Table of Contents

Introduction..............................................................................................................3

What is secrypto? .................................................................................................5
  Dedicated Hardware ..........................................................................................5
  Software ..........................................................................................................6
  Blockchain ........................................................................................................6

A perfect blend: Combining Secrypto and DigiSafeGuard ...............................7

Features of the hardware DigiSafeGuard .............................................................8

DigiSafeGuard use cases ......................................................................................9
  Anonymous Messaging and file transfer .........................................................10
  Hardware wallet ..............................................................................................11
  Login management ..........................................................................................12
  File encryption ...............................................................................................12
  Hardware and communication .......................................................................13

What makes DigiSafeGuard so secure and different? .......................................14
  How does AES 256 encryption work? ............................................................14
  How secure is AES 256 bits encryption? .......................................................14
  How hard is it to crack AES 256 bits encryption? ........................................14

Secrypto blockchain and coin (SCU) .................................................................16
  So, what exactly are “Hostnodes” and how do they work? ............................16
  How does Paid-Content-Management work? ................................................17
  Why external hosting facilities? ....................................................................18
  What is IPFS and SIA network? ..................................................................18

Coin Specs .........................................................................................................20

Closing Remarks ...............................................................................................21
1. Introduction

Internet and growing technologies have revolutionized almost every field in the world by providing ease of communication, by storage of large information data base, by providing access to global opportunities etc. Although internet and technology has overall made life easier but has made things a lot less private and secure. Also, it's hard to overstate the importance of encryption as well as anonymity.

What is encryption?

Encryption is the process of converting your private and sensitive data into codes using algorithm to protect it from being read and accessed by any unauthorized person. There are primarily two types of encryption namely symmetric-key encryption (private key encryption) and asymmetric-key encryption (public key encryption). Encryption protects your data, passwords, privacy, conversations and other details. Encryption plays a vital role in cryptography.

Only the private key holder can decrypt the messages. The cryptographic private key needed to decrypt the messages is stored exclusively on the endpoints. Thus, even the sender of the message cannot decrypt the data once it has been encrypted.

“Securrypto project” endeavors to provide next level privacy and security and make internet a much safer place by monetizing anonymous content distribution and by providing a secure, transparent and trustless system using blockchain technology.
2. What is Securrypto?

Securrypto is a ZeroCoin, Masternode based blockchain project focused on anonymous storage & transferring of encrypted data.

A market agitation technology by:
- Monetizing anonymous content distribution which also gives scope for new emerging market.
- Transfer or storing of untraceable encrypted messages & files across the internet.
- Linking to open source hardware wallet for an extra security layer.

All Achieved by a combination of specially designed:
- Dedicated hardware,
- Software and
- Blockchain

The following 3 unique key combinations (Software, dedicated hardware and blockchain) opens a wide and various door of opportunity to solve many internet related issues and at the same time add a secure, anonymous and privacy layer on the top of it.

a. Dedicated Hardware

It's commonly known that every software, even the one developed by the best in the field, will have bugs and flaws. Securrypto takes the integrity of the project to the next level by designing a dedicated open source hardware for the tasks and combining it to a visual verifiable communication technique which makes remote exploiting of vulnerabilities impossible. Meet 'DigiSafeGuard'!

DSG acts as a hardware wallet for storing and spending your digital assets.
It enables anonymous messaging through any unsecured channel.
2-factor authentication and password management functions are available in DSG.

In addition to above functions, DSG offers a lot more of handful and awesome features.

(Please refer section no. '4' for more detailed info. on features of DSG.)
b. Software

Securrypto software is designed to make a well-balanced system considering the aspect of user-friendliness, security & privacy.

Highest security level can only be achieved by right combination of hardware and software which are specially designed to match each other's functions.

Thus, DigiSafeGuard is obviously the most secure solution when used with Securrypto software and blockchain.

Securrypto is also accessible to anyone no matter what their economic status or geographical location is. The Securrypto software is open source and available to run on other devices covering:

- Linux
- Windows
- Android
- iOS

Any old smartphone or laptop can be converted to an air-gaped security vault.

So, whether you are looking for a safe to store your digital coins or earn some money for your uploaded work as a content uploader or maybe just looking to send encrypted messages without fear of another backdoor installed on your favorite app, Securrypto will achieve all that for you with the power of the blockchain and a team of security tinfoil hat people supporting it.

“Privacy is not a matter of having something hidden, but simply the right of what you want to share. Join the revolution and go now to www.Securrypto.io”

c. Blockchain

For a long time, privacy was a hard to solve issue as our privacy was dependent on trusting third parties. Unfortunately, because of this our privacy has been violated many times by multiple corporations and even governments. Blockchain technology has solved the "trust issue" as every data can now be verified without trusting any specific third party. Securrypto blockchain adds an extra privacy layer on top of every function it offers and at the same time creates a Paid-Content-Management which enables its users to get rewarded for their uploaded content.

Securrypto Blockchain is based on the PIVX using zPoS (Zerocoin protocol). Thus, maintaining user's privacy while using masternodes and staking principles.

Securrypto blockchain is not just another cryptocurrency-based project aimed for transferring of assets, but it's built as a proxy connecting masternodes to external hosting facilities like; IPFS, Sia, Amazon cloud etc.
3. A perfect blend: Combining Securptyo and DigiSafeGuard

Many innovations and betterment in products and services are being made nowadays by combining different technologies to form a single complex working module. In the past years, mixing or blending of different technologies has led to creation of many long lasting and disruptive products. People are combining existing and new emerging technologies to get an innovative outcome which is more advanced as compared to any previous existing version (if any).

Even individual technologies are disruptive and innovative, but value proposition and disruption they offer often tend to increase significantly when combined with a preexisting or a new emerging technology. For example, Artificial Intelligence has been around for a long time and its disruptive potential has been widely discussed but no solid implementation was done unless emergence of Cloud, Big Data technologies, and low-cost compute. Now, Artificial Intelligence is a key component to any enterprise strategy.

IoT, Machine Vision, Data Discovery, Artificial Intelligence, 3D printing, Blockchain and many more leading technology products were built by bringing together various technologies and innovations together to create significant gains in value as well as its applicability. Traffic monitoring and control in smart cities is made much more convenient by combining computer vision, machine learning, 5G and cloud. Even in crypto world, combination of blockchain and smart contracts has produced a disruptive outcome. Two or more disruptive technologies when used in right combination can work as a charm for any new business module or product.

It’s the same with Securptyo. Here, we plan on taking the security and privacy to the next level by combining software, hardware (DigiSafeGuard) and blockchain for the first time. Use of blockchain technology ensures that our system is transparent, trustless and most of all secure. Securptyo and DigiSafeGuard leverage one another to enhance their collective value. DigiSafeGuard (DSG) is surely the most secure product as Securptyo software blends perfectly with it and provides unmatched privacy and security.

Some key advantages achieved by combining Securptyo (software) with DigiSafeGuard (hardware) are: (for detailed info. Refer section 5.)

1. Decrypting is processed on DigiSafeGuard which is secured unlike any other smartphone or computer.
2. Users can use the device (DigiSafeGuard) keyboard to enter the password phrase which is also secured unlike any other smartphone or PC.
3. DSG is an offline device and hence, hackers can’t simply gain access to a device that has no connection to outside world.
4. DSG has a military grade cryptography based on AES encryption.
5. Being open source, there is no scope for any backdoor.
4. Features of the hardware DigiSafeGuard:

- Securely store and spend your digital assets like Bitcoin etc. using DSG device which will act as a hardware wallet.
- Securely send and receive messages and files using any open and insecure channel like WhatsApp, Telegram or email.
- Login securely to online services like Gmail, Facebook, Twitter, banks etc.
- Keep all your accounts and login credentials protected and encrypted on your DigiSafeGuard device.
- Encrypt any sensitive file or directory and keep them safe and secure.
- Easy to use for everyone, even if you don’t understand how encryption works.
- Users can use any insecure channel, even a compromised PC or Smartphone as every byte leaving DSG device will already be encrypted.
- Users don’t need to trust any third-party, not even the Securypoto team to secure their cryptocurrency assets, as they can use any random / widely available services to create unsigned transaction for spending their cryptocurrencies and let the DigiSafeGuard sign the transaction.
- Users can use any publicly available crypto software to decrypt their files and messages as we use well known and documented public AES encryption protocol.
- Users can create, import, export and verify their own RSA key.

*(What is RSA? RSA key is needed to encrypt and decrypt data, refer Wikipedia for detailed technical information)*
5. DigiSafeGuard use cases:

- Anonymous Encrypted Messaging.
- Anonymous Encrypted File transfer.
- Hardware wallet.
- 2FA & Login management.
- Standalone Data Encryption device.
- Hardware Data vault.

Securrypto is not just a gimmick, giving a sense of security, but designed by death or alive thoughts premise)
a. Anonymous Messaging & files transfer:

Like most of the other security/privacy-oriented apps, DigiSafeGuard uses end-to-end encryption as this has already been covered many times and is known to be the best encrypted solution for secure communication. So, we are only going to point out some of the most important differences that make DigiSafeGuard a better choice.

For designing the DigiSafeGuard messaging and files transfer options we asked ourselves a very simple question which everyone would ask before using such an application: Why should I trust this application and its developers? The answer is simple, you shouldn’t. Yes, you heard that right because DigiSafeGuard & Securrypto has been designed in a trustless way. It means that the user does not need to trust anyone, not even the developers of DSG.

So, how does DSG provide such a system?

- DSG lets users create their own RSA key and export it on demand.
- DSG lets the users import their own (somewhere else created) RSA key.

This is very important as otherwise you can't be sure about the integrity of the system. Using end-to-end encryption without letting the user see, create and or import/export his own key is simply a huge security risk.

Next important thing which is again unique about DSG is the “data transfer method” which eliminates any gain from building backdoors or other hidden vulnerabilities. This means that even if we are asked to build a backdoor, it would be useless (See the communication section for more detailed info.). Sending a secure message will be achieved by the following sequences:

1. When using DSG for the first time, user will setup the device by creating a new RSA phrase enabled key pair.
2. Public key can be published online or sent to anyone that would like to send you messages.
3. User type’s his/her message on the DSG device and message will get encrypted using the RSA private key. As all this are done on a device without any connection to the outside world, there is no scope for being comprised remotely.
4. DSG creates QR code from the encrypted data which can now be sent using any unsecured channel like WhatsApp, Telegram, email etc.
5. Receiver scans the QR code which again happens on the DSG device having no connection to the outside world and can decrypt the message knowing that the message hasn't been (couldn't be) read on its way by anybody.

Encryption of large data are also done using the same protocol. The only difference is that a random generated 32ch long key is used to encrypt the data which will indeed be encrypted by RSA and sent together.
b. Hardware wallet

As DSG is a secure vault, it is the obvious that it can also be used as a hardware wallet. Hardware wallets are the only secure way to store and spend cryptocurrencies. As the basics of all currently available hardware wallets are the same, we are only going to point out the main differences that make DSG more secure and a better choice for storing small to large amounts of cryptocurrencies.

- DSG does not rely on any security chips. In other hardware wallets, there are many different levels of available security chips and due to this we need to trust the manufacturers about not having a backdoor. Whereas, on the other hand DSG encrypts the seed by the user generated phrase enabled with 4096 bits RSA key therefore providing no scope for creation of a backdoor even if we want to or we are asked to. This makes it much more safe and secure than other hardware wallets.

- Using RSA key encryption, DSG can store and spend directly from paper wallets without sweeping. Paper wallets are secure against any remote attack but if you want to spend from a paper wallet you need to take a huge risk by sweeping to a Smartphone or desktop wallet. Many old investors still have paper wallets that are worth a lot these days. You really don’t want to store a huge amount into any Smartphone or computer which can easily be compromised. And of course, DSG also offers traditional HD wallet option having your own 24 recovery seed.

- DSG is basically a well pre-configured small pocket size air gapped PC. Ready and configured to use for many different coins. This alone is a huge thing as users don’t need to install and configure many different wallets on an offline PC. Communication goes only by QR codes which provides users with the option to verify every single byte leaving DSG device. User is not forced to use DSG services to create his/her transactions and can use many other online wallets. This reduces the chance of collusions and backdoor creation. The main goal of DSG is to create protocols that eliminate the need of “trusting any third parties”.

- Private keys will never leave DSG and will always be stored in encrypted mode using the 4096 bits RSA key.

As with everything, there is always a tradeoff between user-friendliness and security. “You can’t take a bank vault with you on the road and you cannot put millions in your pocket.” DSG isn’t built to compete with the current hardware wallets but has been created to add a higher level of security to it. Depending on the amount of assets that needs to be stored/secured, you need to wisely choose the best possible vault. Our recommendations are:

- Smartphone, Desktop: amount < 500 USD
- TREZOR, Ledger, KeepKey: amount < 5000 USD
- DigiSafeGuard: from any small amount to amount > 5000 USD
c. Login management

Using the RSA encryption integrated to the DSG security design, users can save their login credentials for online services like Gmail, Facebook, Banks etc. to automate the login process without saving anything in the browser. DSG can also be set to function two factor authentication (2FA) if extra security is needed.

d. File Encryption

Using the RSA encryption integrated to the DSG security design, users can encrypt files and directories or even an entire hard disk for his own use or to send to any specific person. Users can encrypt an entire USB flash using receiver’s public key and by doing so, only the receiver will be able to decrypt the USB flash and read the files. Sending a secure file will be achieved by the following sequences:

1. Sender puts the USB flash in his/her DSG device.
2. Sender’s DSG device encrypts the data using receiver’s public key.
3. Sender gives the USB flash to the receiver. (Encrypted data can also be sent using internet)
4. Receiver puts the USB flash in his/her DSG device and decrypts it using his own private key.

Encryption using RSA is not an innovation and has been in existence for more than a decade and has still not been compromised. However, it’s difficult for the average person to use it in a correct and secure way. What DSG does is, it makes the use of an advanced encryption algorithm which is simple enough to be used by anyone and eliminates any human errors that might occur. This creates many use cases of DSG device. Some real-world applications would be its use by corporations or government institution that need to handover highly sensitive information from one department to another. Without having to invest in security courses by educating every employee to become an encryption expert, you can easily move encrypted data and be sure of security and the integrity of it by using a DSG device. You would expect normally that big corps or government departments have taken care of these issues, but the reality is far from this as we see frequently in the news that someone accidentally lost sensitive information saved on a USB device on the street again. If you can manage your Smartphone, you can use a DSG device or software. It’s that simple! By simplifying the complex encryption steps, we can get DSG to be quickly adopted by people all around the globe.

e. Hardware & Communication

Easiest way to secure your desktop from remote intruders is by cutting your internet cable. But, unfortunately that will also cut you off the internet.

As mentioned before it’s always a tradeoff between security and ease of use. However, sometimes your first and foremost biggest concern is security like storing your cryptocurrencies or encrypting a highly sensitive message. This is when you are willing to take couple of extra steps to sleep well at night.
DSG device does not have any Bluetooth, WIFI, Ethernet connection or GPS. The online connectivity part is simply removed. So, it's not capable of making any connection even if you load it by any vulnerable software. Therefore, even building a backdoor would be useless and users no more need to trust the developers.

One of the reasons that hackers can get in and out of your computer (virtually) is because you can't see it. It's all in virtual world and not everyone in this world is a computer geek. So, we chose to use a visual method for the DSG communication. This way at any given moment, user can scan and see what exactly is leaving or entering his/her DSG device.

There is a tradeoff as you can't move huge amount of data using QR codes. But for sending messages and spending your bitcoin QR code data capacity is good enough. We have also developed a way to play and read multiple QR codes playing in a robe to move 10x more data just in couple of seconds. (To get a better idea, watch our video on our official website https://www.digisafeguard.com)

Whenever there is a need to move larger data files, users can simply use a USB flash to copy large encrypted data.

Although DSG hardware is open source, to make it widely accessible DSG software will also be available on different platforms such as Linux, windows, Android and IOS. This way any old/new laptop or Smartphone can be converted into a secure digital vault.

Using other hardware's will decrease the security level as there is a big chance that they will have a built-in Bluetooth or Wi-Fi and in conjunction with a backdoor software it will become less secure. The odds are very small, but any security related matter should be taken seriously.

Availability of open source software for other platforms will give people easy and cheap access to a personal digital vault and as they are probably more technical oriented crowd, they do understand the risk and calculate this to their use cases.

To make DSG as widely used as possible we are trying to integrate it to the current daily used devices like smartphones and wearable android watches. To achieve this, a Lite-version of the software is under development which will be used on android watches etc. This will turn any Android wear to a hardware wallet and a secure messaging device instead of just eating dust in the closets or being used as a showoff.
6. What makes DigiSafeGuard so secure and different?

- **AES (Advanced Encryption Standard) 256 bits encryption.**

  6.1 **How does AES 256 Encryption work?**
  AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256-bits, respectively.

  6.2 **How secure is AES 256 bits Encryption?**
  The cipher AES-256 is used massively in SSL/TLS across the Internet. It's considered among the top ciphers. In theory, it’s not crack able since the combinations of keys are massive.

  6.3 **How hard is it to crack AES 256 bits Encryption?**
  Breaking a symmetric 256-bit key by brute force requires 2128 times more computational power than a 128-bit key. Fifty supercomputers that could check a billion (1018) AES keys per second (if such a device could ever be made) would, in theory, require about 3×1051 years to exhaust the 256-bit key space.

- **RSA 4096 Key is generated on the device self.**

- **RSA Key is phrase protected.**

- **User uses the device keyboard to enter his password phrase and not some unsecured keyboard of Smartphone or PC.**

- **User uses the device screen to read his messages and not some unsecured screen of Smartphone or PC.**

- **DSG device keeps all users’ private keys in the encrypted mode.**

- **Decrypting will be processed on the DigiSafeGuard device and not on an unsecured Smartphone or PC.**

- **DSG device uses only visible QR code to communicate to the outside world and can always be verified.**

- **Users can also use the one-way dongle to transfer the encrypted data and be in control all the time.**

- **Hackers can’t simply gain remote access to an offline device that has no connection to the outside world.**

- **DSG is the most secure digital vault which uses military-grade cryptography based on AES for anyone that wants real security and privacy and not just a gimmick.**
As stated above, many technical and complicated features are already solved and included in the software. But there are still other not mentioned breakthrough solutions (beside specific designed hardware and QR code communication method) that give DSG his unique powers.

1. **Securrypto is open source and the software is designed to be modular.**

   **What is open source software?**
   It is a denoting software for which the original source code is made freely available and may be redistributed and modified. Therefore, this gives everyone the opportunity to add extra free or commercial features as an add-on.

2. **In conjunction with Securrypto blockchain, user will have anonymous protection layer on the top of all the available features to protect his/her privacy rights.**

Highest security level can only be achieved by a combination of matching designs of hardware and software, therefore DSG hardware will obviously be one of the most secure solution. However, to make DSG accessible to everyone despite of his economic status, DSG software will also be available to run on other devices such as smartphones, laptops, etc. using Linux, Windows, Android and IOS.

*(Every old/new Smartphone or laptop can be converted to a DSG security vault. Best of all, DSG hardware and the software is “open source”!)*
7. Securrypto blockchain & SCU coin

Securrypto blockchain is what adds a privacy layer on the top of all the features offered by the dedicated hardware (DSG) and the software. At the same time, it creates a Paid-Content-Management which enables the users to get rewarded for their uploaded content and the hosts to get paid for their hosting facilities.

Securrypto Coin “SCU” empowers transferring of large anonymous encrypted data and monetizing content distribution at the same time.

Securrypto blockchain is built as a proxy connecting masternodes to external hosting facilities.

- Masternodes get paid by the uploaders. So, there will be an emerging market for hosting of the encrypted files and messages.
- Content uploaders can choose to get paid by the downloads, therefore an emerging market for uploading new content to the network will develop.
- Masternodes include the file location and receiver’s public key on to the blockchain using an onion-based protocol like TOR network.
- There will be no link between the sender & the receiver of messages or files.
- Thanks to AES encryption, only the targeted receiver can read the files.
- Sender & Receiver can exchange keys without compromising their privacy. Full anonymity is finally here.

Securrypto blockchain is based on “POS” and every node will also function as a gateway to hosting facilities. This way users using small devices such as a Smartphone won’t need to run any full nodes. Full Nodes are ideally a VPS server having a 99% uptime and fast connections. Nodes use their own internal or other external storages. For example, connecting to Sia network or use IPFS for files storage. We will call them “Hostnodes”.

7.1. So, what exactly are “Hostnodes” and how do they work?

Securrypto “Hostnodes” are basically a gateway relay between user and different decentralized storage platforms and at the same time it integrates a payment system which allows content providers to get rewarded for their contributions while maintaining the anonymity of the users.

- As Hostnodes will get paid by the sender/uploader, so there will be an emerging market for hosting of the encrypted files and messages.
As sender (content uploader) can also get paid directly from receiver/downloader (if he/she chooses to), there will be an emerging market for uploading of new content to the network too.

The best way to explain the process in simple words is by using a real-life example: When submitting a message or file, Smartphone user (client) makes a connection to one of the many Hostnodes and gets a list of approximately 100 random Hostnodes. From this list client will select randomly one and make a connection to it. Client also saves this list for the next time as list will be updated every time client connects and requests one. So, client connects every time to another random node. This eliminates prediction ability to which Hostnode targeted client will be connecting the next time.

Client sends the encrypted message to the just freshly connected Hostnode and upload message/files in conjunction with public key of the receiver. Hostnode will save the file or message for x-days (depends on selected preference) on another random Hostnode and pay a hosting fee to the second Hostnode as he is not going to host it by himself and just earn some coins to function as a relay/proxy. This will also eliminate IP tracking. Client can pay more and save it to as many Hostnodes as he wants for redundancy purposes. For example, when a client pays 3 coins, 1 coin goes to the relay and 2 coins go to the host. Paying 5 coins means hosting on 2 Hostnodes for redundancy. Obviously, this is a simple example, in real life application the required amounts will be calculated based on the file size, host duration, redundancy count etc...

Second Hostnode that is hosting the file or message by himself or by submitting to IPFS network or Sia network will submit the receiver public key and the IP of the hosting hostnode to the Securrypto blockchain. This way receiver can search and connect to the hostnode that have saved the files or message and download it.

Receiver checks the blockchain for his/her transaction and downloads it from the Hosting facility.


If sender/uploader chooses the paid-content option, receiver needs to pay requested amount of coins before downloading. Files and especially the larger ones will be split and saved on different Hostnodes. This way nobody will host full data. Hostnodes need to have locked x-amount of coins as collateral. Setting up new Hostnodes is easy as everyone can start a Hostnode by simply renting a Linux VPS server and running the install script which downloads DSG Hostnode software from github and installs it on the VPS. During the installation process, one can put his/her DSG address, external storage credentials if any etc...
One can setup 100’s of Hostnodes across the globe in less than a week and pay for the VPS’s yearly and just forget about it, thus generating daily revenue.

Therefore, advantages of such system are:

- Onion based anonymous data transfer.
- Spider network distribution.
- Monetizing by becoming a host.
- Monetizing by becoming a content creator and or uploader.
- Monetizing by Pay per view/Download.

7.3. Why external hosting facilities?

Hostnodes can use their own internal storage, but the real power of Securrypto is its relay ability to connect to other hosting facilities that have hosting content as their core business like IPFS and SIA network. This assures that Securrypto is kept focused on what it does best, that’s ‘Security’! and leave the hosting job to the parties that are specialized in data hosting.

7.4. What is IPFS and SIA network?

Interplanetary File System is a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. IPFS is an open-source project developed with help from the community.

IPFS seeks to create a permanent and distributed web. It does this by using a content-addressed system instead of HTTP’s location-based system.

Instead of using a location address, IPFS uses a representation of the content itself to address the content. This is done using a cryptographic hash on a file and that is used as the address. The hash represents a root object and other objects can be found in its path. Instead of talking to a server, you gain access to this “starting point” of data. This way the system leverages physical proximity. If someone very close to me has what I want, I’ll get it directly from them instead of connecting to a central server. To accomplish this, IPFS synthesizes a few successful ideas from other peer-to-peer systems like Bit Torrent.

An HTTP request would look like “http://10.20.30.40/folder/file.txt”

An IPFS request would look like “/ipfs/QmT5NvUtoM5n/folder/file.txt”
To store data, IPFS uses a Distributed Hash Table, or DHT. Once we have a hash, we ask the peer network who has the content located at that hash and we download the content directly from the node that has the data I want. Data is transferred between the nodes in the network using mechanisms like BitTorrent. A user looking for some content on the IPFS web finds neighbors who have access to that content. They then download small bits of the content from those neighbors. On top of the DHT and the Bit Torrent protocols, IPFS uses a Merkle Tree. This is a data structure like the one Git uses as a version control system and the protocol used in the bitcoin blockchain. In Git, its used to track versions of source code, whereas in IPFS it's used to track content across the entire web. Securrypto adds anonymity and paid content system on top of this genius decentralized way of content distribution by using blockchain technology.

SIA network is another way of storing data in a decentralized way across the internet.

SIA is a decentralized, peer-to-peer network for buying and selling computer storage space. Users pay for transactions within Sia using a cryptocurrency called Siacoin. The SIA Storage Platform leverages underutilized hard drive capacity around the world to create a data storage marketplace that is more reliable and has lower cost than traditional cloud storage providers.
8. Coin Specs

SCU is an utility coin having a real world usage, required to transfer anonymous encrypted data on Securrypto blockchain and monetizing content distribution.

a. Max supply:

Max coin supply: 320,000,000

Securrypto has one of the lowest premine allocation (10%) and the majority of the premine coins is spent directly on marketing and development as shown below.

Securrypto is here to enrich users life worldwide and not the founders pocket. All excess coins from the airdrop, bounty’s, faucets, promotion team etc... will be burned. This creates more scarcity and prevent of coins concentrations in control of one single entity.

b. Premine allocation:

<table>
<thead>
<tr>
<th>Treasury Reserves</th>
<th>5 million</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing, Bountys Hunters</td>
<td>5 million</td>
</tr>
<tr>
<td>Marketing, Faucets</td>
<td>5 million</td>
</tr>
<tr>
<td>Marketing, Partnering</td>
<td>5 million</td>
</tr>
<tr>
<td>Development Blockchain</td>
<td>4 million</td>
</tr>
<tr>
<td>Marketing, Promotion Team</td>
<td>3 million</td>
</tr>
<tr>
<td>Development DSG Hardware</td>
<td>3 million</td>
</tr>
<tr>
<td>Marketing, Airdrop</td>
<td>2 million</td>
</tr>
</tbody>
</table>
9. Closing remarks

Securrypto is Anonymous Masternode based blockchain project focused on anonymous storage & transferring of encrypted data. Maximum security can only be achieved by combining matched design of hardware, software and blockchain together.

DigiSafeGuard use cases are: Anonymous Encrypted Messaging, Anonymous Encrypted File transfer, Hardware wallet, 2FA & Login management, Standalone Data Encryption device, Hardware data vault.

We have designed a dedicated open source hardware which is named DigiSafeGuard (DSG) to level up the security even further. A physical secure digital vault in the palm of your hand for Crypto Payments, Secure messaging, Password management, File encryption and much more. DSG is specially designed to work and interact with Securrypto blockchain to maximize your security & privacy (for more information about this dedicated Open Source Hardware wallet, please visit the DigiSafeGuard website https://www.digisafeguard.com and watch the videos).

We use blockchain technology to ensure that our platform is trustless, secure and transparent. Securrypto is launching a native currency token (SCU) which will enable users to pay or get paid for downloaded or uploaded content respectively and will empower transferring of large encrypted data anonymously as well as monetizing content distribution at the same time.

Also, most importantly securrypto is open source software which enables it to be redistributed and modified by the users.