digipulse

Disclaimer

Disclaimer: this document (hereinafter referred to as “White Paper”) establishes and defines the principles upon which Digipulse, as a service and company will operate, regarding both the business model, as well as the technical solution. The information in the White Paper is subject to change - all changes can be found under the section “Revisions to version”. Please refer to “Terms and Conditions” found at www.digipulse.io for full details.

Abstract

Digipulse service is a decentralised cloud storage with an automated transfer of ownership based on the activity signals received from connected API integrations. It operates as a subscription-based SaaS platform.

The project aims to ensure that all user’s digital assets and crypto wallets can be stored on a decentralized storage, in an encrypted manner and can automatically be transferred to recipients chosen by the original holder, based on pre-set conditions.

As cryptocurrency increases in both circulation and value so does the necessity to secure digital asset longevity and transfer/distribution mechanism. And seen how complete digitalization is still at a relatively early stage, most online services do not consider the potential digital asset loss of their users a legitimate problem.

Contents

The Problem

New innovations and products adapted by the market undoubtedly create new problems. Cryptocurrencies are a virtual form of assets (depending on the jurisdiction) protected by unbreakable cryptography. This attribute makes them a secure way of storing wealth but also creates the risk of forever losing access to one's digital wallet in case of death or loss of memory. This can become a major problem for the relatives of individuals who have invested into an ever growing cryptocurrency market[1].

Due to the characteristics that random modifications and forgery on the records is almost impossible, attempts have been made to use the blockchain in financial asset transactions of the financial institutions as well as general contracts (referred to as "Smart Contract") such as transfer of ownership, inheritance and succession[2]. Blockchain takes the ledger with its transaction details and distributes it into a P2P network, making the participants record and manage the details jointly, instead of placing them into a central organizational server. This process resolves the high cost of network management and increasing hacking issues.

Opportunity

The decentralisation era has provided us with the perfect timing for setting up an asset encryption and distribution storage service. This technology enables Digipulse to encrypt, split and store information on multiple devices across the world, thus ensuring that we as a service provider don't have access to the information a user wishes to encrypt (a decentralized storage) and the threat of internal risks which come from human resources is mitigated enormously.

In addition, we have created a solution that deals with the transfer access send-out in an automated way, namely the "Pulse network", which consists of multiple web based integrations that are utilised to pass on the contents stored online by the user. This allows us to create a subscription-based service with an ideal product fit for the existing cryptocurrency sphere and the 'digital era' in general.

Project creation

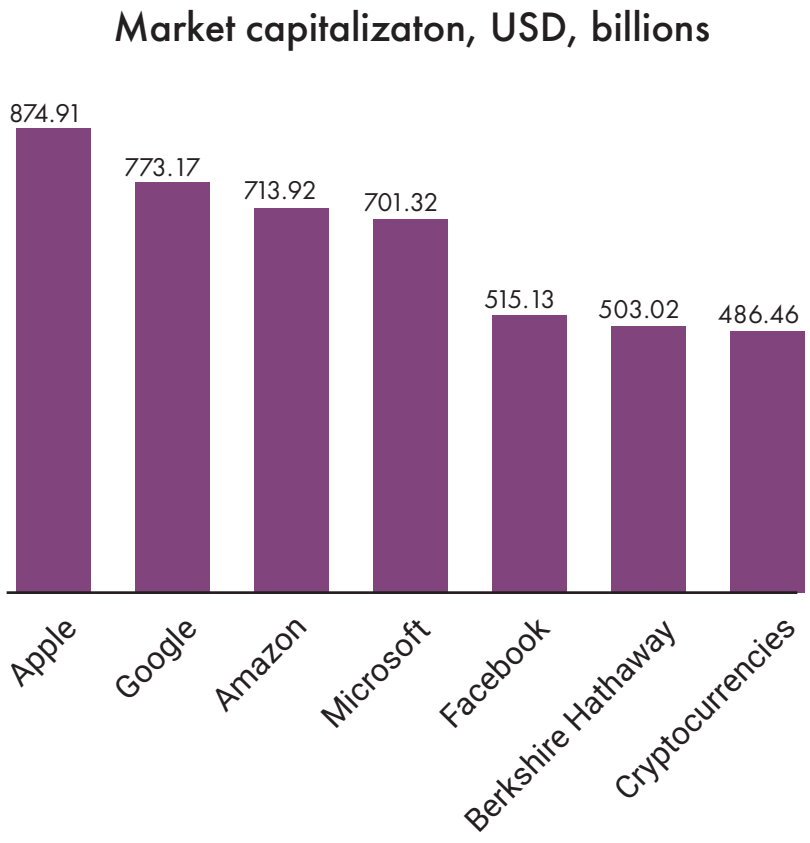
Digipulse was launched in 2016. The concept was developed by a founding team member whose previous ventures provided him with in-depth expertise in the fields of fundraising, IT and psychology. The idea, which originated during his prior employment, was as simple as it was eye-opening: original, non-physical asset owner being unable to access their assets could create large financial losses either for their employer or the individual's family members.

The idea gained additional spin when the cryptocurrency aspect was added to the initial idea of storing memorabilia and valuables. Extensive market analysis indicated no existing services that fulfilled the needs of the initial team members, so we set out to create one ourselves. That service is Digipulse.

Industry analysis

General description

To better understand the size of the cryptocurrency market, one can look to the S&P 500 rating (The Standard & Poor's 500 - the top 500 largest companies by market capitalization listed in American stock exchanges). By comparison, cryptocurrency market capitalization would be in 7th place (as of February 21st, 2018)[3].



And while unbreakable cryptography is an advantageously fundamental part of the entire cryptocurrency sphere, it does have a glaring flaw - it's alarmingly easy to lose, destroy or make cryptocurrencies otherwise unattainable.

In fact, Bitcoins and other cryptocurrencies may even disappear forever because of this. When all 21 million Bitcoins are mined by the [estimated] year 2040, the actual amount available for trade or spending will be significantly lower. According to a research study done by digital forensics firm Chainalysis, 3.79 million Bitcoins are already lost forever, accounting for 23% of all Bitcoins mined to this day.

In monetary terms, the amount currently lost in asset value reaches up to about 40.7 billion USD. But since the market capitalization for Bitcoin (out of all the cryptocurrencies) reaches 39.3%, and fundamentally other cryptocurrencies are subject to the same risks, the total amount of asset value lost is much higher.

More Bitcoins are expected to be lost in the future, but at an assumedly much lower rate due to their increasing (albeit fluctuating) value. This problem not only affects cryptocurrency holder families, but the entire cryptocurrency ecosystem as well. It is therefore paramount to adapt a sustainable industry-encompassing solution.

Demographics and segmentation

Bitcoin, a virtual global currency, has been the topic of much media, internet and policy discussion. Little is known about the characteristics of Bitcoin users, even though thousands of businesses accept them as payment. Transactions with Bitcoin are near anonymous due to the cost associated with identifying a user's electronic signature. Although some convenience sampling of Bitcoin enthusiasts exists, no systematic data collection has been done.

Since Bitcoin is by far the largest and oldest cryptocurrency, it is safe to assume, that the largest proportion of cryptocurrency users are those who own Bitcoin. Because of theoretical anonymity achieved due to cryptocurrency encryption, it is very costly to identify the user amount of cryptocurrencies and their demographics. But there are some data available that allows us to describe the market situation of Bitcoin and their user base.

Since all the transactions that have ever taken place on the blockchain are publicly available through blockchain explorers, it is also possible to estimate the number of Bitcoin addresses.

Unfortunately, while transactional information, such as balance, Bitcoin address and the value of the amount is in the public domain, as is the number of addresses involved, time of the transaction and volume, the parties involved remain private. Nevertheless, this information allows us to estimate the amount of Bitcoin (see table Bitcoin distribution) in circulation.

Bitcoin distribution[5]

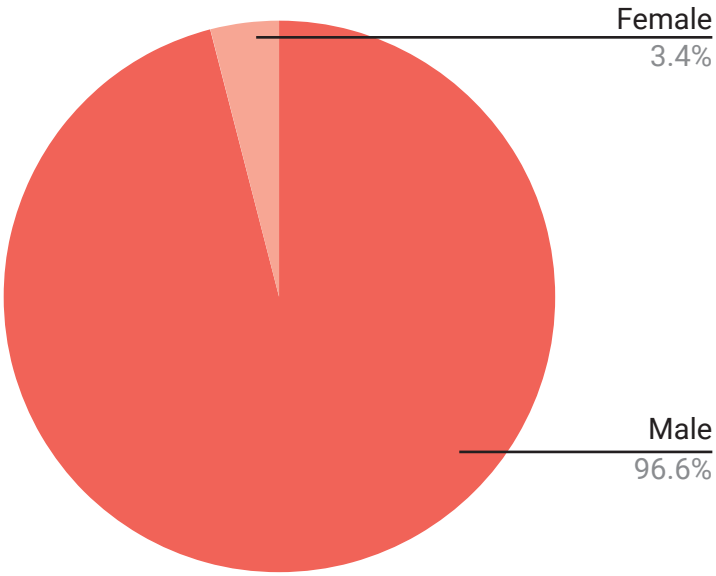
Balance	Addresses	% Addresses (Total)	Coins (BTC)	$USD	% Coins (Total)
0 - 0.001	13385914	53.98% (100%)	2,250 BTC	23,733,656 USD	0.01% (100%)
0.001 - 0.01	5016253	20.23% (46.02%)	21,085 BTC	222,455,743 USD	0.13% (99.99%)
0.01 - 0.1	4006926	16.16% (25.79%)	128,841 BTC	1,359,301,448 USD	0.77% (99.86%)
0.1 - 1	1693874	6.83% (9.64%)	542,740 BTC	5,726,053,352 USD	3.23% (99.09%)
1 - 10	546768	2.2% (2.81%)	1,444,564 BTC	15,240,533,240 USD	8.6% (95.86%)
10 - 100	131722	0.53% (0.6%)	4,360,854 BTC	46,008,165,702 USD	25.96% (87.27%)
100 - 1000	15734	0.06% (0.07%)	3,723,546 BTC	39,284,394,010 USD	22.16% (61.31%)
1000 - 10000	1534	0.01% (0.01%)	3,369,186 BTC	35,545,802,104 USD	20.05% (39.15%)
10000 - 100000	108	0% (0%)	2,882,716 BTC	30,413,419,283 USD	17.16% (19.1%)
100,000 - 1,000,000	2	0% (0%)	325,514 BTC	3,434,260,001 USD	1.94% (1.94%)

There are a total of 24,798,835 Bitcoin addresses as of February 21,2018, belonging to roughly 0,326 % (24798835 / 7,603,569,330 * 100 = 0,326%) of the global population. Unfortunately, it is difficult to determine the precise number of Bitcoin users, but the amount of addresses can provide some approximation.

The data also reveals that Bitcoin distribution amongst its users is uneven. Out of all the addresses, the largest amount of Bitcoin addresses (53.98%) contain less than 0.001 Bitcoin, whilst the biggest amount of Bitcoins are in 0.6% of all the addresses, which contain 67.22% of all the available Bitcoins.

While it is possible to gather Bitcoin address data, researching the characteristics of the audience engaged in the crypto community requires other methods.

Bitcoin community engagement by gender



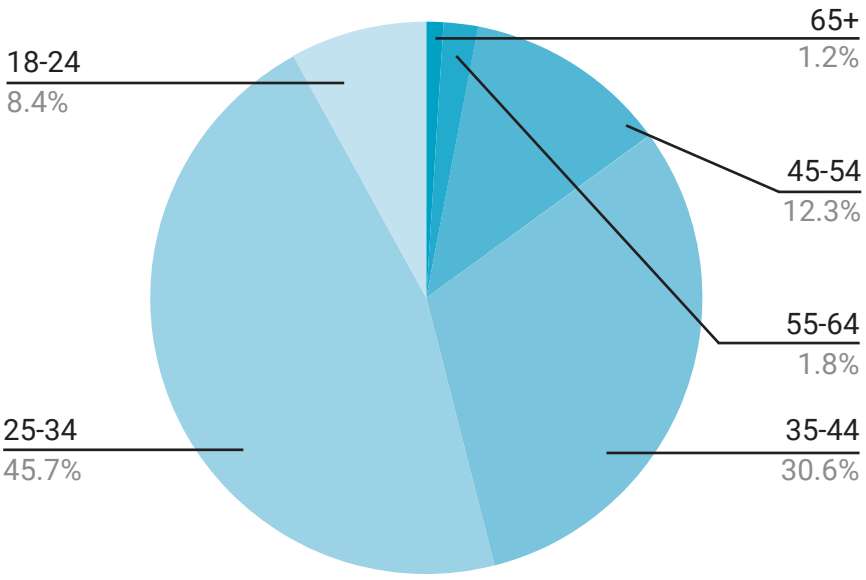
Data gathered from Google analytics that illustrates demographics engaged in cryptocurrencies in regards to gender displays a significant predominance of men in relation to women engaged in cryptocurrencies, with 96.6% for men and 3.4% for women.

Research dedicated to determining cryptocurrency user age groups found the younger generation to be more engaged in cryptocurrencies compared to other age groups.[6,7]

Google analytics data on Bitcoin reveals that the demographic most engaged in the Bitcoin community is the younger generation, namely the millennials (aged 25 - 34), reaching 45.7% of the overall engagement. The second largest group consists of the age group 35 - 54, reaching 30.6%.

According to research results, such data can be supported with the fact that younger people tend to be more tech savvy and generally interested in new ways of investment. Cryptocurrencies are especially attractive for the younger generation since they are more accessible than 'classical investment', have a higher entry barrier from other age groups (which makes it a 'limited investment') and have been created by technological advancement.

Bitcoin community engagement by age



While banks and other financial institutions have been struggling to find ways of connecting with millenials, cryptocurrencies overcame this stigma in a relatively short time period. The data also illustrates that even if older generations are familiar with cryptocurrencies, they will still most likely not invest in them at all.
The last reason for such age group disparity can be attributed to historic financial events, namely that millennials began generating their income after the 2008 financial crisis and many don't trust the tradicional financial services within the current system.

Market need

The biggest issue with recovering lost cryptocurrencies is not the legal aspects or even bureaucracy, but the decentralized and unregulated nature of the assets themselves. Currently for someone to access another's cryptocurrencies, they must be in possession of specific identifying information. In addition, a single wallet can contain an unlimited number of unique identifiers linked to mined Bitcoins, all of which should be known in order to retrieve the entirety of someone's cryptocurrency portfolio.

The issue with transferring cryptocurrency ownership once an account is dormant/inactive, is not entirely unique. In the true spirit of cryptocurrency, there is naturally no centralised authority that could be appealed to fix this. If a Bitcoin or any other cryptocurrency owner passes away without sharing their account information, those coins are simply abandoned, which in turn, decreases the overall amount of the remaining assets.

One of the potential solutions would be to include a person's cryptocurrency wallet information right alongside their bank accounts and other assets in their will. Unfortunately, if this happens, anyone who can access the will would also be able to empty the wallet before a recipient would be able to view it.
Another option is to prepare a handwritten guide on how to access one's assets, online accounts and cryptocurrencies and hide it in a secure location that only specific people know about. But this too has certain vulnerabilities, e.g. someone accessing such a storage while the asset owner is still alive or the only other person privy to the location meeting an unexpected fate themselves.

Digipulse solves the aforementioned issues by providing a platform where users can encrypt their data and store it in a distributed, decentralised manner.
Additionally, asset owners don't need to notify their selected recipient(s) of these assets beforehand, since the "API ping network" takes care of automatic data distribution in case a user's activity drops to zero. And because recipients are not informed about the existence of any assets beforehand, they cannot access them. Digipulse is thus one of the safest solutions currently available.

Service description/ Technology

Digipulse service is a decentralised cloud storage with an automated transfer of ownership based on activity signals received from connected API integrations. It operates as a subscription-based SaaS platform.

As a company, our primary development goal is to ensure that no unencrypted data should ever leave a user's computer and that the digital assets stored online could be transferable in case of the original asset holders inactivity. In addition, we are always on the lookout for vulnerabilities and ways in which malevolent parties might want to take advantage of user data. The encryption part of the service is made possible by the encryption key that the users themselves provide, which is always kept only locally within the user's browser.

Recipient access

A recipient can gain access to the contents of a vault only when the vault creator's activity has dramatically decreased for two sequential check-up periods. The recipient can obtain vault access by following an invitation email from Digipulse to access the contents of the vault. To gain access, the user must answer several security questions with the exact same answers as the vault's creator, who wrote the questions. This will in turn generate the same 'key' used to encrypt the file contents. A user can thus gain access to a vaults contents and download all files present.

“Pulse network”

Pulse network is a collection of the user’s online activity through various API integrations on a daily basis. The more integrations are connected to the account, the more precise the activity tracking. The activity is tracked through connected 3rd party API integrations and outgoing transactions of the user’s cryptocurrency wallet (refer to the website to see which cryptocurrencies are supported). The possible sources for recorded activities fall into two categories - 3rd party API integrations and the Digipulse API.

Activity from 3rd parties is recorded via scheduled tasks run on a predefined time based interval that is tailored for each service provider individually, depending on their API specifications. Digipulse API will record activity as often as a connected service utilises the API endpoints. Aggregated stats from these integrations allow Digipulse to determine the user’s online activity and ‘act’ accordingly in cases when this activity stops. The goal is to have a dataset in place precise enough for the user to feel in control and know that there will be no *false-positive* data releases.

Connecting with services through their APIs

A variety of services people use on a daily basis have the possibility of being integrated into other products. To name a few - Facebook, Twitter, Gmail, Dropbox, Linkedin and others. Integrations even allow using events for tracking user activity in an aggregated manner in one place - Digipulse. This enables the aggregation of all user activity in one place, along with an accurate understanding of a user’s online presence, which is near impossible *not* to have in the 21st century. Each time an activity occurs on one of these services (opened email, a ‘like’ on some article or post, etc.) it counts as activity contributing towards overall activity tracking within the Digipulse service.

Digipulse API for full integration possibilities

In conjunction with 3rd party API integrations, the service offers its own API. This API can be used by services to offer their customers an opportunity to connect their service with Digipulse. Once users connect their account to their Digipulse account, they can use this connected integration to not only receive activity information, but also leave access to this service to the recipient in an 'easy-to-access' way. Services which provide this integration to their customers will receive information about the selected account recipient once Digipulse stops receiving aggregated activity about the user's online activity, so they can speed up the process of passing digital assets on by contacting the next recipient themselves. This would allow services to reduce their customer churn rate and help them provide ease of mind to their customers, namely that their accounts will be delivered to the user's selected recipient(s).

Encryption

'Encryption' is certainly the most commonly used word when describing the Digipulse service. Everything is encrypted, starting from the uploaded files, chunks in which the files are split on a decentralised storage, emails when stored in the database and, of course, the access key for the recipient. AES-256-CBC encryption is being used throughout the project.

Inheritance

Before addressing the technical aspects of the process, it is important to note that the Digipulse service is not an alternative to a traditional inheritance model. The user is still subject to all inheritance laws in their respective jurisdiction. Inheritance is merely one of the use-cases that Digipulse offers and is by no means legally binding between the parties involved.

The encryption process of the access keys is performed in several steps to prevent brute force attacks and increase stored data entropy. The access information encryption flow is performed by collecting 5 answers (5A) to standard questions, then requesting a user to create 2 custom questions (2Q) and provide expected answers to these questions (2A) that only they and the vault recipient would know. The encryption happens in the following order:

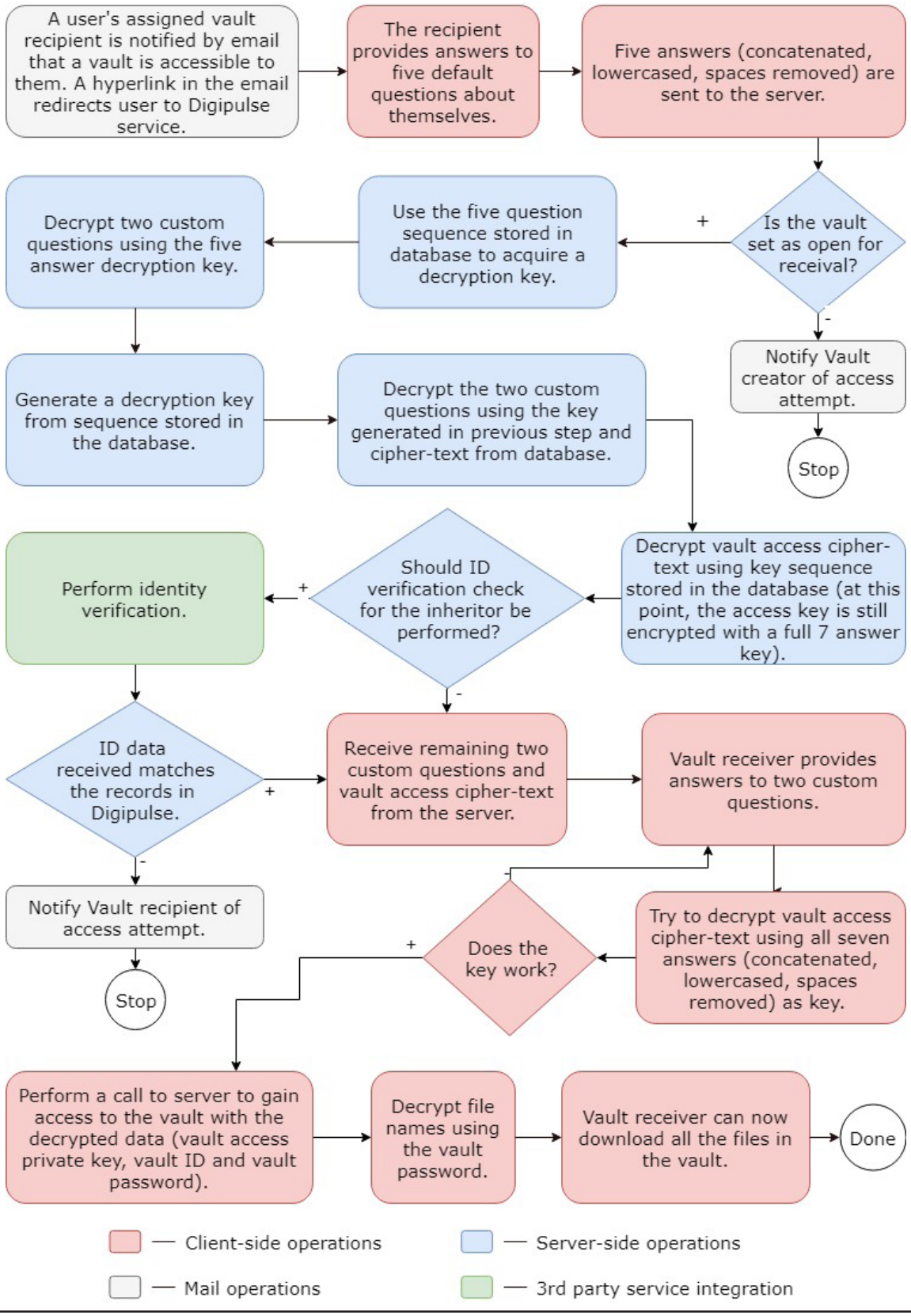
- User provides answers to 5 questions locally;
- User creates 2 custom questions and 2 answers to these questions;
- Using all 7 answers, a 'key' is created to encrypt the recipient's access information (private key, passphrase);
- Send the encrypted access information to a server where it is encrypted with a custom key sequence and stored in the database;
- Use the first 5 answers to encrypt the 2 custom questions and send the encrypted data to the server and store it in the database.

To summarise - Digipulse servers receive 2 encrypted sensitive information packages, both of which are encrypted with the key which is present only at the creation time in the user's browser and is never sent out from the user's computer.

File upload and access

All files which leave the user's computer are encrypted with an encryption key known only to the vault's creator. There is technically no need to share this key with the recipient, since for the simplicity of the transfer procedure, the recipient is required to only know the answers to the security questions. A Trezor integration has been added for additional security, which allows to access a vault and provide the encryption key without the necessity of typing-in the encryption key every time a vault access is being performed.

Vault access as the recipient



File Storage

The encrypted files are stored in a decentralised manner across all storage provider instances in several copies, thus providing the necessary data redundancy in case a particular storage provider goes offline. The storage providers are incentivised by receiving Digipulse tokens as a form of payment. In the primary phase, the service will operate with limited storage space of 1Gb per vault. Once there is enough storage space to allow further service scaling, this number will be increased.

Each vault can have only one specified recipient. Sending information to two different parties will require two separate vault setups.

Data storage: Centralised vs Decentralised

The service is based on the decentralised storage solution provided by Storj. Digipulse used the openly available source code to provide its own version of a file storage that enabled the set-up of its own decentralised version by utilising the storage space provided by individuals who in return gain DGPT tokens. When comparing both options, the seperate network was chosen in favor of flexibility in terms of improved security and custom functionality necessary to provide the Digipulse service.

Although encrypted files are distributed in a decentralised manner, the information necessary for the activity tracking, recipient contacts and billing state is kept centralised due to the limitations of blockchain technology and security considerations. To avoid the possibility of brute forcing the secret questions, requests have to be rate limited, thus they need to be pipelined through a centralised infrastructure.

Digipulse as a service might well be adjusted in the future to operate on a fully decentralised architecture, but only when the technological solutions on the market will allow for this setup, especially regarding the extensive features, which are required by the activity tracking without the high risk factor.
Since Digipulse is a subscription-based service, in the unlikely case of business insolvency, all users would be notified. This is therefore not a risk factor. There are two

scenarios that might occur if Digipulse terminates its services:

- If a user is engaged online and is actively using the service, they will get informed about the termination of the service and choose a new service to secure their digital assets;
- A user's selected recipient has been already contacted and the contents of the vault have been delivered.

Ownership transfer

The ownership transfer process happens as follows: a user's selected recipient is informed through the predefined system channels of communication (email, phone number). In case of a non-response the Digipulse team takes care of manual attempts of reaching out to the person. If all attempts fail, the vault then remains in the system for a period of one year and is deleted afterwards.

Privacy

None of the Digipulse team members or employees have access to user data stored on the servers. The data itself is unreconstructable without the security answers of the recipient or the encryption key known only to the vault creator.

Taking this into consideration, the only necessary user information is an email address, so that we can contact the vault creator in case the activity drops. Optionally, the user can provide their phone number, so that we can also try to contact them via phone. There is no need to perform KYC (Know Your Customer) or provide any other PII (Personally Identifiable Information) to use the Digipulse service.

For additional security, all information stored on Digipulse servers is encrypted and nothing is kept in plain text, so that even if a database breach were to happen, the information retrieved would be meaningless without the appropriate decryption tactics. These rules apply to all PII too - emails, phone numbers and other data. As an additional safety measure, Digipulse is complying with PCI DSS category SAQ-A standards on data handling, which is the type of certification used by financial institutions.

Risk factors

Just like for any other service, the main risk factor and primary system weak point is the integrity and safety of a client's computer. Malwares, viruses, keyloggers and any other malicious software can serve as the weak point and compromise the security of one's credentials. Digipulse is therefore committed to providing the best possible guidelines and user practices towards safeguarding of our user digital identities, with the practice execution falling upon the users themselves.

There are currently two vulnerable security aspects. The first is the decryption key for unlocking a vault's contents. To protect oneself, we strongly recommend using hardware wallets to handle the encryption/decryption process. This second aspect relates to the provided answers and questions for the safekeeping of the encryption key. Since the task of creating elaborate security questions and answers falls onto the users, we recommend rising up to the challenge by composing questions and answers not easily guessed or deducted by using social engineering.

Recipient verification

One of the methods of avoiding the so-called "phishing" attempts of gaining access to one's vault contents, would be to perform identity verification of the recipient before they can answer the remaining 2 questions. The verification process is optional, but highly recommended since this reduces the risk of phishing significantly due to the video based verification which is the most precise and error prone way of online ID verification.

Competitor analysis

While it's obvious that the issue of cryptocurrency inheritance requires a sustainable solution, Digipulse is currently one of the few services operating towards cryptocurrency-sphere sustainability.

The market already contains several differing services (and approaches) tackling the transfer of ownership due to the passing of the original asset holder. Some of them include traditional methods, such as deposit boxes, cryptographic key management firms and even saving one's keys in a personal vault, where everything would be stored on a 'paper wallet' or a hardware file storage device (USB, hardware drive).

In analysing Digipulse product and service competitors, two industries must be taken into account:

1. Digital deposit box and vault providers;
2. Digital inheritance providers.

Several companies already operate within the 'digital safety deposit box' field, providing rather similar services. The main differences between these companies lie in their respective value propositions, offered services and pricing. The same can be said for the 'digital inheritance' market players, although these services involve little to no automation, with a dramatically different price range.

For the competitor analysis, each company was researched both individually and in comparison to other field players (see *Service feature comparison*).

Digital safety deposit box market players:

Futurevault: https://www.futurevault.com/

Versa vault: http://www.versavault.com/

fidsafe : https://www.fidsafe.com/

Dswiss: https://www.dswiss.com/en/

Digital Fortress: https://safedepositboxinsurance.com/digital_fortress/digital-fortress-main/

XAPO: https://xapo.com/vault/

SafeKeet: https://safekeet.io/

Digital inheritance (only) market players:

(ICO) Mywish (inheritance only) - https://mywish.io/index.html

(ICO) Safe Haven (inheritance only) - https://safehaven.io/

Third Key Solutions - https://thirdkey.solutions/

Service feature comparison

Name	File Deposit	Crypto	Inheritance	B2B2C B2B	Decentralised	Activity Tracking	Option for Anonymity	Pricing
Futurevault	x		x	x				individual
Versa vault	x	x			x			N/A (coming soon)
Fidsafe	x			x				free
Dswiss	x			x				individual
Digital Fortress	x		x					USD 1.70 - 12.50
Safekeet	x	x			x			N/A (coming soon)
XAPO		x						free
Safe Haven		x	x					N/A (coming soon)
Mywish		x	x	x	x	x		USD 16 - 640
Third Key soultions		x	x	x				USD 150 - 1500
Digipulse	**x**	**x**	**x**	**x**	**x**	**x**	**x**	USD 6.99 (in DGPT) USD 9.99

Overall, the ‘digital safety deposit box’ industry, can be described as new and unsaturated. Most companies operating within the industry have directed their production efforts towards developing specific features, adapting to their customer needs, with the majority providing file storage space and secure encryption. And while some of the companies offer inheritance solutions for businesses and individuals, only a select few are focusing on delivering solutions for cryptocurrency owners; most market players are operating solely in the field of inheritance.

The aforementioned competitor analysis demonstrates that all market players have their own strengths. What sets Digipulse apart from other services, other than its product multi-use cases, is the key feature of users being able to use the service completely anonymously, which no other solution provides.

Currently, Digipulse might even be considered a first mover within the industry of blockchain based safety deposit boxes. A successfully executed market entry strategy is predicted to ensure that Digipulse conquers a large market portion.

Business structure

Digipulse offers a subscription-based service comprised of two categories:

- "Active vault" - a decentralized asset storage (both digital and crypto), which enables users to remain anonymous and manage their asset transfer to predefined recipients based on an automated trigger release mechanism;
- "Pulse network" - by utilising third party API's, a user's online activity is supplied into the platform triggering the vault release mechanism alongside information about the subscribed services.

The company plans to provide Digipulse's "Pulse network" to every user **free of charge.** Users will only pay a monthly fee for their "active vault" . *("Active vault" pricing is disclosed on the website)* "The service can either be paid for in Digipulse tokens (DGPT) or in fiat currency - the token price will be about 30% lower than that made in fiat. The price difference is made in order to stimulate the underlying token mechanics.

Digipulse will also gradually and continuously expand the "Pulse network" by integrating existing API's of services into the network and on-boarding businesses through the integration of the Digipulse API into their services.

Token mechanics

An integral part of the business is the underlying token mechanism that is put in place to sustain the operations of Digipulse. The incoming user payments will be distributed into three categories:

- Storage providers - will receive a "base" rate of 4 DGPT + 12.5% of all incoming payments (the distribution will afterwards happen on a pro-rata basis, depending of the allocated storage space - the minimum shared space to be eligible for receiving the reward is X GB).

  storage space reward = 4 DGPT + 12.5% * *incoming payments*

- DGPS holders - will receive 37.5% DGPT in Ethereum of all incoming payments (the distribution will afterwards happen on a pro-rata basis, depending of the DGPS tokens owned).

  DGPS claim = 37.5% * *incoming payments*

- The Foundation - will receive 50% of all the incoming payments.

  Foundation = 50% * *incoming payments*

Whether payments will be made in tokens or fiat will largely be irrelevant - upon the distribution calculation, the payments made in fiat will be converted into DGPT and the missing portion of tokens will be covered from the 25% company pool (see: Post-burn token overview). The company will manually evaluate the necessity to refill the company pool by utilising the incoming funds.

The conversion of DGPT to ETH (in the storage provider distribution) will happen automatically by using UpCoin exchange - this will ensure that the tokens are put back on the market for users to obtain.

DGPS holders

Digipulse profit sharing will only be available **after the legal framework will be set up**. These precautions are being made in order to protect both investors and their assets. DGPS token. The token holders who have amassed more than 10’000 DGPT will be eligible to transfer their existing tokens to DGPS (ratio of 10,000 DGPT : 1 DGPS). DGPS will grant profit sharing from the incoming payments for the service use. DGPS holders will collectively be eligible to receive 37.5% from the incoming payments in the form of Ethereum tokens, based on real time DGPT/ETH exchange rate (distributed on a pro-rata basis).

Once holding a DGPS token, the underlying DGPT tokens are frozen and are unusable. During the request for a token swap, a KYC procedure may be conducted in order to identify if the user is eligible to participate in the profit sharing process.

---

* *DGPS - this token **will not** be traded on exchanges. Its sole purpose is to act as means for the smart contract to identify those who are eligible for profit sharing.*

The Digipulse token

Token technical info:

- Name - Digipulse token
- Token ticker - DGPT
- Token type - Utility token*
- Token standard - ERC20
- Decimals - 18
- Smart contract address: https://etherscan.io/address/0xf6cfe53d6febaeea051f400ff5fc14f0cbbdaca1

Exchanges:

The Digipulse token is traded on the following exchanges:

- Upcoin.com: https://upcoin.com/
- Cryptopia: https://www.cryptopia.co.nz/Exchange/?market=DGPT_BTC
- EtherDelta: https://etherdelta.com/#DGPT-ETH

* *For the legal opinion of the Utility token see appendix A.*

The Company

The Digipulse Foundation Trust is the sole owner and executor of the Digipulse project. The Trust has attracted highly skilled and motivated IT professionals that are passionate about developing new blockchain-based applications.

Active project development started in September 2016, with an initial focus on helping individuals discover digital assets accumulated by their family members. This vision further evolved into having a single space for 'all things digital' and utilising the existing network possibilities to make the transfership process automated. This idea then received additional spin when the crypto-based service Coinbase was added to its scope.

December 2016 saw an updated brandbook and a name change, from the more complex *Unobliterate* to the more memorable *Digipulse*.

In 2017 the idea was further presented to investors during a leading Baltic tech event TechChill, where the initial investor feedback gave Digipulse founders confidence that they were on the right track, developing a solution to a problem that has not been tackled yet.

The initial project development was done during the founder spare time, while trying to secure funding from the European Fund "Horizon 2020".

When Bitcoin saw a huge price spike in May of 2017, the founders came to realise that the majority of the technologically savvy population is catching up with cryptocurrencies, thus switching the primary focus to targeting crypto users and leaving the project's memorabilia aspect as the secondary focus.

We truly do believe that blockchain and cryptocurrencies are the future behind decentralised services. Digipulse is created by crypto users, for crypto users. Our ultimate mission is to ensure that each individual feels safe about their digital and crypto assets.

Sources

1. Areiel E. “A Case Study for Blockchain in Healthcare”, MIT Media Lab, 2016
2. http://www.symbolsurfing.com/largest-companies-by-market-capitalization, February 21st, 2018
3. Roberts, J.J., Rapp, N. (2017, November 25) Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. Retrieved from http://fortune.com/2017/11/25/lost-bitcoins/
4. Top 100 Richest Bitcoin Addresses. Bitcoin Rich List. Retrieved on February 21, 2018 from https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html
5. Little, S. (2017, December 14). Bitcoin latest: Third of millennials will be invested in the cryptocurrency in 2018. The Independent. Retrieved from https://www.independent.co.uk/news/business/news/bitcoin-latest-news-millennials-cryptocurrency-investment-2018-london-block-exchange-a8108106.html
6. Gitlen, J. (2017, October 31). Ethereum, Ripple, and Initial Coin Offering (ICO) Survey Data & Report. LendEDU. Retrieved from https://lendedu.com/blog/ethereum-ripple-ico-survey-data-report/

Appendix A

Thomas Easton, Esq.
California State Bar No. 109218
967 Sunset Dr, Springfield OR 97477
541-746-1335 easton3535@gmail.com

January 6, 2018

DIGIPULSE FOUNDATION TRUST
P. O. Box CB.11816
Nassau, The Bahamas

RE: Attorney Letter with Respect to DigiPulse Token DGPT

INTRODUCTION

This opinion is for the purpose of determining the status of DGPT under the laws of the United States. The undersigned grants DGPT Trust full and complete permission and rights to publish the letter for viewing by the public and regulators.

The undersigned is a U.S. resident and was retained by the DigiPulse Foundation Trust for purposes including the rendering of this opinion and reviewing all public disclosure documents. This opinion is based on our knowledge of the law and facts as of the date hereof. The undersigned has examined such corporate records and other documents and such questions of laws as deemed appropriate for the purposes of rendering this opinion.

The undersigned is admitted to practice law by the Bar of the State of California. The undersigned is permitted to practice before the Securities and Exchange Commission ("SEC") and has never been barred from practice in any of the foregoing jurisdictions.

In rendering the legal opinion contained in this letter, we have reviewed certain documents and information furnished by the Issuer but not limited to the DGPT White Paper, Terms & Conditions and such other documents we deemed relevant and necessary as a basis for the opinion hereinafter set forth. In such examinations, we have assumed the genuineness of all signatures set forth on each document, the authenticity of all original documents and the conformity to original documents of all copies as such documents as may have been supplied to us during the course of our examination.

For the purposes of rendering this opinion, we have assumed that no person or entity has engaged in fraud or misrepresentation regarding the inducement relating to, or the execution or delivery of the documents reviewed. Furthermore, we express no opinion as to the validity of any assumptions, form or content of any financial or statistical data contained therein. The terms used in this opinion shall have the meaning ascribed to them in the documents relied upon in rendering our opinion. I have no reason to believe that such information contained an untrue statement of a material fact or omitted to state a material fact in order to make the statements made, in light of the circumstances under which they were made, not misleading. The undersigned has also discussed this matter with the Trustee and Counsel.

Appendix B

CLEMENT .C. CHIGBO (ESQ)

LLB(HONS) (ABU),L.LM(Lond),PhD(ABD), (Aberdeen),B.L, L.E.C., Dip.Lat (Rome),MCL.Arb(UK)

BARRISTER,SOLICITOR AND ADVOCATE

Solicitor of England and Wales, Registered Associate of the Supreme Court of the Bahamas, Attorney at-law (Pro-hac vice) (Turks and Caicos Islands, of the British West Indies), International Legal Consultant in corporate and commercial law, and property Law and conveyancing

Dr. Clement Chigbo
C/O College of Law
Afe Babalola University
KM 8.5 Afe Babalola Way
PMB 5454, Ado-Ekiti
Ekiti State, Nigeria

UK Address:
148 Twickenham Road
Leytonstone
London
E11 4BH

Our Ref:.....

Your Ref:.....

Date:..... **January 8, 2018**

DIGIPULSE FOUNDATION TRUST
P. O. Box CB.11816
Nassau, The Bahamas

RE: Attorney Letter with Respect to DigiPulse Token DGPT

This opinion letter is for the purpose of determining the legal status of DGPT under the laws of the United States and The Commonwealth of The Bahamas. The undersigned grants DigiPulse Foundation Trust full and complete permission and rights to publish the letter for viewing by the public and regulators.

I am a Registered Associate Attorney of the Supreme Court of The Bahamas and was retained by the DigiPulse Foundation Trust for purposes of providing this opinion and reviewing the supporting documents. I am currently on assignment as a law professor. I am also the author of several books and treatises on Bahamas' law including:

A Practical Guide to Land Law, Conveyancing, Wills, Probate & Administration in The Bahamas

Business and Investment Law in The Bahamas

Company Law and Practice in The Bahamas

This opinion is based on law and fact and I have examined such corporate records and other documents and such questions of laws as deemed appropriate for the purposes of rendering this opinion including but not limited to the attached opinion of Thomas Easton Esq. and the DigiPulse Foundation Trust Declaration of Trust.

I concur with the attached opinion of the US SEC practice lawyer Thomas Easton Esq. and incorporated herein that DGPT is not a security, equity, or any other regulated issuance or investment subject to the jurisdiction of the SEC. I can also vouchsafe that the DigiPulse Foundation Trust is properly constituted under the laws of The Bahamas.

Further it is clear to me that DGPT has not and never will be offered or used by US Persons and that the DigiPulse Foundation Trust does not conduct business or have any connection to the United States. Therefore, I can concur with Mr. Easton that DGPT offers no risk of being regulated by the SEC or classed as a security.

Sincerely,

Clement Chigbo
Registered Associate of the Supreme Court of The Bahamas