Geens

WHITEPAPER

Version 1.1

CONTENTS

1. What is Geens?

Geens is a privacy focused document storage platform with blockchain timestamping services.

Private document storage is the backbone of the Geens platform. The platform can be compared to Dropbox or Google Drive, with Geens holding a higher level of privacy.

Because of the end-to-end encryption, the unencrypted data never leaves the user's device. It is first encrypted on the user's side and only then is sent to the Geens servers.

High security standards guarantee that even in the worst case scenario, there are practically no chances to decrypt and steal Geens user's data.

Geens is user friendly, intuitive, and simple. Using the floating cards interface, users can work with their documents directly on Geens. They can also securely share files.

Geens is GDPR compliant. GDPR compliance will become obligatory under EU law from 2018, and Geens can offer business solutions to the large EU market and beyond.

Geens' encrypted document storage is connected to the Ethereum blockchain. The blockchain as a technology is immutable and incorruptible.

Geens users can timestamp their documents on the blockchain without revealing the content of their document's or their own identities.

Among other applications, document timestamping is used to protect copyright, unique ideas or patents; to prove that the document was signed prior to a specific date; to acknowledge ownership; and to produce virtual IDs. Blockchain timestamps can be used as legal evidence in courts across the globe.

Some Geens users timestamp their files while other users work as legal assistants, consultants, or validators and receive GEE tokens in return for their services.

Geens is a nonprofit organization (NPO). It is supervised by the ethical committee under international law.

To cover operational costs, Geens provides premium services for individual users, custom solutions for enterprises and gets commissions from the GEE economy.

All extra profits are then returned back to the NPO members. Geens users can opt-in to become NPO members and enjoy the benefits.

As a nonprofit organization, Geens can never be acquired by anyone.

Geens

2.

Overview of the current market situation, competition analysis

2.1. THE CONTEXT

Today more than 2 billion individuals and millions of companies are using the internet as a global information architecture that allows them to conduct their activities online. Millions of communication devices are sending and receiving private data every second.

Digital data is doubling in size every two years, and by 2020 the data created and copied annually will reach 44 Zettabytes, or 44 trillion Gigabytes. There is a huge need to provide effective tools for managing personal & private data and to develop a wide range of data services such as cloud computing, data timestamping, data mining and analysis.

Data storage solutions are offered by various providers such as Google, Amazon, Microsoft, and Dropbox. Additional needs are generated mostly by higher quality multimedia (pictures, HD, 4K, email attachments).

Large amount of personal data - typically multimedia, but also personal letters, emails, messages, contracts, personal pictures, confidential presentations - need a place on the web that is both private and secure. Therefore, there remains a large market for end-to-end encrypted data storage solutions. Such data storage could be offered to individuals, governments and companies, and then used for storing highly private & sensitive data.

2.2. DATA PROTECTION TRENDS & ENCRYPTION OF PRIVATE DATA

Rapid technological developments and globalization have brought many new challenges for the protection of personal and private data. During the last decade, the scale of collection and sharing of personal data has increased exponentially. With the upcoming fourth industrial revolution, the trend will continue. Responding to these developments, the European Union started one of its most ambitious legal reforms in the sphere of data protection. and the reform culminated in the adoption of the General Data Protection Regulation (GDPR), which will come into force on 25 May 2018.

The GDPR regulations contain a set of measures designed to protect the personal data of EU citizens. GDPR brings a high standard of protection and, in case of failure to comply with the data protection requirements, establishes sanctions of up to 20 million EUR or up to 4% of the annual worldwide turnover. Due to the severity of sanctions, businesses may no longer afford to ignore data protection regulation and requirements.

The GDPR will be directly applicable to every company and organization established in the European Union. Furthermore, the Regulations will also apply to companies established outside the Union, if such companies are processing personal data of European citizens and conduct business activities in the European Union. Furthermore, the European Union allows transfer of personal data to third countries only if the latter ensure adequate protection of such data. Therefore, it is safe to assume that the high standard of data protection would see widespread adoption in the future.

One of the most important requirements for processing personal data established in the GDPR is the implementation of technical and organizational measures to provide appropriate protection to the personal data that companies hold and process. The GDPR does not specify which particular security measures should be used. Encryption, however, is mentioned as one of the most important security measures.

Encryption, therefore, can serve as a technical and organizational measure to ensure the security of personal data and to reduce the risk of sanctions under the GDPR. Encryption of personal data would ensure both the anonymity of an individual and the compliance with the GDPR. This would significantly lighten the burden for companies processing data. Encryption of data also implements fundamental and obligatory data processing principles established in the GDPR – data minimization, storage limitation and proportionality, which inter alia means that processing of personal data should be reduced to a minimum. As part of privacy by design obligation, any company processing personal data shall have an obligation to consider data protection at the initial stage of each new service or product development. This shall involve adapting technical measures such as encryption of personal data.

Due to aforementioned reasons, data encryption shall play a key role in ensuring data security and compliance with the data protection requirements. No enterprise is able to conduct business without processing of personal data, therefore, encryption shall be relevant in activities of all companies and organizations.

2.3. EXISTING ENCRYPTED CLOUD PROVIDERS

Data storage platforms combined with cloud services are becoming irreplaceable for most private users, small & medium businesses (SMB), or large corporations. According to Forbes, the market of cloud computing is projected to increase from $67B in 2015 to $162B in 2020, attaining a compound annual growth rate (CAGR) of 19%.

The public cloud market is dominated by major providers such as Amazon, Google, Microsoft, IBM, and Dropbox. These providers, however, use their servers to store unencrypted data.

This approach has resulted in many high-profile data breaches, resulting in total damages estimated in the billions of dollars. Therefore, such a dominant data cloud model is vulnerable to a variety of outside attacks and cannot be considered reliable in terms of ensuring data privacy and protection.

End-to-end encryption based data storage technology means that user data is encrypted (on computer or smartphone) before it is sent over a network or to a server. In case of a breach, the attacker will only be able to access encrypted data, which remains unintelligible. The model of E2E encryption is rarely used within the common data cloud industry as encrypting requires more disk, processing power, and quality control.

At present, Mega and Tresorit are among few companies that offer end-to-end encryption based data storage services. The table below provides a description of the main features for both clouds:

FEATURE	TRESORIT	MEGA
Free storage	0 GB	50 GB
End-to-end encryption storage	Yes	Yes
End-to-end encryption sharing	Yes	Yes
Zero knowledge authentication	Yes	Yes
2FA authentication	Yes	No
Sync function	Yes	Yes
Data backup	No	Yes
Business mode (for B2B clients)	Yes	Yes
Data timestamp	No	No

Mega (New Zealand based) offers 50 GB of data storage for every registered user, free of charge. Its approach to end-to-end encryption and the offer of 50 GB of free storage allowed the company to reach 89 million users. A Mega user can upload data from the mobile app, can share such data with the public, and can upload an entire folder using a browser. At the same time, Mega applies 10 GB bandwidth limit, that is reset every 30 minutes. Also, Mega does not offer advanced links for data sharing like password protection (only via public link).

Tresorit is based in Switzerland and Hungary, where data privacy laws prevent third parties from accessing your data without your explicit permission. Based on the zero knowledge principle, Tresorit offers uploading data from a mobile app, team management options for business accounts and a 2FA authentication function. Tresorit, however, has limitations: there is no "free" version of data storage, the platform has an expensive pricing model, mandatory expiry and download limits on links, password protected links only exist on business accounts, and file size limits exist on all tiers.

In conclusion, Mega and Tresorit allow its users to store and share private data in a secure way. Neither of the two clouds, however, offer services which go beyond pure data storage, such as data timestamping, data verification, or data validation. Their services remain incomplete and are unable to meet the market demand for a full range of services in terms of managing privacy and identity.

2.4. BLOCKCHAIN TIMESTAMPING PROVIDERS

Any private data, be it a file or a text, could be timestamped on a blockchain network. The logic of blockchain timestamping fits into a few steps. A unique digital fingerprint (commonly referred to as a "hash") is calculated from a file. Next, a timestamp is generated and added to the file hash. Finally, the file hash is submitted to a blockchain network (it might be Bitcoin, Ethereum, or any other network). After the transaction on the blockchain network is approved, the owner receives the hash, private key, and timestamp information.

The blockchain as a technology is immutable and incorruptible. Timestamp, therefore, proves that a particular set of information existed prior to a specific point in time. This also demonstrates the integrity and the immutability of any kind of information. The blockchain timestamp therefore is of major importance for a secured, transparent and efficient process of data management and has real-life applications.

Here we list blockchain timestamp providers that exist in the market.

https://po.et/

Po.et aims to generate and to timestamp certificates of ownership for digital creative assets. By providing an open network for registering digital creative assets, Po.et plans to give tools to automate the licensing process. The Po.et project is dedicated mainly for content creators, publishers and journalists. Currently, only an Alpha release of blockchain timestamp exists.

https://www.bernstein.io

Bernstein allows companies to create a digital trail of records of their inventions, designs and proofs of use by using blockchain timestamp technology. Later proof of ownership, existence and integrity of any registered asset can be verified. Bernstein is planning to offer the zero knowledge architecture, which means that all documents submitted by the user will be encrypted in the browser. At the moment, the Bernstein project is in the concept phase only.

http://proofofexistence.org/

A tool that allows generating blockchain timestamps for documents. By filling a form and uploading a file, the user receives a link with a proof of existence of a timestamped file. Later, the existence of a particular document can be verified.

https://proofofexistence.com/

It offers to generate blockchain timestamp for a document and to store its proof of existence certificate on a blockchain network. Later, the existence of a particular document can be verified.

https://stamp.io/

Stamp.io offers a tool to timestamp documents by uploading them on the site. The service of blockchain timestamping is free of charge. The timestamps are generated by leveraging both the Bitcoin and the Ethereum blockchain networks.

https://chainy.info

Chainy offers to timestamp URL shorteners (e.g. bit.ly) on the Ethereum network. Due to Chainy services, the real address destination (URL) is saved in the blockchain with the unique short code and can never be altered by anybody. The proof link will be included directly in a smart contract. The link will be short and easy to retype by hand.

https://docstamp.io/

DocStamp offers to timestamp documents on the Ethereum network. In order to be able to timestamp a document and later to verify its proof of existence, a user should register by e-mail.

https://notareth.herokuapp.com/

This is a tool to submit documents and to make timestamps on the Ethereum network. No other functions are offered.

https://app.originstamp.org/home

OriginStamp is a non-commercial trusted blockchain timestamping service that can be used free of charge for any digital files. OriginStamp offers to timestamp text, notes or ideas. A user can upload digital content on the OriginStamp site and its timestamp will be created. Any text can be typed directly into their desktop app and be timestamped. All timestamped data can be verified later by uploading the document or text.

All hashes made on OriginStamp are submitted to the bitcoin network only once per day. In order to accelerate the hash submission the user should pay extra.

https://github.com/goblin/chronobit
https://github.com/bitcoinaustria/bitnotar
https://github.com/goblin/chronobit

A number of other blockchain timestamped focused projects can be found on the github.com site. All of those projects remain in a concept phase.

A review of existing timestamp providers shows that most of the services available on the market offer to timestamp documents on a blockchain network. Some of the projects are only available in a concept phase, making it difficult to evaluate them. Other projects such as chainy.info or po.et seek to focus on particular areas, such as timestamping URL shorteners or providing dedicated timestamp services for content creators.

No one in the current market can offer a complete solution – a safe and an encrypted space to store documents and the possibility to timestamp them on the blockchain. This makes the Geens platform unique.

2.5. OTHER RELATED SERVICES

Other specific services such as content copyright management and protection exist on the market. From the technological point of view, the market offers a number of services that are based on processes managed manually (Myows, MyFreeCopyright). More sophisticated services already integrate the blockchain technology (Creativechain).

A traditional approach for content copyright management (Myows) requires uploading an original work or content on the platform. Then a copy of that work will be saved and a certificate of content authentication will be generated. In case of unauthorized usage, a user can accordingly build a case against infringers. Myows will assist the owner in contacting the unauthorized user and will be able to provide verifiable evidence in the case. This way intellectual property rights would be protected. The process of solving a case, however, can take a long time and be rather complex, consisting of many steps which should be taken by the user. Moreover, all original content stored in Myows platform is unencrypted and therefore vulnerable to outside hacks.

Another example of content management is to offer services which already integrate the blockchain technology. Creativechain seeks to design a decentralized platform for content registration and P2P distribution that will certify the intellectual property. With the support of the blockchain technology, the timestamps of digital content will certify the intellectual property of any digital content provided through their platform. Additionally, the management of collections, payments, and donations will be offered to the authors through Creativecoin token (CREA). Creativechain is yet to release any product created by the platform itself, making it hard to judge the utility of the enterprise. Moreover, Creativechain does not intend to offer data storage for users content. Instead, the process of content management will be implemented through a social network model. This might be a significant shortage to provide a full range of services of content management and to ensure a high level of data privacy and security.

3. THE UNIQUENESS OF GEENS. PRIVACY FOCUSED DATA STORAGE WITH BLOCKCHAIN TIMESTAMPING

The worldwide demand for delivering the different type of private data-focused services, tools, and solutions is quickly growing. At the same time, new trends of data regulation aim to strengthen measures and requirements for appropriate protection of the personal data that companies hold and process.

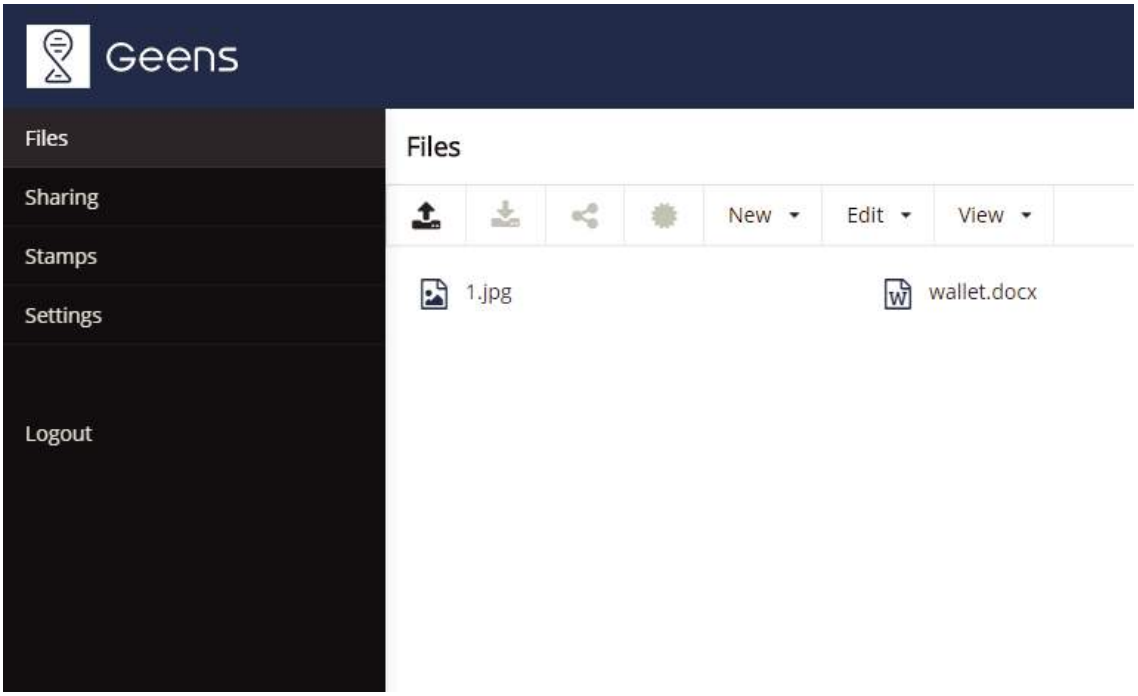
Due to the recent rise of innovative technologies, the market offers new and modern ways of handling private data. There is no doubt that some of such services are valuable and offer proper solutions to a user. On the other hand, the market for private data services and solutions remains fragmented. In order to receive a full range of solutions, the user is forced to choose several services from a range of providers. For example, if a user needs to validate his virtual ID and to share it with a third party in a fast and secure way, he or she needs to find a service provider for a blockchain timestamp, a service provider for encrypted data storage, and a service provider for ID validation. Such practice remains cumbersome and insecure.

Geens has come to recognize the inefficiency that exists in the market. The platform has, therefore, chosen a development strategy which brings together different instruments and tools for private data management. To put it simply, Geens offers a solution to a set of issues and addresses various needs of private data with one log-in to Geens.

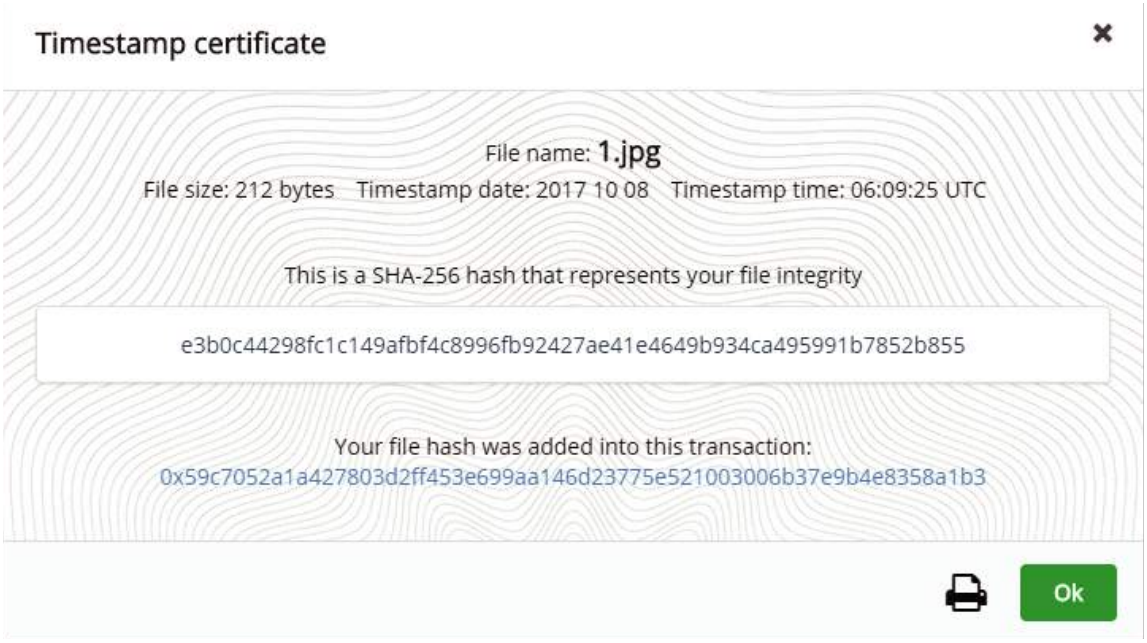
Two keywords could be used to define Geens – PRIVATE and PUBLIC. Geens is where the two come together. PRIVATE is the end-to-end encrypted "zero knowledge" document cloud storage service. It works as a virtual office for our users' documents and is the backbone of the Geens platform. The data our users store on Geens is completely private, meaning that the data owner is the only one with the access. Even Geens administrators are unable to see it.

PUBLIC is the blockchain part, also called a public ledger that is an incorruptible, reliable, and provable way for document timestamping. Geens private files storage is connected to the public blockchain on Ethereum network. Users can timestamp their files without revealing their own identity or the content of their files. These timestamps can later be used as a legal proof of existence or ownership.

The development of the Geens project commenced two years ago. The Geens private storage cloud is stable and user friendly. All data can be easily uploaded, downloaded and shared. Video, audio; and photo files of various extensions can be viewed directly in Geens.



Every file stored in Geens could be timestamped on the blockchain, meaning that for each file a timestamp certificate will be generated automatically. The timestamp certificate is stored in a special folder in Geens. The certificate contains such information as timestamp date and time, a file hash which represents file integrity, and an address of transaction by which the file hash was added into the blockchain.



4.

Geens solution in detail

4.1. END-TO-END "ZERO KNOWLEDGE" ENCRYPTED DOCUMENT STORAGE TECHNOLOGY

A term "Zero knowledge" was invented to describe a different process than it is generally used in public today. The term "Zero Knowledge Archive" (ZKA) is used to describe storing of private digital data in an encrypted form while collecting, disclosing, and storing as little private information (metadata) as is economically reasonable and possible with a goal to support and develop the system for the long term.

ZKA by definition also includes services provided by Tresorit and other providers mentioned above. Any communication or transaction between two different actors in the system uses energy and leaves so called informational trail of "breadcrumbs". To address the issue, Geens renders the breadcrumb trail sparse, randomly distributed, and hard to follow.

Due to historic and economic reasons, the most common unified platform is a JavaScript-programmed web browser. Web browsers are complicated virtual machines based on an insufficient security model, which contains many documented security problems. Many of those issues are hard to fix and avoid. If the highest data security standard is required, Geens could be securely accessed using the native cross platform client which will be available after the release of the beta version, removing many layers of abstractions and security risks.

Even such simple action as attempting to send a simple message from one user to another is put at risk by software layers and abstractions. Some by design, some unintentionally leak user information at every step. Moreover, global, regional and local legal requirements add various informational leakage points to the system. That leakage could be made intentional or even unintentional. For example, region related cultural patterns, time zone, preference and dislike of certain topics can leave a trail. This trail could then later be followed and be used for physical, economical, or informational violence or theft against individuals.

One of the main problems with storing user data is privacy leaking software that is popular and even purposefully designed to leak user information to interested parties.

This document is describing a data storage system which allows to transparently and verifiably indicate the current factual state of the privacy of your data and metadata, storage, and decentralized document storage and signing system.

In terms of public and private storage, four different types of files exist:

Public (-Indexed) - information that anyone can access provided they know the first time generated security token;
Public (+Indexed) - information that is available in public, is indexed in public search engines, and is easy to find and to access;
Private (-Shared) - information that is only known to a private user;
Private (+Shared) - means, that the information has been used by more than one person, and the control of the information has been effectively lost.

Private user information that is never stored on the Geens platform: files, file hashes, user email, phone number, file chunk request by IP address, keys of keys, a method of data decryption and disassembly, IP address, date and time of access, user agent, other (file meta author, exit tag).

Private user information that is known by Geens (shared): blockchain address (ETH, BTC).

Public user information that the user can disclose without fear: unlimited number GEE token addresses, account addresses for public signatures.

The basic logic of the data encryption and decryption process could be explained as follows:

User sends file to archive:

BROWSER (CLIENT'S SIDE)	SECURITY (SERVER'S SIDE)
U1 ----> F1 ----> ENCRYPT ---->	e.U1F1 ----> PR ----> e.UXF1 ----> S1
U2 ----> F2 ----> ENCRYPT ---->	e.U2F2 ----> PR ----> e.UXF2 ----> S1
U3 ----> F3 ----> ENCRYPT ---->	e.U3F3 ----> PR ----> e.UXF3 ----> S1

User requests file from archive:

BROWSER (CLIENT'S SIDE)	SECURITY (SERVER'S SIDE)
U1 <---- F1 <---- DECRYPT <----	e.U1F1 <---- PR <---- e.UXF1 <---- S2
U2 <---- F2 <---- DECRYPT <----	e.U2F2 <---- PR <---- e.UXF2 <---- S3
U3 <---- S3 <---- DECRYPT <----	e.U3F3 <---- PR <---- e.UXF3 <---- S9

U - User **F** - File **PR** - Privacy Router **S** - Server
e.UXF - Encrypted File of Unknown User **e.UF** - Encrypted User's File

Encryption and decryption of files, keys, onion routing, keys of keys and reassembly of chunks are processed in the Geens ZKA. The general process of the Geens ZKA system could be explained in further steps:

a) A trust line between user and system is established and public keys are exchanged for the first time. This forms the base and the first fact from which all trust between a user and Geens server flows.

b) Private data is encrypted on the client side in Geens (a web browser's virtual machine is using SHA256 symmetrical key encryption, key re-encryption, and sharing functions).

c) After the encryption, every file receives a public and private key, which in turn are re-encrypted with another key, making sharing of the files possible without copying data in ZKA environment: 1. secret: new file is received and encrypted by client side VM; 2. keys_to_secret: pub/priv key pair is generated; 3. keys_to_secret_keys: pub/priv key pair is generated; 4. during sharing of the file, the keys_to_secret_keys are regenerated with a specific user id.

e) The replicator .geens.io receives a ticket for the storage requests.

d) An encrypted file is chunked into 1.5 blocks and streamed into the server.

f) Data is transmitted using the specified privacy tier tunnel.

g) Stored data is replicated and shared by the Geens chunk cluster.

h) Cold data older than > 365 days is moved to cold storage.

Data is stored in highly redundant centralized and decentralized block storage platforms on the cloud and in the local Geens market by choosing the most economical storage and access vendors.

As the data is split into chunks, and SHA256 is hashed for indexing, this index is also used by a Geens tailless (only head) Merkle tree, which is append only and created for tracking and versioning documents of each user. This tree is checkpointed on a daily basis into the Geens private cloud cluster, and into the 3 most robust blockchains.

4.2. BLOCKCHAIN TIMESTAMPING SERVICES

The value of recording information with a timestamp and a method to verify the authenticity of such recording using social trust vectors and simple token sharing schemes has been known and used for centuries.

In modern times, the recording is usually confirmed and supervised by a trusted third party, which was also tested, certified and trusted by a higher authority, forming a hierarchical tree of trust. A good example would be a registry or a bank, or a state certified notary service, or a diploma provided by a university. These institutions are hierarchical and centralized aggregators and validators of trust. Because of this centralization, usual incentives for defection from trusted actors are also increased. Such system can be corrupted by malicious actors, which can coordinate with insiders and complete decision/action loops faster, thus gaining an advantage and grabbing more resources than "fair" in a game of "Nash equilibrium" over static slow moving hierarchical organizations that are tasked to defend from such corruptive acts.
For example, the notaries, or the banking tellers, can be malicious themselves or provide knowing / unknowing support for malicious actors.

The first blockchain "Bitcoin" has demonstrated that it has become possible to assemble a system of mathematics and social incentives, and to create a decentralized system which supports decentralized economies with a functional immutable ledger. The ledger is certified by millions of dollars spent "mining" proof of work.

An append-only distributed ledger, which can timestamp the data, and pay for the transaction of timestamping at the same time is still being used mostly as a ledger only and hasn't been widely adopted in other non-financial services. This decentralized ledger with a network consensus - blockchain – allows for timestamping of a data hash and can be stored in a blockchain transaction.

Distribution of "proof of work" allows its users to move from passive consumers to service providers in a crypto economy. The constant growth of users who are starting to recognize the value of the blockchain and have enough resources and time ensures participation in this economy.

Therefore, Geens is proposing a tiered decentralized system of timestamping. Geens will provide a system that allows to easily sign and to verify documents. Common personal/business task oriented templates and Geens-recommended document indexes will allow users to use the platform in order to solve real life problems.

The platform will provide an interface that is accessible to non-technical users. Secured and trusted by design, the platform will allow a vendor and a user to make private transactions: to create and to verify documents.

In the Geens technical beta the Ethereum blockchain is being used to implement the timestamping service. The platform provides a common wrapping API for other blockchains. The proposed timestamping model with automatic instant pricing of stamps by different blockchains is planned for further implementation. GEE Token is a utility of the Geens ecosystem and will be used as the main instrument to cover the costs of decentralized timestamping services.

Geens will offer a tiered document timestamping service model, which allows the end user or developer to choose the level of required privacy:

TIER3 TIMESTAMP

it can be used for transferring high value assets

3 blockchain:	Proof of Block
3 digital notary:	Proof of Peer
1 physical notary	Proof of Peer
1 Geens vault	Proof of Chunk

TIER2 TIMESTAMP

it can be used for 3 party-asset transferring: user1, user2, notary

1 blockchain	Proof of Block
1 digital notary	Proof of Peer
1 Geens vault	Proof of Chunk

TIER1 TIMESTAMP

it can be used for timestamping e.g. a new logo design

2 agents: user, blockchain

1 blockchain	Proof of Block

4.3. DIFFERENT LEGAL TIMESTAMPING ASPECTS

Before a document or a fact can be introduced in legal proceedings before a court or a governmental institution, the party presenting or relying on such a document or a fact bears the burden of proof to show its authenticity or veracity. A court or a public institution is unable to take a decision, if the authenticity of a document or veracity of a fact is called into question.

In case of a document, the party who wishes to introduce a document as evidence in legal proceedings must show the truth of the statements a document contains and demonstrate that the document is what it appears to be. A party might be required to prove that the will expressed in a document truly represents the will of a person who issued or signed this document. Usually, documents would need to be verified or authenticated as original. Furthermore, if a party wishes to rely on a fact, she or he must be able to prove the veracity of such a fact through evidence.

In order to show authenticity or truth of a document or a fact, a party may use a number of means. For example, in certain cases, authenticity of a document might or even must be confirmed by a notary. Furthermore, in order to prove a fact, a party might use assistance of a bailiff, whose collected is more reliable before courts, as opposed to other usual information collected by parties themselves. A party may also rely on witness testimony or other evidence proving a fact.

The above listed means of demonstrating authenticity or truthiness are costly and may ultimately prove unreliable. Testimony of an individual or records made by a notary or a bailiff cannot completely eliminate the probability of mistake or fraud.

Blockchain as a secured, chronological, and decentralized consensus ledger could potentially solve the above mentioned issues and provide reliable proof concerning recorded facts or documents. For example, blockchain based timestamping might be used to determine contractual parties, contractual provisions, content of documents or existence of certain recorded facts at a certain time.

The legislature of Vermont State of the United States approved the first law in the United States to use blockchain technology to verify and authenticate records and information. Under this law, a fact or record verified through a valid application of blockchain technology is presumed to be authentic for the purpose of introducing such a fact or record as evidence in legal proceedings.

The legislature of Vermont State suggests that blockchain based timestamping might be recognized as having legal power in other states and countries as well.

4.4. GEENS DATA MARKETPLACE

In its essence Geens is privacy focused data storage with blockchain timestamping services. In order to provide the full range of services of privacy and identity management, and to reflect a changing legal, social and cultural environment, such as GDPR regulation, e-governance, implementation of virtual IDs, the Geens data marketplace is offered. The marketplace contains all necessary infrastructure with its core utility – the Geens Network Token (GEE), which enables the exchange of services and the transfer of data among the users of Geens. The mechanism of providing and receiving services or transferring data will be implemented via signing of smart contracts. These contracts are signed cryptographically on the Geens blockchain network and are intended to provide greater security and to reduce transaction costs compared to a traditional contract.

In the sequence of the development of the road map, the GEE economy v1 (enables exchange of services) and the Geens data marketplace (enables exchange of data) will be offered.

Below Case 1 shows an example of how the Geens data marketplace is going to function.

CASE 1

Conducting clinical research in data marketplace

A fundamental human subject protection is universally recognized as a critical requirement to the conduct of any kind of clinical research involving human subjects. In all cases confidentiality or even anonymity of information collected from the participants of clinical research should be ensured.

The Geens data marketplace could be used as a “safe” and is fully compliant with data privacy for conducting clinical research. A simple illustration in a few steps follows. All data of participants required for clinical research will be uploaded on the Geens platform and stored using E2E encryption. Such data could be timestamped, validated, and shared with the research institution without revealing any information of personal ID. The research institution, therefore, will be certain about authenticity of the data with no need to contact directly the participant for data authentication. Moreover, the smart contracts of data sharing to the clinical research institution could be set automatically on a regular basis. For example, a participant will upload his blood test results on Geens every three months and then such results will be automatically shared with the research institution.

Two different approaches of data management for clinical research exist in the Geens data marketplace: 1) an institution in charge of clinical research can invite the participants who are outside-selected to join Geens; 2) participants for clinical research can be selected from the members of Geens. In both cases, the agreement between the parties will be implemented via smart contracts. Accordingly, the agreed amount of GEE tokens as a compensation for data sharing will be paid by the clinical research institution to the participants.

4.5. GEENS FOR BUSINESS

Geens services and tools of private data management as a primary goal are designed to benefit its members. Most of the services in Geens can be used free of charge. In order to cover its operational costs and to be able to consistently maintain a good quality services for its members, however, Geens has a business mode for private data management (Geens-for-business). Geens-for-business focuses its services to several specific areas.

Every user of Geens automatically gets 1GB of free storage within the Member plan. Users of the Member plan can use all the main functions and services – to upload, to send, to share, and to edit private files in a secured, easy, and expedient way. Additionally, for individuals who require advanced services, two **premium plans** exist: Premium plan (100 GB storage space) and Professional plan (1000 GB storage space). An incentivized pricing strategy of some services is applied to users of different plans. For example, a regular price of document blockchain timestamp costs 25 GEE tokens per one timestamp. For the subscribers of the premium plans such blockchain timestamp services are available at a reduced rate – 20 GEE tokens per timestamp for a member of the Premium plan and 15 GEE tokens for a member of the Professional plan.

Another important Geens-for-business mode – **custom features and solutions** of data management offered to enterprises. Geens offers to enterprises to host their data (as customer databases, internal documents) and documents on the Geens servers of which the technology is based on the most protected end-to-end data encryption. Any amount of data storage space needed could be offered. Enterprises can use the Geens DB which is GDPR compliant, access-limited and confidential. Geens allows to integrate a single sign-on system into third party applications. Enterprises can set up a team work mod, and manage files in team folders, safely and remotely send and share documents, define different level of access to those folders or data, among other functions.. Encrypted Geens chat and anonymous voting system are offered for the team work as well. All the necessary support for business services will be provided by the experts of Geens.

The Geens data marketplace is of major importance for Geens-for-business. As a real-life application of the Geens data marketplace was explained in detail previously, here it is important to emphasize its economic logic. An exchange of data between the participants of the marketplace will be implemented via signature of Geens smart contracts. The smart contract will automatically transfer GEE tokens agreed to be paid by a service receiver to the account of a service provider. For every transaction, the smart contract will allocate a fixed amount of GEE tokens to the Geens account. The commissions received in the form of GEE tokens is a compensation to Geens for providing all infrastructure of the data marketplace.

4.6. GEE ECONOMY

A long-term goal of the Geens project is to move towards a self-sustainable, independent, and decentralized model of the GEE economy in terms of privacy management. The model of GEE economy integrates together all ideas already presented in this whitepaper, and brings new ones in the later phases of project development. An equilibrium and efficiency of the entire GEE economy will be achieved in the long term. The Geens Network Token (GEE) is a central utility of the GEE economy enabling data transfer, exchange of services and ideas among the members of Geens. A purpose of the GEE economy is to provide efficient instruments (for example, data marketplace, smart contracts) and to create a mechanism of incentives to manage and to solve all kind of privacy issues that may arise among users of Geens.

Three main principles will be used in building the GEE economy:
1) Proof of Chunk (private document cloud data is protected by encrypted data chunks);
2) Proof of Block (timestamping and document signing service using blockchain network);
3) Proof of Peer (A service provided / received by a user on the Geens platform).

After a user chooses a combination of features, he or she can initiate the request to find providers for each service. Services involving only digital data are initiated instantly and automatically. Physical services available in the GEE economy v1 are provided by creating an on-off temporary market/auction with time and other requirements specified by the user. the Geens platform automatically completes the cycle and writes the hash of the transaction into the immutable blockchain. When the minimum requirements for the transaction to proceed are met, the transaction is completed and signed.

Bellow Case 2 and Case 3 illustrate how the GEE economy v1 is going to work.

CASE 2

Identity (ID) validation in GEE economy v1

Geens users can timestamp their private data on the blockchain. Documents of personal identity such as a driver license, ID card, passport or utility bill can be timestamped. An attestation of proof-of-existence for every blockchain timestamp is generated. Such attestations of personal identity could be verified and used in many cases where person identification is required. For example, it may include service providers as financial, medical and municipal institutions.

Trustworthy validators, persons who have an authority and license to verify identity, would be able to provide services of ID validation in the Geens data marketplace. A process of ID validation among user, service provider and validator will be completed via a smart contract after approval of the user. In every case of identity validation, the smart contract will automatically allocate GEE tokens, paid by service provider, to the validator as a compensation for a validation and to the user as a compensation for participation.

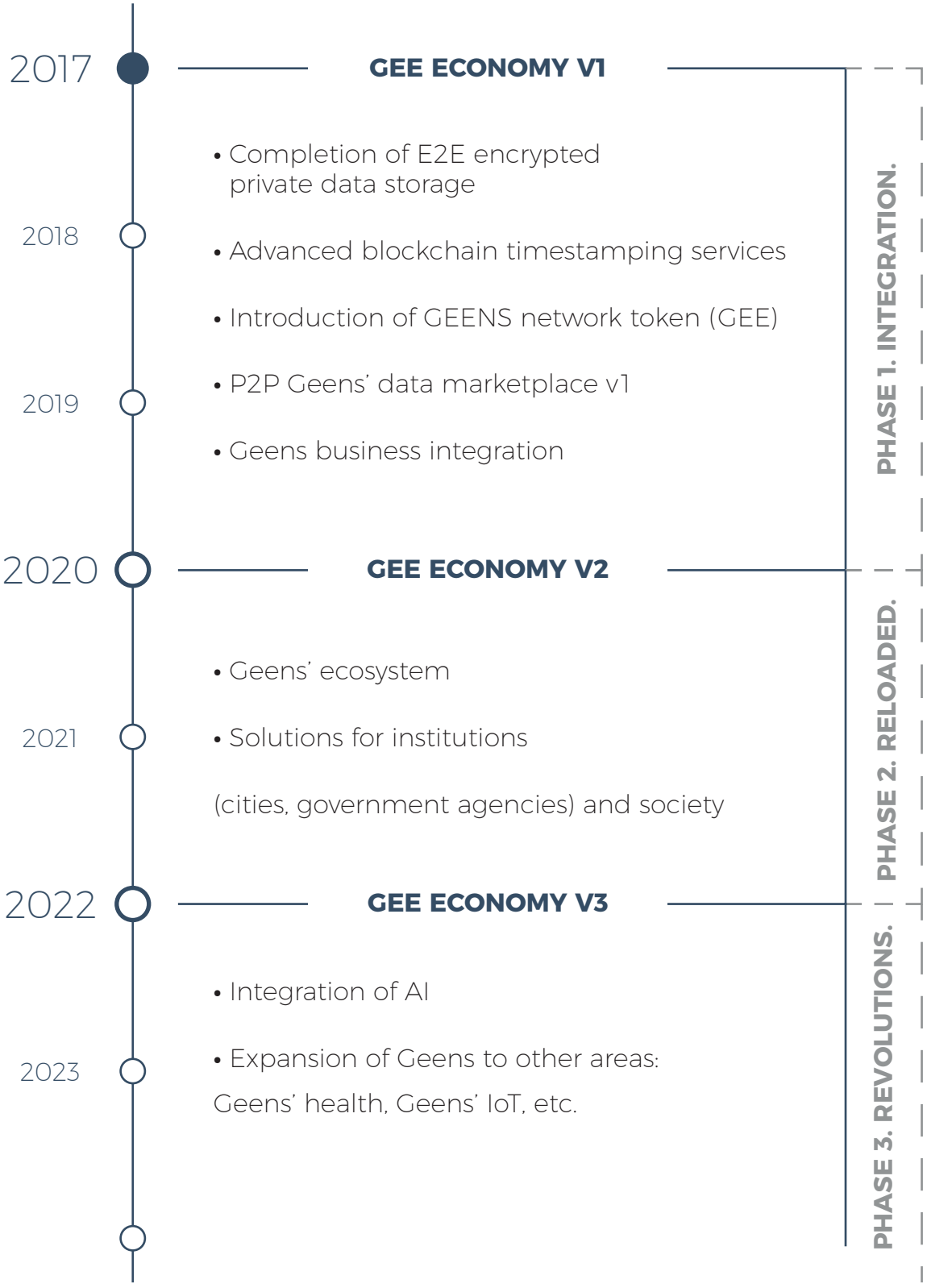
CASE 3

Protection of intellectual property and copyrights in GEE economy v1

Any private data, document and digital content stored on the Geens platform can be easily timestamped on a blockchain, and so an incorruptible and immutable timestamp that allows to certify the authorship of intellectual property or copyright is created. A license of usage and distribution of any content can be certified as well. In the event of a conflict of unauthorized usage of private data and breach of intellectual properties by a third party, the owner of such content will always be protected.

At the same time, a user who is struggling from a breach of intellectual properties at the Geens marketplace can receive support from the lawyers specialized on intellectual properties. A lawyer will be able to guide and manage all required procedures in order to claim and defend the rights. As in Case 2, the agreement of setting a breach of intellectual properties between two parties will be implemented via a smart contract.

A long-term vision of the GEE economy is based on 3 development phases. Phase 1, which could be called “Integration”, is dedicated for completing all activities outlined within the roadmap (see chapter 5). In phase 2, which is named “Reloaded”, the GEE economy v2 will be created. The main activity for the GEE economy v2 - is to complete the development of the Geens ecosystem and based on that to develop separate modules that could be offered as solutions for privacy and identity management to the state actors (cities, governmental agencies, etc.). Finally, in phase 3, "Revolutions", AI will be integrated in the Geens platform, and Geens will continue to expand to other areas, such as Geens health, Geens IoT, etc.



The scope of this whitepaper is to present the GEE economy v1 in detail. Therefore, the GEE economy v2 and v3 will not be comprehensively illustrated but are mentioned in order to show just the long-term vision of Geens.

4.7. NPO MODEL OF GEENS

Geens is a nonprofit organization (NPO) operating under Belgian law. A legal form of NPO provides the best ground for achieving Geens goals in the field of privacy management. Being a nonprofit organization Geens is able to achieve the maximum transparency and openness to bring the highest values for its members, and to be long-term oriented. All of those values are core to Geens. Geens as a nonprofit organization uses its surplus revenue to further achieve its goals – to constantly develop the Gee economy.

The main benefits of the Geens NPO are:

• Geens can never be acquired by anyone;

• Geens is fully independent;

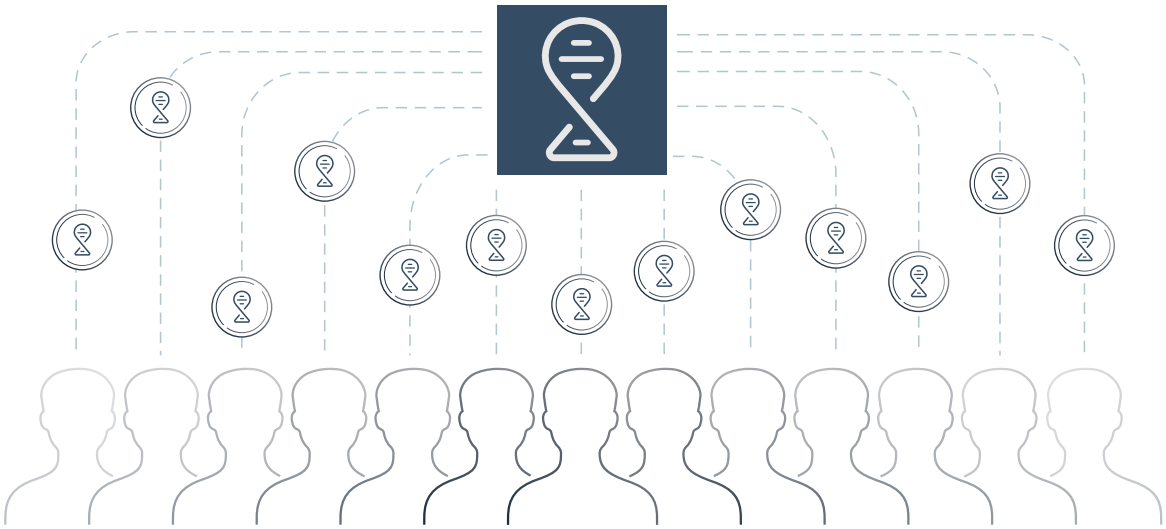
• Geens has indefinite life (all stored private data, timestamps, etc. have no time limits);

• Geens is fully GDPR compliant;

• The mission, goals and philosophy of the Geens NPO, and the organization remain bound by it;

• Any profit cannot be taken out from Geens, it will be returned back to members of NPO and will be used continuously to maintain and develop the Geens' project;

• Any member of the Geens NPO could actively participate in the management of Geens. A voting mechanism for NPO members will be introduced in the near future. Members of Geens will be able to vote and to decide on key projects and initiatives within the GEE economy.



Geens is supervised by the Ethical Committee. The Committee, which is formed from independent persons, follows the objectives of the Geens NPO. Every person can freely join the Geens NPO and enjoy the benefits. Membership of the Geens NPO is free of charge. Mission of the Geens NPO is to provide practical, secured, and easy tools to manage data privacy.

Key strategic initiatives of the Geens NPO are as follows:

1) a stable and secured private data storage platform, which is based on E2E encryption;

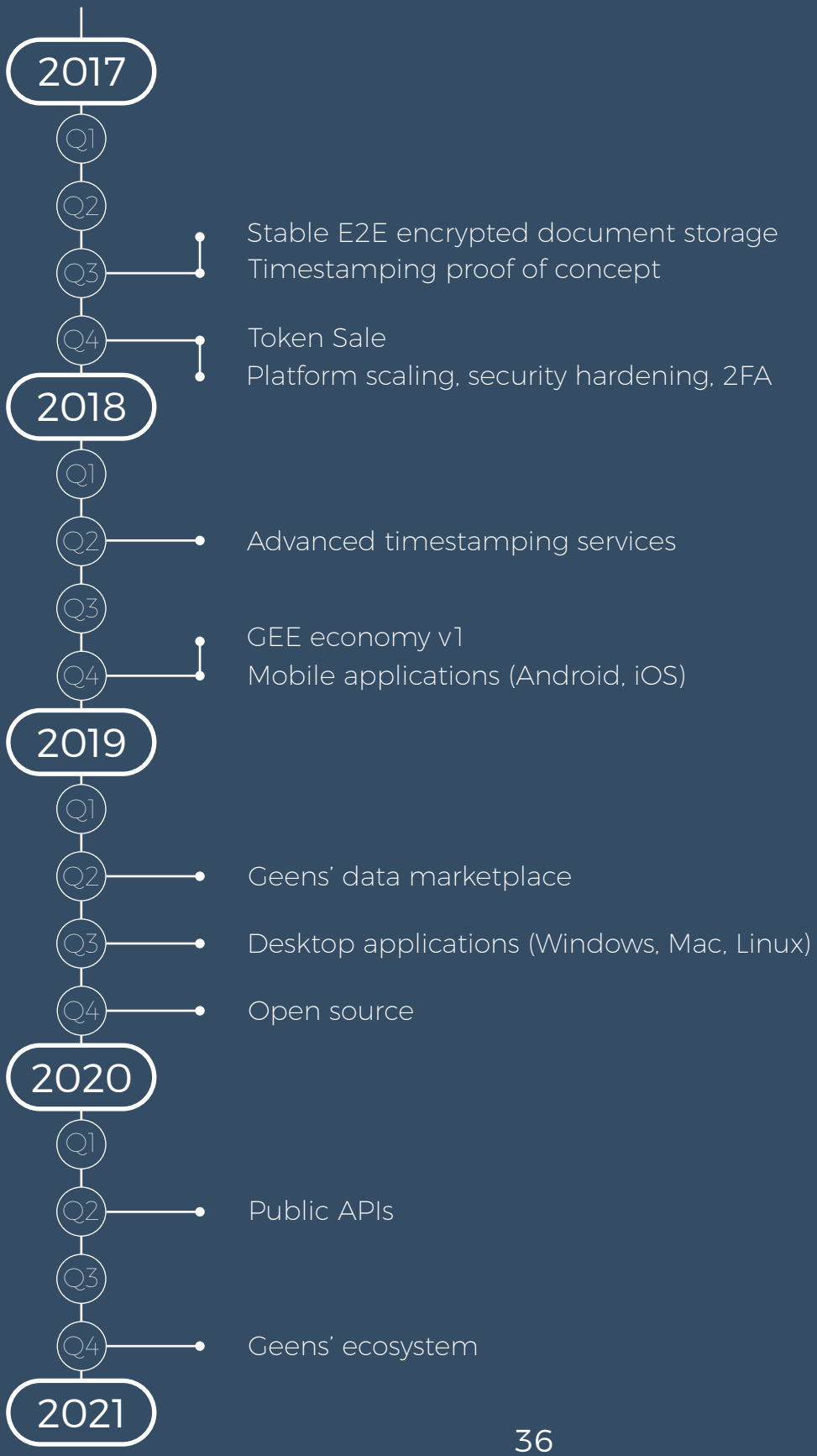
2) private data blockchain timestamping services, which are adopted in various areas of life;

3) exchange of data and services among the members of the NPO through the Geens Network Token;

4) The Geens data marketplace allowing to receive and provide data privacy services among the members;

5) The Gee economy.

5. ROADMAP


2017
Q1
Q2
Q3
Stable E2E encrypted document storage
Timestamping proof of concept
Q4
Token Sale
Platform scaling, security hardening, 2FA
2018
Q1
Q2
Advanced timestamping services
Q3
Q4
GEE economy v1
Mobile applications (Android, iOS)
2019
Q1
Q2
Geens' data marketplace
Q3
Desktop applications (Windows, Mac, Linux)
Q4
Open source
2020
Q1
Q2
Public APIs
Q3
Q4
Geens' ecosystem
2021

6. TEAM & ADVISORS

BOARD MEMBERS

JAAK GEENS

Entrepreneur, founder of Geens platform and president of Geens NPO

LINAS BUKAUSKAS

Assoc. prof. dr. of Vilnius University, vice president of Geens NPO

TEAM

GIEDRIUS CIBULSKIS

Geens platform designer and project manager

JULIUS SKAČKAUSKAS

Strategy, GEE Economy model

TIBOR VAJDA

Full-stack developer

MINDAUGAS VALANČIUS

IP lawyer, timestamping legal advisor

AGNĖ MAČIUKAITĖ

Smart contracts developer

DARIUS LOPETA

Full-stack developer

KLAUDIJUS VALINTĖLIS

Front-end developer

MINDAUGAS JANUŠKA

Crypto infrastructure supervisor

VIKTORIJA JANAVIČIŪTĖ

Sales

INGA IVANOVAITĖ

Legal advisor

PAULIUS ŠVAGŽDYS

Smart contracts developer

AIDAS ŠALTIS

Mobile apps developer

DENIS ORLENOK

Communication design

LINAS MAKAUSKAS

Motion graphics lead

CSABA TOTH

Back-end developer

JONAS JEGOROVAS

Developer, tester

INGA BARANAUSKIENĖ

Financial officer

GABIJA ENCIŪTĖ

Public relations

7. TOKEN DISTRIBUTION CAMPAIGN

In order to develop the roadmap of Geens and to create a self-functioning GEE economy, Geens will conduct a Geens Network Token (GEE) distribution. The GEE token sale will be issued by Geens.com, a Belgian non-profit organization. Participants willing to support the development of the Geens project can do so by sending Ethereum to the designated address.

Geens Network Token (GEE) distribution is summarized below:

Token name	Geens Network Token (GEE)
Ticker	GEE
Legal qualification	Utility Token
Structure of token distribution	4 Tier price structure
Currency accepted in GEE token distribution	Ethereum (ETH)
Price structure of GEE token, GEE/ETH	1 Tier, 3 days, 0.0006 ETH 2 Tier, 7 days, 0.00067 ETH 3 Tier, 10 days, 0.00074 ETH 4 Tier, 10 days, 0.00082 ETH
Total Geens Network Tokens (GEE) issued	100 000 000
Hard cap in GEE	67 000 000
Hard cap in ETH	40 200 ETH (~12 000 000 USD)
Soft cap in ETH	4 000 ETH (~1 200 000 USD)

% of GEE tokens offered to token distribution	67%
% of GEE tokens offered to the team	12%
% of GEE tokens offered to NPO community (partners, early adopters, social bounties, NPO foundation)	21%
Max. purchase amount	1000 ETH
Min. purchase amount	0.03 ETH
Date of token distribution start	7 of November
Date of token distribution end	7 of December

In case not all of 67 000 000 (67%) of Geens Network Tokens (GEE) will be sold to the public, the remainder will be burnt automatically by the smart contract.

The Geens Network Tokens (GEE) distribution will be finished when one of two conditions is met: 1) a hard cap of 40 200 ETH is reached; 2) Tier 4 of The Geens Network Tokens (GEE) distribution ends. When Geens receives ETH to the designated GEE token sale address, accordingly GEE tokens will be automatically credited to the same ETH address. GEE tokens will be locked on the ETH address of participants until the end of Token distribution campaign.

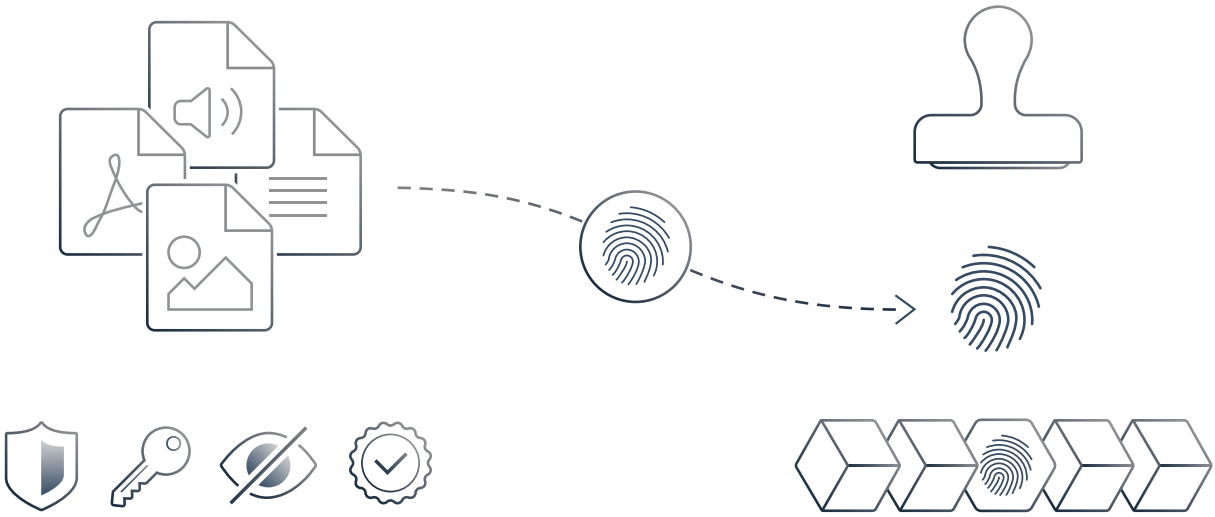
A portion of 21 % of GEE tokens will be distributed to the Geens NPO community and to its partners.

Geens

Encrypted document storage and blockchain timestamping services.

Both comprise a single unified product that allows users to privately store documents and timestamp them on the blockchain. End-to-end encrypted document storage is secure and private, the user is the only one who has the key, even Geens administrators cannot see users data,
Geens is GDPR compliant.

Some users timestamp their files, while other users work as legal assistants, consultants or validators and receive GEE Tokens in return for their services.



Geens is supervised by the ethical committee

It can never be sold to anyone

https://geens.com