in their application, like their salary. With blockchain, an employer and the network could verify the individual's pay without revealing any personal information. Stealing someone's identity is therefore significantly harder when personal information is no longer widely available.

SETOKEN

SETOKEN

5.0 SET PLATFORM

We've built a platform…

…to securely and decentrally store your digital identity.

How do we get from an insecure, centralized information model to a decentralized authentication model like how we interact in the real world?

The answer is a combination of cryptographic hashing and blockchain technology - called SETOKEN.

SETOKEN platform stores your personal identifier data and also your digital identity data on the blockchain, encrypted in form of digital lockboxes.

Once someone has access to your digital data and texts this is the gateway to getting into many online services, even if you were being diligent and using two factor authentications.

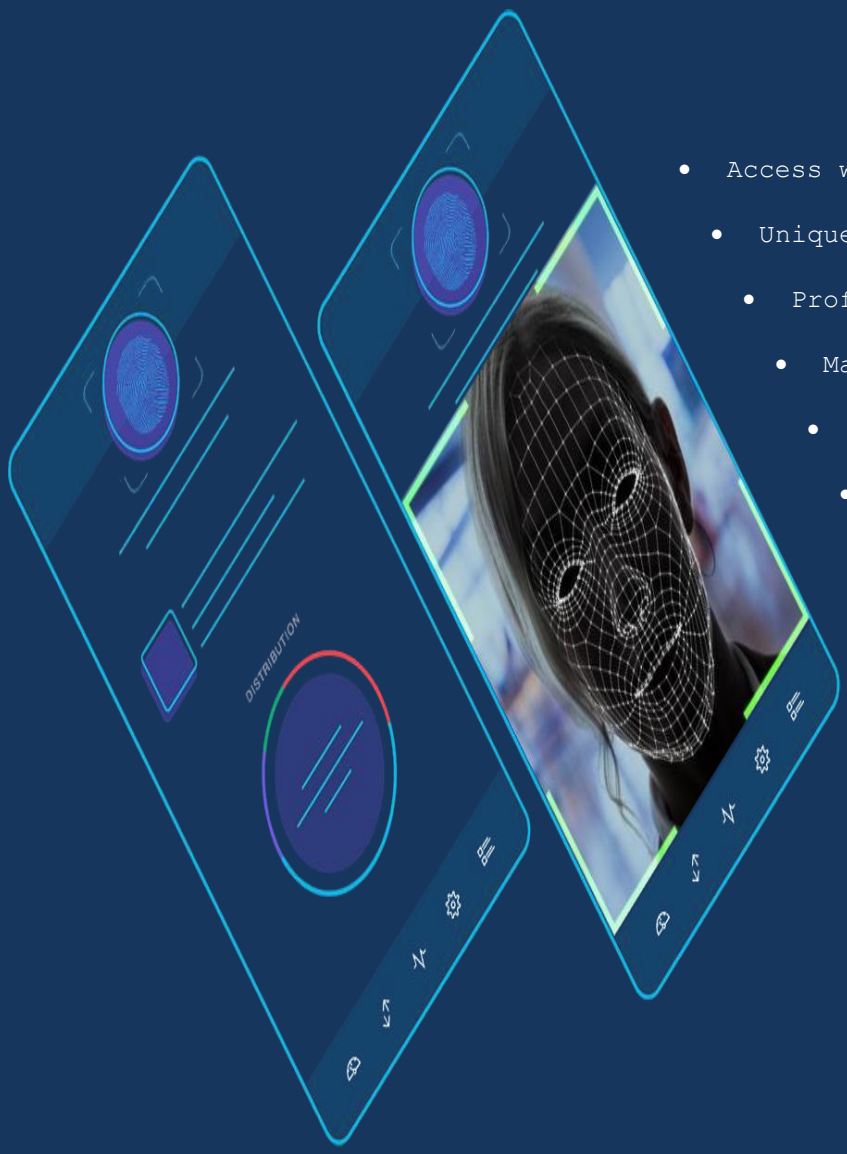
Imagine a world where you are in direct control of your personal information, a world where you can limit and control how much information you share while retaining the ability to transact in the world. This is SETOKEN.

SETOKEN

5.1 MOBILE APP

Once you've entered into our userdata platform, you can mange every thing.

You can verify yourself with your unique privateKey, as well as with your biometrical data like fingerprint and, **if technically completely safe**, face recognition and take control about your digital identiy.



- Access with privateKey and biometrical data
- Unique authentication model
- Professional ecosystem
- Manage your digital identity
- Instant access
- Token-based payment system

SETOKEN

SETOKEN

6.0 ICO
TOKEN-SALE

SETOKEN will be released on the basis of Ethereum platform (ERC20). It's compatibility of the token with third-party services wallets, exchanges etc, and provides easy-to-use integration.

Acceptable currencies

Ethereum ETH

Minimal transaction amount

To participate on Token Sale you must at least buy SET Tokens for minimum 0,1 ETH.

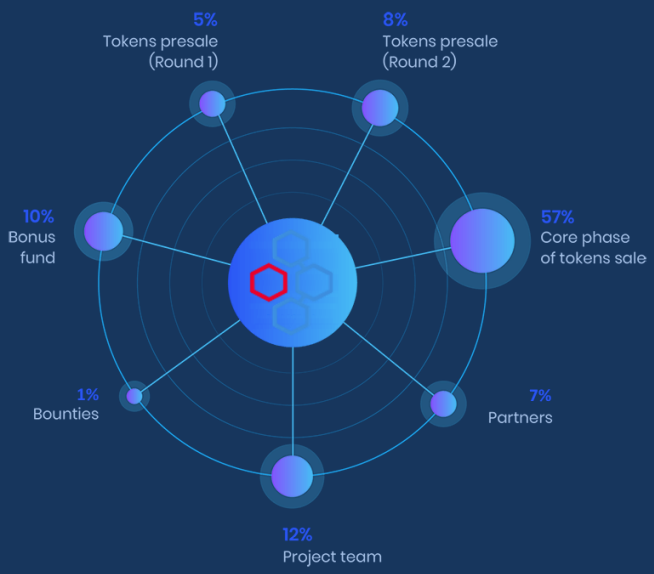
Tokens exchange rate

1 Ethereum, ETH = 40,000 SET

Number for tokens for sale

total for sale: 350,000,000 SET
total supply: 500,000,000 SET

Distribution of Tokens



Use of proceeds

6.1 TOKEN PRE-SALE

There will be two rounds of pre-sale.

1st round starts on Monday, 26th of March and ends on Friday, 25th of May.

In the first round there will be 25,000,000 SET Tokens (5% of total supply) for sale.
In this stage you can get the +40% early-bird bonus.

2nd round of token pre-sale starts in late Q2 2018, exact date will be:

Start: 18th of July
End: 30th of July.

In this round the amount of tokens for sale will be 40,000,000 SET (8% of total supply).
You can get an exclusive bonus for participating in this stage of 25%.

6.2 MAINEVENT TOKEN-SALE

Our Token-Sale Mainevent will start on 10th of September and ends on 22th of September.

At the Mainevent the amount of token for sale is 285,000,000 SET (57% of total supply).

By participating at the Mainevent you still can get a bonus of 15%.

7.0 ROADMAP


July 2017
Start of the SETOKEN vision.
October 2017
Alpha platform-launch
December 2017
SETOKEN ICO Website goes live
January 2018
Preparing for Token Sale
February 2018
Beta platform goes live (internal)
March 2018
Start Token Sale Round 1 & new website launch
Q2 2018
Start Token Sale Round 2
Q3 2018
Developing SETOKEN MobileApps
Q3 2018
Start Token Sale Mainevent
Q3 / Q4 2018
SETOKEN platform final launch
Q4 2018 / Q1 2019
SETOKEN MobileApps final launch

8.0 CONTACT

Website: www.setoken.eu

Email: info @ setoken.eu

Admin @ setoken.eu

Twitter: @SETech_official

Instagram: @socialenvironmenttechnology

MEDIUM Blog: @SETech

SETOKEN

SOCIAL ENVIRONMENT TECHNOLOGY

www.SETOKEN.eu – decentralized blockchain-based identity storage