Hybrid blockchain platform with a conscience

Whitepaper

Version 1.20 — Published on 14- jan - 2019

The Smilo platform was born from a spark of inspiration in June of 2017, when the founders of Smilo noticed some blockchain-based platforms were created with privacy and anonymity in mind, but none of these platforms could provide users with smart contracts and decentralised applications.

Smilo is different.

Introduction

Ethereum was initially proposed in 2013 in a white paper[1] by Vitalik Buterin, a cryptocurrency researcher and programmer. In the white paper, Vitalik Buterin described Ethereum as a public, open-source, blockchain-based computing platform featuring smart contract functionality. Since the release of Ethereum in 2015, several other projects have emerged which can also host smart contracts and decentralised applications, but these platforms are unable to host both anonymous and public smart contracts.

For mass adoption of blockchain technology, the Smilo team firmly believe that there must be a connection between a blockchain and its actual use cases. In order to ensure this connection, it is important to choose the best platform to connect with the use cases. Currently, there is no suitable blockchain-based computing platform for the medical sector, nor one that is an all-in-one solution for private escrow arrangements. All of the current smart blockchain-based computing platforms are public, but few people prefer their medical records or escrow arrangements to be public.

To address these shortcomings, what is needed is an open-source, hybrid, blockchain-based computing platform: one that features hybrid transactions, hybrid smart contracts, and hybrid decentralised applications. This is where the Smilo platform shines.

Summary

What is the Smilo platform?

Smilo is a unique blockchain platform which supports the combination of hybrid transactions, hybrid smart contracts, and hybrid decentralised applications — with 'hybrid' referring to both public and private. Smilo's intent is to use blockchain technology to create an alternative protocol for decentralised applications.

What is Smilo's unique selling point?

Smilo's unique strength stems from its combination of several features. The best affordances of the Smilo platform are the hybrid transactions, -smart contracts, and -decentralised applications. No other platform has yet to combine these features.

A combination of these features is very useful in many different scenarios, examples of which are explored further below.

Business overview

The core team of the Smilo platform consists of members with various specialities. In addition to the core team, the Smilo platform has access to over 200 developers to work for Smilo through freelance partnerships.

The leaders of the Smilo platform have over 30 years of business and IT experience.

Technical background

The intent of Smilo is to create a full-featured blockchain platform which hosts hybrid transactions, smart contracts, and decentralised applications. Smilo has been built in Golang, integrating some of the essential building blocks of Ethereum (e.g., Patricia tree, EVM, RLP, P2P and the account model) to deliver technical features that are tailored to deliver the intended benefits of the Smilo hybrid blockchain in terms of privacy, speed, security and scalability.

Token management

Two types of tokens will be driving the Smilo Platform:

- Smilo (XSM)
- SmiloPay (XSP)

The Smilo tokens are intended to act as a subscription model to be able to transact on the Smilo Platform as well as to allow its owners to have a stake into the future development of the network. The SmiloPay token is the transaction currency to be released to Smilo owners over time to be able to pay for service fees and upkeep of the Smilo Network.

Index

Smilo platform

What is the Smilo platform?

The Smilo platform is a decentralised hybrid blockchain platform – 'hybrid' meaning both public and private. This platform is the first of its kind to support the combination of hybrid transactions, -smart contracts, and -decentralised applications.

Smilo's intent is to use the blockchain to create an alternative protocol for decentralised applications. Smilo's unique strength derives from the combination of multiple features:

- Hybrid smart contracts
- Hybrid decentralised applications
- Hybrid transactions
- Transparency
- Privacy and anonymity
- Connection to real life applications

Hybrid smart contracts

One of the most significant features of the Smilo platform is the hybrid smart contract functionality, which allows for direct interaction between public and private smart contracts onto one decentralized chain. Other blockchain platforms provide their users with the ability to implement either private or public smart contracts. Meanwhile, the Smilo platform is the first, and currently only, platform to provide developers with the means to develop or deploy public as well as private smart contracts onto one and the same decentralized chain. This feature is specifically intended in any situation in which an individual is engaging with either a public or a private organization, exchanging sensitive information. Take the social funding sector for instance: Many people wish to donate their money to charity, but only if they know it will be spent responsibly by the NGO collecting it. Organisations which implement the hybrid technology offerings of the Smilo platform can show their benefactors the exact course of their donations through public smart contracts while using private smart contracts to keep open the option to donate anonymously.

For instance, Jacob loves nature, and he is very concerned about the ongoing climate change. Therefore, he wants to donate a significant amount of money to Greenpeace. However, Jacob does not want to publicly share the details of his donation, though he does want insight into the expenses of Greenpeace. Greenpeace can use Smilo technology to keep Jacob's personal donation private, whilst the expenses of Greenpeace are public, both

through the use of hybrid smart contracts. This hybrid process generates more transparency and trust in charities, and Jacob can anonymously donate money to his favourite causes.

Hybrid decentralised applications

Another great feature of the Smilo platform is the hybrid decentralised application option. Just as with hybrid smart contracts, hybrid decentralised applications offer usage possibilities to various applications for many different situations.

For a private and secure messaging app, for example, the Smilo blockchain network can host public messaging apps. However, some of the messages sent through the messaging app need to be private and secure. Therefore, it is very important that the Smilo platform can manage both private and public decentralised applications.

Hybrid transactions

Public transactions are completely transparent through Smilo, and they are visible through our blockchain explorer. On the other hand, when privacy and anonymity are required, we provide fully anonymous transactions that are both untraceable and non-linkable.

Transparency

In this new digitalised world, transparency is a way for many companies to (Re)gain consumer trust, as transparent operations overcome the perception of scams, overcharging, unnecessary and expensive intermediaries, and disuse of personal data.

With the inherent features of blockchain technology put in the form of mutual record-keeping in a near-irrevocable time-stamped ledger, we bridge the gap of the trust deficit, which otherwise would not be possible. Transactions can be executed significantly safer and more transparent than ever before.

The Smilo blockchain will be publicly available through the blockchain explorer. We see this explorer as a source of competitive advantage. Through this explorer transparency, efficiency and security are being warranted to all parties involved. It is the place where customers meet suppliers to validate their transactions, openly and transparently.

Privacy and anonymity

There are a number of successful platforms hosting smart contracts and decentralised applications, but none of these platforms have the ability to facilitate both public and private smart contracts and decentralised applications on one and the same decentralized platform. This is why we developed the Smilo platform. Smilo is able to make certain smart contracts, transactions and decentralised applications anonymous, if the user so desires.

Connection to real life applications

The team behind Smilo firmly believes that connections to actual use cases are critical for a successful blockchain platform. To ensure Smilo's connection with real-life applications, we want to link our platform to actual Use cases, specifically in the following categories:

- Medical sector
- Social funding sector
- Product tracking
- Insurance sector
- Public sector
- Logistics sector
- Escrow arrangements

Through our Smilo blockchain technology as laid out in this white paper, the digitisation of these applications can be decentralised, trustful, traceable, highly transparent, anonymous (if desired), and free of intermediaries.

Use cases

In this chapter, we are going to elaborate on some of the use cases mentioned above.

The medical sector

The medical sector processes millions of patients' records every day. These records are confidential and not intended to be public, but leaks due to human failure unfortunately do occur.

With the Smilo platform, it is possible for the patient to host his medical records on the blockchain. By doing so, only the patient with the private key can access the records. The patient can choose to use a smart contract to give permission to others, such as a doctor or hospital, to view selected sections of the record for a period of time.

The social funding sector

In the social funding sector, transparency and trust are important. Let's take a charity organisation, for example:

A benefactor may want to support a charity but does not want to share its intentions and its personal data with anyone except the organization, but even then only under specific terms as laid out in a smart contract. As the Smilo platform offers the option to make transactions private, the benefactor can choose to make an anonymous donation. To offer transparency, the charity organisation chooses a public smart contract, will allow the general public to keep treacle of the proceedings of its activities and how funds as being used to achieve certain goals.

Product tracking

The technology behind Smilo can also be applied to supply chains to establish provenance of products, which makes the supply chain more transparent and ensures full product information from not only producer to consumer, but raw resource to waste. Smilo verifies that the product has an authentic record and came from where it was supposed to come from. It is even possible to get a full historical footprint of a product from end to end, which so being audited is a breeze. Smilo's unique features allow information to be transferred in a trustworthy and anonymous way, as it essentially provides a trusted network that allows information to move smoothly down the supply chain. Meanwhile, information moves without revealing the identities of people or large corporations, so there's no fear of losing competitive advantages.

This is far more effective in ensuring transparency than using a centralised supply chain, as relying on one party creates an inherent

bias and weakness in the system, while blockchain overcomes that weakness with a greater level of authenticity and neutrality.

The insurance sector

We see different scenarios throughout the global insurance industry where Smilo could have a significant impact. It was, and should still be today, a business of utmost faith that can benefit from opacity and Byzantine operating standards. The erosion of trust is bad for everyone, and therefore our blockchain technology can hugely benefit this sector.

Public sector

Just like social sector, transparency and trust in the public sector are essential. Let's take a government as an example.

Alis is a resident of the European Union, she does not intend to publicly share her tax details with the world. However, she does want her government to be more transparent, and she would like to have greater insight into their expenses. Therefore, her personal file can be made private, while the governmental expenses can be made public using our smart contract platform. This duality generates more transparency and trust in the government, while giving Alis peace of mind that her personal details remain private.

Business overview

Background

Individuals have become the moral gatekeepers in today's society, largely thanks to the global access of information, and a societal shift towards accountability and transparency. With this movement, individuals have started to shift the balance of influence in their favour, and away from businesses, governments, and non-profit organisations. The challenge for these entities is thus to adapt and facilitate this increasingly demanding public in terms of speed of delivery, level of integration, sustainability, privacy, and security. In light of these developments, we identified the need for a hybrid blockchain platform that provided these public entities the right tools to reaffirm their relationship with its stakeholders, warranting transparency whilst protecting the individual's data.

Mission

Our mission is to create an environment that aligns the consumer's need for privacy and security with the processes of governments, NGOs, financial institutions and corporations by providing full accountability and transparency whilst safeguarding the mentioned consumer needs. All in a decentralised, safe, fast and sustainable way. We will be sharing all this in open code so future blockchains, organisations and its applications can apply this to their specific needs.

Vision

Our vision is to facilitate a culture of transparency by making collective data publicly available irreversibly, whilst protecting individual data. This will make most middleman redundant and significantly limit the chance of corruption, whilst simultaneously acknowledging the need to safeguard an individual's data. This combination of public and private transaction on the same decentralized platform based on the BFT protocol defines Smilo as a hybrid blockchain platform with a conscience.

Proposition

Smilo: Hybrid blockchain platform with a conscience:

- Sustainable: an eco friendly platform though our improved Smilo BFT+ protocol.
- Transparency: an open source environment which grants easy access for audits.
- Privacy protection: through the hybrid transactions and hybrid smart contracts.
- Anti-corruption: through the non-reversible data lock in for tenders and elections.
- Scalable and fast: over 100 times faster than Ethereum and other platforms.
- Security: through our improved BFT protocol.
- Affordable: By holding sufficient Smilo over time, transactions will be virtually free.

Relevant and applicable use cases:

- Medical records being owned by individuals and shared with medical institutions and insurance companies upon request.
- Elections or referenda being facilitated through secure and private voting to rule out any post-election influence.
- Donations through a private smart contract construction which ensures the anonymous donor that the money will be spent in an honorable way.
- Public tenders where the RFP's are being listed anonymously but also definitely and irreversible to avoid adjustments after the assignment has been granted.

The Smilo team and its beliefs

Smilo is being developed by an experienced, multi-skilled, ambitious and accessible team. The attitude overall is one of transparency, collaboration, dedication and straightforwardness. So no fake advisors but actual contributors, no corporate name dropping but actual value adding partnerships. All our efforts go into the successful development and implementation of the Smilo platform, since we are a firm believer of our concept and its potential. Nevertheless we will not sell you theories without tangible and verifiable data, we will not seek any funding before presenting a working prototype and sharing the source codes on Github.

Conclusion

The Smilo Platform will develop a significant and varied user base with a large amount of transactions, which requires a solid platform that can guarantee sufficient scalability, speed, security and low transaction costs, all executed in a sustainable way. That is why we have developed the Smilo platform the way we have.

Decentral, hybrid, fast, safe, cheap and sustainable.

Strategy

Smilo's strategy consists of multiple parts:

Smilo platform

The Smilo platform is a unique blockchain platform that can combine public and private smart contracts on one chain. We will implement our own improved version of the well-known Byzantine Fault Tolerance mechanism to ensure an optimally efficient way of reaching consensus and securing the network.

The Smilo Platform has been specifically created with application developers in mind and with full dedication and in close collaboration with our partners to launch a platform that is optimally designed, solid and rigidly tested in terms of performance and security. We intend to launch our mainnet in Q1 2019.

Smilo Knowledge and Smilo Support

As soon as our mainnet has been launched, an extensive knowledge base will be available for use within projects. Not only will there be a place for developers to find their documentation, there will also be training materials and presentations.

Smilo Modules

Smilo's ready-made easy-to-use modules are specifically designed to be applied in your projects. These modules come with a working proof of concept to present to your development team and also include technical documentation as well as presentations.

Market of the free

We at Smilo believe in an open world where knowledge and technology are created to benefit everyone. Therefore, Smilo implementation in Golang (go-smilo) will be free of charge under the Open Source GNU licence[12].

Smilo will stimulate adoption through the offering of specific enterprise solutions and consultancy and execution of applications. For clients who want more support with implementing their blockchain solution, we have Smilo Works. Here, our clients can receive help through co-creation: from concept creation and workshops, to proof of concept, and a fully tailored solution implemented on the Smilo platform. At Smilo Works, we tailor our services to your needs.

Thinking ahead

While our initial aim is to make the Smilo Platform available to our partners and users, the founders of Smilo strongly believe in building a sustainable project for the long term. Smilo's strategic choice not to execute an ICO but rather focus on getting actual transactional partnerships through the offering of enterprise solutions and the direct sale of Smilo tokens is meant to avoid volatility and speculation and through the gradual release of SMilo tokens based on actual transactions with no pre-mining also is intended to ensure a continuous and long term development of the Smilo platform and its community for many years to come.

Core team

Elkan Roelen – CEO

Hi, I am Elkan Roelen! I have over 10 years of experience in entrepreneurship, development, security, performance testing and DevOps. Furthermore, I have over 9 years of blockchain experience (the good and the bad) with a focus on security (penetration testing) and performance tuning.

Thomas Modeneis – CTO

I'm an IT professional with 15 years of experience in software development and various other roles across the board, from engineering to solutions architect and technical testing. Some of my clients are: IBM, William Hill, MDL, SKY and Brobot. During my career, I developed some solid knowledge of team leadership, vendor management and contracting as well as managing large data pools, data streaming, smart contracts and blockchain core development.

Andy Kalbvleesch – COO

Hey, I am Andy Kalbvleesch. I have over 20 years of experience with entrepreneurship and business development. I have been a project manager in a wide variety of business applications, though mostly related to IT. In addition, I also have over 20 years of experience with full-stack development and over 5 years of blockchain experience.

Patrick Joore – CMO

As a seasoned international agency executive with over 25 years of experience in building brands around the globe, I have worked with a wide range of blue-chip clients. I hope to shine my light on the opportunities that Smilo has to offer in terms of strategic partnerships. In particular, I will focus on international private and public spheres, NGOs, and all other global organisations that will benefit from the safe proposition of transparency that Smilo will soon offer.

Fabio Cruz — Blockchain Architect

Hey! I'm a Software Engineer with 20+ years experience, working as a Solution Architect on large enterprise projects around the globe for IBM customers. I strongly believe that blockchain and smart contracts will disrupt the way the world is doing business today.

Cristiano Mazzon — Blockchain Developer

I started programming at the age of 9, just over 30 years ago. I am a BCS at USP (renowned educational institution in Brazil) and I love to see little hexadecimal numbers smiling at me. As a Blockchain early adopter, I love to see how it's evolving. Well, in fact I saw a lot of rising and fading technologies and became charmed by start-ups and new challenges.

Mathyn Buiteveld – Front-end & Mobile App Developer

Hello, I am Mathyn Buiteveld! I am a resourceful software developer graduated from the Windesheim University of Applied Sciences in 2013. Since my graduation, I have been actively involved in multiple technology start-ups, such as Movin. Consequently, I have extensive experience as a software developer and entrepreneur.

Daniël Leushuis – Front-end & Mobile App Developer

Hi! My name is Daniel Leushuis, a software developer graduated from the Saxion University of Applied Sciences. My career as a software developer started at VUORA, and since then I contributed to multiple software related companies. Furthermore, I have two years of experience with blockchain technology by my own companies Radiu and getAcryp. I'll use my knowledge to contribute to the Smilo Platform, exploiting the huge potential blockchain technology has to offer.

Dion Jakobs – Front-end & Web Developer

Hey! My name is Dion Jakobs, and I am currently a full-stack developer. As a kid, I was always interested in technology. During high school, I kept trying to turn off the teacher's computer through the network, and in fact, I actually succeeded at one point! Then, at the age of 16, I became an entrepreneur and started developing websites. Later, I evolved to full-stack development. Ask me to build anything, and I am your man.

Michael Hassan – Project Manager

Hey, I am Michael Hassan. I am an all-round project manager who creates synergy between the different assets. In the last few years, I have been working on innovative projects which got me interested in the opportunities blockchain has to offer the market. What I've learned from my projects and studies is that blockchain has huge potential in a wide range of applications when it is developed properly. With the

Smilo platform, I want to contribute to the development of blockchain to its full potential.

Nickel van de Mortel – Content Manager

Hi! I am Nickel van de Mortel. I am very passionate about new technology, and I always want to learn more about it! My first encounter with blockchain technology was in 2013, and since then, I have been following the blockchain space. My experience lies with professional writing, translation, and development. My goal is to contribute to the world using the Smilo platform.

Advisors

Eyal Shalev

Eyal is a blockchain expert who is involved in several big projects and ICO's. He has earned the respect of the crypto community by the various contributions he made to the blockchain space over the last few years. Eyal Shalev has over twenty years of experience in the IT industry, and his skills include business development, startup projects, and architecture in software and hardware products. His skills and experience have contributed to a number of projects that can be found in today's top 100 cryptocurrencies.

Stephan De Haes

Stephan is the COO at Krypt.ly, a crypto FinTech start-up. He takes the lead in all social media and ICO-related subjects and oversees the general operations of the company. Stephan has grown an extensive network of connections by working with successful companies for promotional advisory in the ICO and crypto space.

Marcel Bodde

Marcel has been the ICT Manager of KroeseWevers since 2000, which means that he has over 15 years of experience with ICT and accountancy. His specialties include people management, ICT specialism, and business administration.

Hans van Egmond

Hans has a background characterised by a stellar combination of general management, project management, and extensive experience in the field of IT, which is enhanced by his in-depth knowledge and involvement in the energy

sector. In recent years, he has gathered extensive understanding through his experience with innovation and business development.

Technical background

The intent of Smilo is to create a fully-featured hybrid blockchain platform facilitating public as well as private smart contracts, transactions and decentralized applications. The platform is programmed in Golang, its GNU Lesser General Public License means it is cost free.

Smart contracts

One of the most alluring characteristics of the blockchain is the decentralised nature of it, allowing for equal and full accessibility to anyone involved. No hierarchy, no 'notary' or 'trusted third party' charging you for this obsolete role, but the collective of participant to warrant the security and legality of any transaction performed.

> *In 1994, Nick Szabo, a legal scholar, and cryptographer, realized that the decentralised ledger could be used for smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts. In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain. This would also result in ledger feedback such as transferring money and receiving the product or service.*[2]
>
> *The best way to describe smart contracts is to compare the technology to a vending machine. Ordinarily, you would go to a lawyer or a notary, pay them, and wait while you get the document. With smart contracts, you simply drop a bitcoin into the vending machine (i.e. ledger), and your escrow, driver's license, or whatever drops into your account. More so, smart contracts not only define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations.*[2]

In this way, smart contracts can facilitate the exchange of assets such as currency, property, shares but also data, in a fully transparent, secure and tamper-free way while avoiding the mostly costly and time consuming interference of the so-called trusted middlemen.

Hybrid smart contracts

One of the Smilo platform's most prominent features is the functionality of its unique hybrid smart contract set-up. A combination of both public and private smart contracts to be available on one decentralized chain can be beneficial in many scenarios.

Smilo's private smart contracts are hosted on full-node clients owned by the contract holder and as such only accessible, amendable and visible by the author. The public smart contracts are hosted on all full-node clients, these are always publicly visible through the Smilo block explorer.

Transactions

Transactions are initiated by the users of the Smilo platform. These transactions are collected into blocks, and these blocks are automatically generated by masternodes. These nodes are designed specifically to create and process blocks.

Hybrid transactions

One more significant feature of the Smilo Platform is its set-up of hybrid transactions. Where privacy and anonymity are required, we provide completely anonymous transactions that are both untraceable and non-linkable. Our technique for these anonymous transactions can be applied to two options of possible implementations to be selected by user based on its specific elements and benefits.

1) zk-SNARKS protocol. This technique was first presented by several MIT researchers[3] back in the 1980s.

> The zk-SNARKs protocol works on what is known as zero-knowledge proofs systems. In simple terms, zero-knowledge proofs means that between two parties of a transaction, each party is able to confirm/prove to the other party that they possess a specific set of information, without revealing what that information is. This is significantly different than other systems of proof where at least one party needs to know all the information.
>
> An important aspect of our solution is its autonomy. The sender is not required to cooperate with other users or a trusted third party to complete transactions, hence each participant produces a transaction independently.

2) Smilo Vault.

> The functional role of the Smilo Vault is to encrypt and share private smart contracts states via P2P/HTTPS, outside of the blockchain, allowing users to allowing users to create (GDPR compliant) DAPPS.
>
> The data that is sent via P2P/HTTPS to a node, is encrypted using TweetNACL "crypto library in a 100 tweets" in Golang.[9]
>
> Smilo Vault generates a 32 byte shared key for the hashed key-exchange described for curve 25519 and uses this key plus a random nonce to encrypt and secure the smart contract state.
>
> The smart contract state is never saved in the blockchain, only a hash that is consequently used as a checksum, so nodes can validate whether they have received a valid state. If the state is invalid, a node will automatically refuse it and the peer who sent the faulty data will be temporarily blacklisted.
>
> TweetNACL was extensively audited and the source code was found to be bug-free.[10]

Caveats

The main disadvantage of using zk-SNARKS for private smart contracts is that the information is permanently stored in the blockchain. If for some reason the user wants to delete it, it won't be possible (GDPR regulations). This is why Smilo Vault can be the preferred option based on the use case.

In any case where transparency is deemed beneficiary, we will be able to provide public transactions. These transactions can be viewed via the nodes or a blockchain explorer.

Applications and ecosystem

Smilo offers a platform for a wide range of possibilities in many areas:

- Industry applications
- Financial applications
- Semi financial applications
- Governance applications

The industrial market has already expressed their interest in the many advantages of blockchain technology. Smilo offers this rapidly evolving market a productive ecosystem as well as extensive guidance and support for building their applications on our platform.

Next to the many industrial applications, we will focus specifically on the financial sector. In this rapidly expanding and modernizing sector, numerous applications are being designed to facilitate new ways of financial management as well as insurance applications which can benefit from Smilo's offering.

In contrast to financial applications, semi-financial applications are not built solely for managing money. Semi-financial applications mix the monetary side of financial applications with information from outside of the blockchain. A perfect example of semi-financial applications are for instance specific insurance contract relying on external weather reports.

Governance applications are intended for purposes such as online voting and decentralised autonomous organisations. With governance applications, it becomes possible to form leaderless organisations.

Examples of dApps:

- Token systems
- Financial derivatives
- Decentralized file storage
- Decentralized autonomous organisations

Smilo's intent is to create an intelligent blockchain-based platform with smart contracts and decentralised applications. In order to build such a platform, it is essential to have an excellent ecosystem which developers can use to construct their applications. Smilo will provide the developers with development tools, detailed tutorials, training activities, and financial support.

Development of decentralised applications

The Smilo platform will be (co-) designing and developing a wide variety of decentralized applications on behalf of its clients. Some examples of relevant application areas include:

- A decentralised exchange
- Social funding solutions
- Product tracking solutions
- Public sector solutions
- Insurance sector solutions
- Medical sector solutions
- Escrow arrangement solutions
- Logistics sector solutions

Being a decentralized platform, there are no set requirements or limitations as to the development of decentralized applications on the Smilo Platform. Furthermore, the Smilo platform will provide developers with an SDK development kit for the development of decentralised applications. We are happy to offer support for Solidity, Java, Python, and JavaScript.

Consensus mechanism

After investigating and studying the crypto industry and blockchain technologies, Smilo came to the conclusion that the Byzantine Fault Tolerance (BFT) mechanism is best suited for our blockchain application. However, the BFT mechanism is not perfect, which is exactly why Smilo opted to improve the standard BFT mechanism by creating our own improved version of it: the Smilo Byzantine Fault Tolerance mechanism (SBFT).

The SBFT mechanism provides fast transaction verification times, demotivates most attack vectors and upholds a single blockchain version with no risk of forks or alternative blockchain records emerging — regardless of how much computing power, or coins an attacker possesses. [4]

Our improved SBFT is a consensus mechanism that enables large-scale participation in consensus through Smilo Proof of Resources and Time (SPoRT).

The objective of the Smilo platform is to allow everyone to digitise real-world assets, such as medical records and escrow agreements. Since Smilo platform is a blockchain-based platform with SBFT as a consensus mechanism, attacks on our blockchain-handling securities of this sort are close to impossible.

Network speed

Within the blockchain community, the notion of scalability is currently heavily debated. Many blockchain-based platforms struggle with a large amount of transactions; Bitcoin, for example, can only handle three to four transactions per second. As blockchain platforms continue to grow and become more mainstream, there is a necessity for the capacity to process more transactions per second. The Smilo platform tackles this hindrance. Our latest performance test indicate an average of more than 3000 on-chain transactions per second.[11]

Security

When a computer initiates transactions, the system uses digital signatures for authentication purposes. However, while that protection layer may offer strong enough encryption to secure those exchanges today, they will be unable to withstand quantum computers.

What is quantum computing?

Quantum computers are incredibly powerful machines that take a new approach to processing information. Built on the principles of quantum mechanics, they exploit complex and fascinating laws of nature that always exist but usually remain hidden from view. By harnessing such natural behaviours, quantum computing can run new types of algorithms to process information more holistically. They may one day lead to revolutionary breakthroughs in materials and drug discovery, the optimisation of complex man-made systems, and artificial intelligence.[6]

Why is quantum computing a threat to cryptography?

Quantum computing technology could potentially allow a computer to be powerful enough to crack modern cryptography, which means that a quantum computer would potentially be powerful enough to generate a private key from the corresponding public key. This possibility poses a major challenge to all cryptographically based mechanisms, but especially for the Rivest-Shamir-Adleman (RSA) algorithm- and Elliptic Curve Cryptography (ECC)-based cryptographic mechanism. Quantum computers could, in theory, solve the enormous sum of decomposition problems on which RSA relies, and they could presumably unravel the elliptic curve discrete logarithm on which ECC depends.

Anti-quantum cryptography

The current cryptography of Smilo, every account has a private key secp256k1 that controls it. The network will only accept transactions if the author of the TX can sign a transaction with his private key. How clients store the private key file in a secure manner is an implementation detail. Smilo can handle encrypted keyfiles containing a single key, but this will soon be replaced by arbitrary accounting logic that can then be lattice-based.

*At present, quantum computers are presumably unable to quickly solve the shortest vector problem and the closest vector problem.

The smart contract owner could then deploy a "new smart contract" with Lamport signatures and send his funds over to that. The beauty of this solution is that we can easily upgrade if someone cracks secp256k1 in few years.

Clients

The Smilo platform can be accessed through different clients with many use cases. The typical user most likely needs the light client, while developers probably prefer the full node client. Both the full node client and the light node client will be available for Windows, Mac OS, and Linux.

Full node client

The full Smilo platform client is the optimal solution for developers. All full client users can download the blockchain from each other through a peer-to-peer connection and enable the ability to install private and public smart contracts.

Web client

The web client is a lightweight Smilo platform client. This client does not require an installation process nor act as a network node, as it only connects to other peers which are online via an internet connection. The web client does NOT store private keys.

Light client

The light client is a lightweight Smilo platform client. This client does require a small installation process and will be available for Windows, Mac OS, and Linux. The light client does not act as a network node, as it only connects to other peers which are online via an internet connection.

Android and iOS client

The mobile clients allow the users to access the Smilo platform while on the go. The mobile client will be available for both Android and iOS.

Hardware wallet

We are planning to support hardware wallets for the web client and light client. For more information on the timeframe, we recommend consulting the roadmap[7] of the Smilo platform.

Token management

Economic model

With the dawn of the new hybrid Smilo platform we will create two types of tokens that drive the network.

- Smilo (abbreviated symbol XSM)
- SmiloPay (abbreviated symbol XSP)

The first type is the Smilo token, which will be created within the Smilodon block — the genesis block. The second type is the SmiloPay token, which will be generated every block following the Smilodon block.

The two types of tokens fulfill different roles in the network.

Smilo

Smilo tokens are a representation of the stakes held by a user, and as such they represent a user's ability to influence the Smilo network evolution. Every Smilo token counts as a vote, so the more Smilo tokens you own, the more influence you will get over the Smilo ecosystem's evolution. As a Smilo token holder, you have the following privileges:

- Send free transactions with SmiloPay
- Voting for network parameter changes

You will be able to vote for the following:

- Changing the price of Tx fees
- Changing the price of smart contract execution fees
- Changing the price of smart contract deployment fees

Each block of the Smilo blockchain generates twenty SmiloPay tokens, which will be distributed amongst Smilo holders.

SmiloPay

SmiloPay is a currency which is issued to SMilo holders for users who hold Smilo, cannot be traded and can only be can only be consumed to pay for transactions, representing the fee to use network resources (transactions, computing, storage, bandwidth, etc.). When you acquire one Smilo, you will be granted a (eg: 1.000 SmiloPay) to be released to you gradually over a period of (eg: 10 years), which you can then use to pay for transactions.
In other words, the zero transaction cost does not mean that the network can be used without any cost, we will need to secure, grow and maintain the network and as such reward the nodes processing the transactions. Is means that as long as you hold sufficient Smilo, which is of course an upfront investment, hence not free, the release of the SmiloPay to you will make transactions cost virtually free.. The more the number of Tokens held by the user, the more SmiloPay there is, so the network resources that can be used.

We can compare the usability of SmiloPay on Smilo like a battery. With a battery, the Smilo value determines the maximum capacity volume and charging speed. When a user uses a device, it consumes a certain amount of energy to power the device. The energy consumed should be higher if the device is more powerful. For the SmiloPay mechanism, the number of Smilo held by user is the capacity value. The maximum capacity volume is the Smilo of the account. The capacity recovery rate is SmiloPay/block. The task of using different types of devices is to perform different types of operations such as transferring or deploying contracts.

SmiloPay is different from Gas in ETH: For each account, the maximum SmiloPay is fixed when the account balance is fixed; SmiloPay can be restored, and the recovery speed is positively related to the number of Smilo in the account; In ETH, calculating the fee through Gas is an accumulation process. The operation of consuming SmiloPay in Smilo is similar to the type of operation that consumes Gas in ETH: Sending a transaction requires an account to consume SmiloPay; The larger the amount of Data carried during the transaction, the more SmiloPay is consumed; The more complex calculation of the data in the contract, the more SmiloPay is consumed; The order in the transaction pool is sorted by Gas Price from high to low.

References and further reading

1. White Paper. (2017, 18 September). Retrieved on 30 November 2017, from https://github.com/ethereum/wiki/wiki/White-Paper
2. Smart Contracts: The Blockchain Technology That Will Replace Lawyers. (2017, 11 December). Retrieved on 15 December 2017, from http://www.machinelearningto.com/blog/smart-contracts-the-blockchain-technology-that-will-replace-lawyers
3. Goldwasser, S., Micali, S., & Rackoff, C. (1989, February). The knowledge complexity of interactive proof systems. Retrieved on 25 March 2018, from http://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf
4. Econotimes – Blockchain project Antshares explains reasons for choosing dBFT over PoW and PoS. Retrieved on 16-12-2017, from https://www.econotimes.com/Blockchain-project-Antshares-explains-reasons-for-choosing-dBFT-over-PoW-and-PoS-659275
5. PoET 1.0 Specification. Retrieved on 20 December 2017, from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html
6. What is quantum computing? Retrieved on 20 December 2017, from http://www.research.ibm.com/ibm-q/learn/what-is-quantum-computing/
7. Smilo website/roadmap. (2018, February). Retrieved on 21 February 2018, from https://www.smilo.io
8. The Apache Software Foundation. (2004, January). Apache License. Retrieved on 22 February 2018, from https://www.apache.org/licenses/LICENSE-2.0
9. NaCl: Networking and Cryptography library, from http://nacl.cr.yp.to/box.html and http://nacl.cr.yp.to/secretbox.html
10. Review-Report Crypto Library TweetNaCl-js (Cure53, Berlin · 2017, february) from https://tweetnacl.js.org/audits/cure53.pdf
11. Smilo Network Performance Test Demo (2018, December), from https://www.youtube.com/watch?v=-vNawAjdNAw
12. GNU Lesser General Public License http://www.gnu.org/licenses/

Disclaimer

Last updated: March 20, 2018

The information contained in this document is for general information purposes only.

THIS DOCUMENT DOES NOT GIVE PERSONAL, LEGAL, OR FINANCIAL ADVICE. YOU ARE

STRONGLY ENCOURAGED TO SEEK YOUR OWN PROFESSIONAL, LEGAL, AND FINANCIAL

ADVICE.

- The purpose of this white paper is to present the Smilo platform and the Smilo tokens to potential Token holders in connection with the proposed Token sale.
- The information set forth herein may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information to potential Token holders in order for them to determine whether to undertake a thorough analysis of the company with the intent of purchasing Smilo tokens.
- Nothing in this white paper shall be deemed to constitute a prospectus of any sort or a solicitation for investment, nor does it in any way pertain to an offer or a solicitation of an offer to buy any securities in any jurisdiction.
- This document is not composed in accordance with, and is not subject to, laws or regulations of any jurisdiction, which are designed to protect investors.
- Smilo tokens are not a digital currency, security, commodity, or any other kind of financial instrument and have not been registered under the Securities Act, the securities laws of any state of the United States, or the securities laws of any other country, including the securities laws of any jurisdiction in which a potential Token holder is a resident.
- Smilo tokens are not intended for sale or use in any jurisdiction where the sale or use of digital tokens may be prohibited.
- Smilo tokens grant no other rights in any form, including but not limited to any ownership, distribution (including but not limited to profit), redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights, other than those specifically described in the white paper.
- Neither by Smilo platform B.V. or their respective directors, executive officers, core development teams, employees, or team representatives acting on behalf of Smilo platform B.V. (as the case may be), nor any affiliates, representatives, or advisors are under any obligation to update, supplement, or correct this white paper or accompanying materials in any respect, or otherwise to provide any recipient or reviewer of these materials with access to any additional information. In addition, the project management and core development teams, Smilo platform B.V. and the development teams reserve the right, without prior notice to any reviewer or recipient of this white paper or any accompanying materials, to terminate, at any time, further participation until tokens are generated. We reserve the right to modify any applicable procedures without giving advance notice thereof and without providing any reason therefor.

- All statements contained in this white paper, made in press releases, or expressed in any place accessible by the public, in addition to any oral statements that may be made either by Smilo platform B.V. or their respective directors, executive officers, core development teams, employees or team's representatives acting on behalf of Smilo platform B.V. (as the case may be), nor any affiliates, representatives or advisors, that are not statements of historical fact, constitute "forward-looking statements". Some of these statements can be identified by forward-looking terms such as "aim", "target", "anticipate", "believe", "could", "estimate", "expect", "if", "intend", "may", "plan", "possible", "probable", "project", "should", "would", "will", or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding the financial position, business strategies, plans, and prospects of Smilo platform B.V. and the future prospects of the industry in which Smilo platform B.V. exists are forward-looking statements. These forward-looking statements, including but not limited to statements of the revenue and profitability, prospects, future plans, other expected industry trends of Smilo platform B.V. and other matters discussed in this white paper regarding Smilo platform B.V. are not historical facts but rather predictions.
- This white paper can be modified to provide more detailed information. This English-language white paper is the primary official source of information about the Smilo platform.
- The information contained herein may from time to time be translated into other languages or used in the course of written or verbal communications with existing and prospective customers, partners, etc. In the event of any conflict or inconsistency between such translations and communications and this official English language white paper, the provisions of this original English-language document shall prevail.
- The white paper may be updated or altered with the latest version of the document prevailing over previous versions. Smilo platform B.V. is not obliged to give notice of changes. The latest version of the white paper in English is available at the website https://www.smilo.io. While we make every effort to ensure that all data tendered in the white paper are accurate and up to date at the point in time that the relevant version has been disseminated, the proposed document is not an alternative to consulting an independent third-party opinion.
- Due to the very short history of crypto tokens and crypto-economic systems, there are several challenges that token holders face when trying to value these projects and underlying tokens. The short history of crypto tokens has generally shown an even shorter lifespan of many of the projects. This is especially true because projects present a significant principal-agent problem. This challenge differs from those of a start-up, which usually raise money in a series of rounds over several years. Secondly, there is some level of systemic risk associated with the crypto markets that cannot really be diversified away. The industry is too nascent for such an option. Therefore, no refunds will be given by Smilo platform B.V. in any form.
- Token holders take on both project-specific risks and market risks when they acquire tokens in a specific sector. Systemic risks are very hard to predict due to the short time span and are unique to the industry. Everything from hard forks to new crypto attacks are a source of systemic risk from which traditional investments do not suffer. Generally, as the development of blockchain tokens continues to enable new business models, new legal issues come into focus. For developers, legal and regulatory uncertainty can be one of the main barriers to building new blockchain protocols and applications. We emphasise in the strongest possible way that Smilo tokens do not represent ownership or a security interest over any entity, asset, or property. They do not represent a debt owed by any entity and shall not be considered a debenture under any applicable law. It is for these reasons that we believe that our tokens are not securities and may be purchased by anyone. If you determine that our tokens may constitute securities subject to regulation in any country, we strongly advise you against acquiring them and suggest you immediately notify us of the possible risks. Again, there will be no refunds given by Smilo platform B.V. in any form.