DIGITAL INHERITANCE USING SECRET SHARING SCHEMES

Research Manual

By

Harry L. Dunne

Institute of Technology, Carlow

Date of Submission

01/11/2019

Abstract

Digital Inheritance refers to the transfer of assets which exist on electronic systems. These assets, making up the owner's *digital estate*, include passwords, usernames, online accounts, contracts, receipts, financial transactions, and medical information. The transfer of the digital estate occurs when there is a prolonged, or permanent absence of the original data owner. This research paper looks at the feasibility of using Secrete Sharing Schemes to store sensitive private information. As well as how other technologies, such as Blockchain, could potentially compliment this cryptography and provide a secure solution to digital inheritance.

Contents

DIGITAL INHERITANCE USING SECRET SHARING SCHEMES

Inheritance, the process of gifting valuables to friends and family after death, is a tradition that can be seen throughout human history. While the concept of inheritance hasn’t changed, the assets deemed valuable enough to be passed on, have evolved. The bequeathing of non-traditional assets, such as those only existing electronically, have been situated under a relatively new term – Digital Inheritance.

Digital inheritance is the process of handing over (personal) digital media in the form of digital assets and rights to (human) beneficiaries. Unlike other forms of inheritance, digital inheritance always involves the exchange of electronic data. The information exchanged can involve passwords, usernames, software, contracts, receipts, financial transactions, public keys, private keys, seed words - etc. *[1 - 3]*

The introduction of online currency, such as Bitcoin, has put a dollar value on data that anyone with a computer and internet access can create. Private keys and seed words for example, may simply be a string of text, but they represent the digital equivalent of a key and deed, allowing access to coins that have value. Failure to properly save and transfer this data, can lead to massive monetary losses.

A study conducted by Chainanalysis *[4]*, an organisation specialising in blockchain analysis, suggested that the number of Bitcoin lost is somewhere between 2.3 and 3.7 million. At the current market price of - $9424 *[5]*, this would mean between £21.6 to $34.8 billion worth of Bitcoin has been lost. Some recent individual cases involving the loss of digital data include-

- $135 million dollars lost by Canadian asset exchange after the CEO, who was the only owner of Bitcoin wallet’s private key, dies unexpectedly. *[6]*

- Billionaire dies leaving $500 million worth of the cryptocurrency Ripple lost. *[7 - 8]*

- Early Bitcoin miner dies at 26 in plane crash, leaving behind millions of dollars his family will never be able to access. [9]

Other types of data such as documents, photos, and message can also be worth saving. These are typically stored within devices or cloud services, without authentication access into devices or cloud services, it can be hard for individuals to retrieve these files. For this reason, information such as device, cloud services, accounts, authentication details, and instructions for how to access these, may also be worth passing on. The ability to store various important private information now and release it to only those who need it at a time that cannot yet be known, is an extremely helpful tool for individuals and organisations.

Google trends indicate that searches for "Digital Inheritance" is growing, with a large spike in interest during 2018. Comparing that data to the search frequency data of "Bitcoin", "Cryptocurrency", "GDPR" and "Have I Been Pwned?" a distinct correlation can be made between the interest in all these topics. *(Fig. 1)*

Whether it is coming from the rise of cryptocurrency or the backlash against companies misusing customer's personal data that helped introduce the GPDR legislation. There is a shift in public culture around the importance of an individual's digital data. As the value that is placed on cyber information increases, the desire to pass it on just like other personal belongings is sure to become more frequent.

Areas to be covered

This project aims to find the legitimacy of building a secure, middleman-free, decentralised, and practical schema, for digital inheritance. Using a combination of technologies such as blockchain and secret sharing cryptography. This paper will only cover the technical setup of a functioning digital inheritance system, it will not provide information regarding legal responsibilities benefactors have to follow in their country.

Research

Current Solutions to Digital Inheritance

Criteria

Both products advertising themselves as a service specifically for digital inheritance and DIY alternative methods of digital inheritance, will be investigated. Services will be found directly through internet search. Found solutions will be compared to the following list of criteria:

Criteria	Description
Free	If the service is free
Fast	If the service takes < 1 hour to setup
Decentralised	If the service is decentralised in nature
No single point of compromise	If there isn't a single point that can compromise scheme
Open source	If the project is open source
Simple Setup	If the project can be considered easy to setup
Opt-in/opt-out	If the inheritance scheme can be ended at any time
Stores multiple types of data	If multiple types of data can be stored and transferred
Minimal beneficiary input	If the process doesn't involve > 1 beneficiary input
Doesn't need personal information	If the service doesn't require personal information

Marked: ✓ - True X - False ☐ - Unknow

Services

PassOn *[16]*

PassOn is a to be a token backed smart contract platform, yet to be released. It aims to use its tokens to create custom smart contracts designed to meet an existing condition before executing and distributing assets.

Criteria table: (fig. 2)

TrustVerse *[17]*

TrustVerse is an AI driven data analytics platform, allowing users to create identities and wallets on its platform. TrustVerse has released a unique Proof of Death (PoD) consensus model, allowing for exchange of cryptocurrency assets, in case of death.

Result table: (fig. 3)

Crypto360.it *[18]*

Crypto360 is an Italian based company offering the secure storage of cryptocurrency related information. This information will be sent to heirs when a specific condition is met.

Result table: (fig. 4)

Safehaven.io *[19]*

Safehaven.io says it offers blockchain solutions to clients, with an emphasis on businesses. Safehaven's Trust Alliance Network is looking to perform both the technical and legal aspects of digital inheritance with business partners. Trust Alliance Network is not currently offering a service.

Result table: (fig. 5)

Digiplus *[20]*

Digiplus was an Erc20 token, looking to offer inheritance based smart contracts. The project has been abandoned and the website's domain is for sale.

Result table: (fig. 6)

Alternative solutions

Hardware wallet (Hot storage / Cold Storage)

A hardware wallet is a portable device that stores cryptocurrency. This is the most recommended way of storing large sums of cryptocurrency. Inheritance is not a key feature of these devices; however, they can easily be transferred to heirs if desired. Although, in some cases authentication into the devices may be hard if no authentication details have been passed along with the device itself. This scheme setup still requires a way to give beneficiaries authentication details, without leaving details open to being compromised.

Result table: (fig. 7)

Legal document

Legal documents, such as wills, can be used to hold specific data intended for recipients. This document will usually be given to a legal professional and held until the time it needs to be used.

Result table: (fig. 8)

Cold storage

Storing details of a wallet offline in a paper document or USB, is far cheaper than a hardware wallet. This method is extremely safe from digital attacks, but very weak to physical attacks. Benefactors need to be informed that this is where information is being stored and any details to find where these physical items are held.

Result table: (fig. 9)

Computer storage

A computer can be used to store information that the owner wants shared eventually. A way for beneficiaries to access the device needs to be supplied.

Result table: (fig. 10)

Dead man's switch

A dead man's switch is a tool which waits for, or lack of, an event/action, before executing. Usually dead man's switches are set to release information, either by email or website, after there is no response from the initial creator of the switch.

Result table: (fig. 11)

Cryptocurrency Exchange

Cryptocurrency exchanges are a common way to hold cryptocurrency. Because the exchange holds coins, in a way which mimics how banks hold fiat currency, many individuals see them as equivalent and as such, possibly able to do inheritance. The extent of which an exchange will go to recover coins for individuals who are not the account owner, is unknown.

Result table: (fig. 12)

Findings

The research found that there are multiple types of solutions that intend to address this problem. Services for the market are new and mainly aimed at cryptocurrency. This illustrates a divide between digital inheritance aimed solely at cryptocurrency and one encompassing multiple types of electronic data. Many of these new services look to utilise unique tokens that power a blockchain with custom smart contracts capable of asset transactions without the original owner available. As of October 2019, there are no cryptocurrencies designed for inheritance within the top 200 coins based on market cap *[5,21,22]*. The current consensus appears to be favored towards method covered in the "alternative" section of options. Simon Goldring, a lawyer, specialising in inheritance. Wrote a piece in the National Law review *[23]*, where he stated his recommended practice for cyber assets-

"The best advice lies in the old adage, prevention is better than cure. It may be that a specific gift of the digital asset is contained within the Will itself or a Letter of Wishes is prepared, to sit alongside the Will, detailing instructions on how to access the funds or the private key itself." [23]

He recommends writing the details of assets and heirs in a will, while avoiding putting any of the private information within the will. Suggesting that the assets should be left on an exchange which have API's capable of tracking activity and releasing funds if there is no account activity for a prolonged time.

"Certain platforms have made use of Application Programming Interface (API) integrations, which measure activity signals. Users are able to predefine a period of inactivity, e.g., three years, which on elapsing will trigger the transfer of digital assets to select beneficiaries." [23]

While some may find this service valuable, keeping assets on exchanges introduce unique problems. Ledger, a hardware wallet company, compiled a list of exchange hacks, finding a total of $1.7 billion was stolen from exchanges in 2018 alone *[24]*. Individuals who wish to avoid the theft of assets through cyber-attacks, are encouraged to use cold storage of assets and not online wallets or exchanges.

In 2013, Hal Finney, the first person to receive a bitcoin transaction, wrote a forum post describing how he stored his Bitcoin information-

"Those discussions about inheriting your bitcoins are of more than academic interest. My bitcoins are stored in our safe deposit box, and my son and daughter are tech savvy. I think they're safe enough. I'm comfortable with my legacy." [25]

While the preferred alternative method depends largely on the individual, each of these methods appear to be much more popular than separate paid services. Nearly all alternative methods also utilise some physically stored attribute in the schema, whether that be a safe that holds paper documents or will in the hands of a lawyer.

Conclusion

As of October 2019, no one solution fits all the specified criteria and nearly all solutions are designed specifically for cryptocurrency. In the choice between products designed for inheritance and alternative methods, there is a general preference towards alternatives. Alternative schemes tend to use a combination of both physical and electronic storage.

Secret Sharing

Criteria

The goal of this research is to find the validity of using Shamir’s Secret Sharing encryption to create a schema for digital inheritance. To pass, this encryption type will have to be found to be:

1. Secure enough to store high value private information
2. Compatible with commercial desktops.

Findings

Secret Sharing is information-theoretically secure, meaning that even an attacker with infinite computing resources cannot break the encryption [27 - 29]. This makes this cryptography ideal for storing sensitive and highly important, including missile launch codes. Information-theoretically secure cryptography is considered “perfectly secure” and is not vulnerable to attacks from quantum computers. It is possible to attempt to brute force guess the keys themselves. However, this can only be done when the encryption is being used on small amounts of data and the attacker knows how many keys are used. *(fig.13)*

The more data that is being encrypted and a larger amount of key will make guessing a key exceptionally difficult. For example, encrypting only 32 characters of data into 2 keys with Shamir’s secret sharing, creates two 51 character keys. Attempting to guess a key, would be the equivalent of brute forcing a 51 letter password.

Secret sharing is considered secure as long as-

X = Total number of keys
Attacker owns (X – 1 keys)

Conclusion

Secret sharing encryption are exceptional for protecting high value and sensitive information. Considered a perfectly secure cryptography, the encryption is secure against attackers with infinite resources. The ability to split keys and share these keys with others, may be very valuable in an inheritance scheme.

Research Conclusion

Research has indicated there isn't yet a sufficient solution to digital inheritance. A consensus amongst the general community shows more of an interest in alternative schemes. However, new projects designed to solve the issue, are trending towards complex token based smart contracts and receiving little success. It is possible that the ability these smart contracts have to take coins out of a wallet and send them to inheritors, make people feel uneasy. A study showed that out of the Bitcoin users asked, 60% of them felt scared to simply make one normal transaction *[26]*. An inflexible "ticking" smart contract that forcefully removes coins from an individual's wallet, may appear more as a threat and burden than a reassurance. Compared to a more passive solution assuring the benefactor, that data they chose to pass on, can be pieced back together by inheritors only after a certain condition is met.

The information found during research of the market, shows that there is a need for a solution which can meet all the previous criteria. While maintaining the characteristics of an alternative method that doesn't take any control out of the user's hands.

Secret Sharing has been found to be an exceptional choice for data of this sensitivity, as it is information-theoretically secure. Shamir's Secret Sharing is the most popular form of secret sharing and will be the choice for this project. The updated criteria the design of the schema should match has been updated. New criteria:

Criteria	**Description**
Free	If the service is free
Fast	If the service takes < 1 hour to setup
Decentralised	If the service is decentralised in nature
No single point of compromise	If there isn't a single point that can compromise scheme
Open source	If the project is open source
Simple Setup	If the project can be considered easy to setup
Opt-in/opt-out	If the inheritance scheme can be ended at any time
Stores multiple types of data	If multiple types of data can be stored and transferred
Minimal beneficiary input	If the process doesn't involve > 1 beneficiary input
Doesn't need personal information	If the service doesn't require personal information
Gives Users full control of their data	Users still have full control of asset while using scheme
Resistant to cyber and physical attack	Can withstand cyber-attacks or in person robbery attacks
No preemptive release of information	Extremely difficult for heir to get data before release
Private	Hard for outsiders to know the scheme is being used
Not burdensome	Doesn't interfere with the lives of benefactor or heirs

Project Specifications

Web Hosting

Criteria

The websites role will be to perform online encryption/decryption of Secret Sharing keys, host instructions for using the application, and possibly interact directly with a blockchain.

1. Provides good performance
2. Cheap annual cost

Choice

Netlify [32]

Netlify is a web hosting provider that offers free hosting with cutting edge features. It is trusted by more than 500,000 developers and businesses across the world.

Application type

Criteria

The application type needs to be available for people around the world to use and it needs to be opensource.

1. Available to everyone
2. Opensource

Choice

JAMstack [32]

The JAMstack refers to websites using a – Javascript, API, and Markup technology stack. This technology stack allows for the creation of fully functional websites without depending on a web server, or backend code. Instead it uses Content Delivery Networks, to distribute the site to visitors and decentralised API driven databases, such as FaunaDB to store user data.

Database

Criteria

The database needs to interact directly with JAMstack Netlify sites.

1. Easy to integrate
2. JAMstack driven

Choice

FuanaDB [33]

FaunaDB is a global serverless database that gives ubiquitous, low latency access to app data, without sacrificing data correctness and scale. It uses GraphQL as its querying language.

Code repository

Criteria

A web accessible code repository is needed to have version control and a ledger of changes and edits

1. Free
2. Easily integrated with the rest of the system

Choice

Netlify Build

As the hosting that will be used is with Netlify, the easiest code repository for the web application will be with Netlify itself.

Programing Language

Criteria

The languages used in the project will be based on which ones suit the project design. Frontend design languages like HTML and CSS are necessary to the web development section and for this reason compulsory. As the project will be following the JAMstack, a backend language cannot be used. For this reason, a language that can perform complex encryption tasks and can be used on the JAMstack is needed.

1. Language that can be used to perform encryption and decryption and complies with JAMstack standard.

Choice

JavaScript

JavaScript is a client-side web language, meaning that it is placed within websites, but run on the users end instead of the server. Because of this, JavaScript is always visible to the user in comparison to a server-side language such as PHP. JavaScript complies with the JAMstack and as it is visible to users, can be publicly audited.

Tables

Search Trends

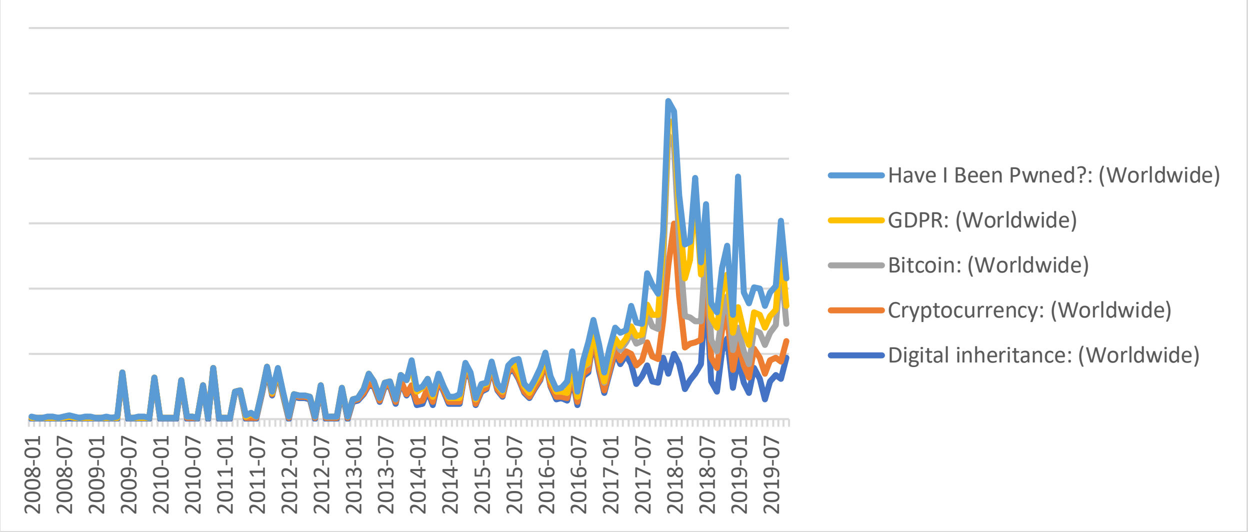
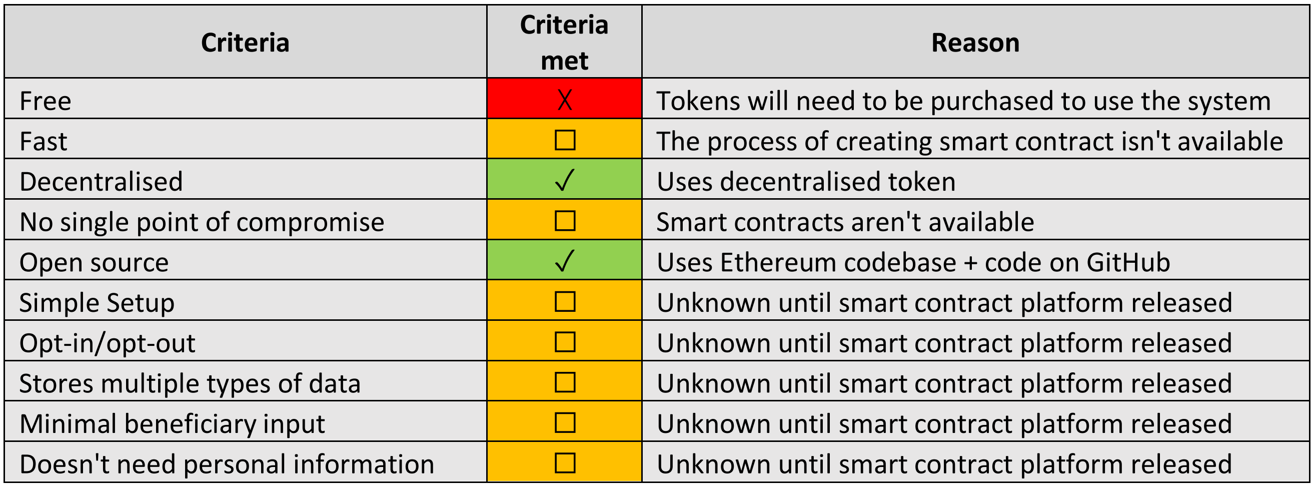


Figure 1. References [10 – 15]

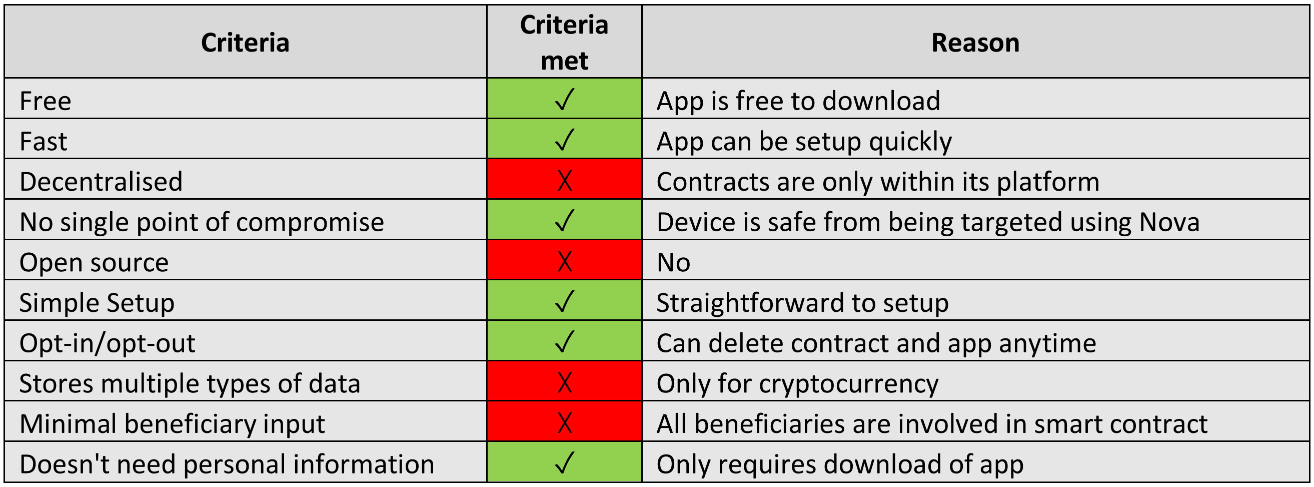
Criteria: PassOn



Criteria	Criteria met	Reason
Free	X	Tokens will need to be purchased to use the system
Fast	□	The process of creating smart contract isn't available
Decentralised	✓	Uses decentralised token
No single point of compromise	□	Smart contracts aren't available
Open source	✓	Uses Ethereum codebase + code on GitHub
Simple Setup	□	Unknown until smart contract platform released
Opt-in/opt-out	□	Unknown until smart contract platform released
Stores multiple types of data	□	Unknown until smart contract platform released
Minimal beneficiary input	□	Unknown until smart contract platform released
Doesn't need personal information	□	Unknown until smart contract platform released

Figure 2.

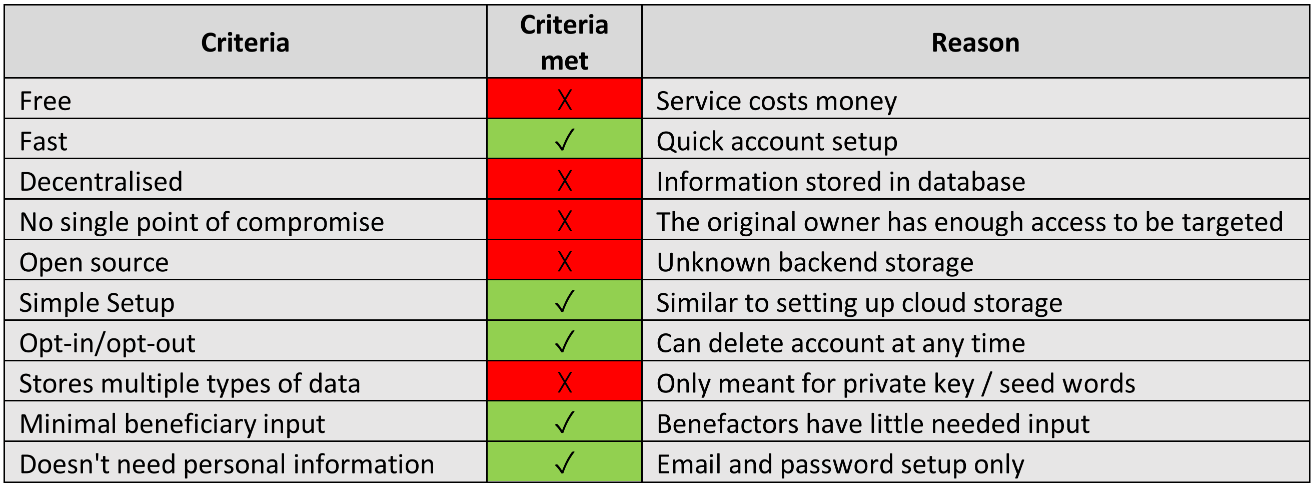
Criteria: TrustVerse



Criteria	Criteria met	Reason
Free	✓	App is free to download
Fast	✓	App can be setup quickly
Decentralised	X	Contracts are only within its platform
No single point of compromise	✓	Device is safe from being targeted using Nova
Open source	X	No
Simple Setup	✓	Straightforward to setup
Opt-in/opt-out	✓	Can delete contract and app anytime
Stores multiple types of data	X	Only for cryptocurrency
Minimal beneficiary input	X	All beneficiaries are involved in smart contract
Doesn't need personal information	✓	Only requires download of app

Figure 3.

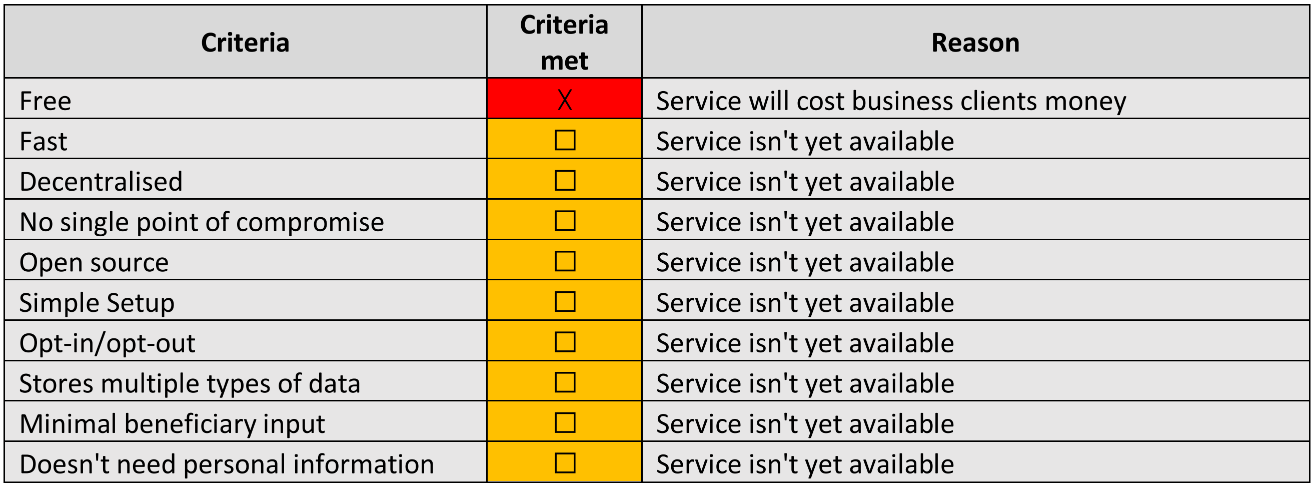
Criteria: Crypto360.it



Criteria	Criteria met	Reason
Free	X	Service costs money
Fast	✓	Quick account setup
Decentralised	X	Information stored in database
No single point of compromise	X	The original owner has enough access to be targeted
Open source	X	Unknown backend storage
Simple Setup	✓	Similar to setting up cloud storage
Opt-in/opt-out	✓	Can delete account at any time
Stores multiple types of data	X	Only meant for private key / seed words
Minimal beneficiary input	✓	Benefactors have little needed input
Doesn't need personal information	✓	Email and password setup only

Figure 4.

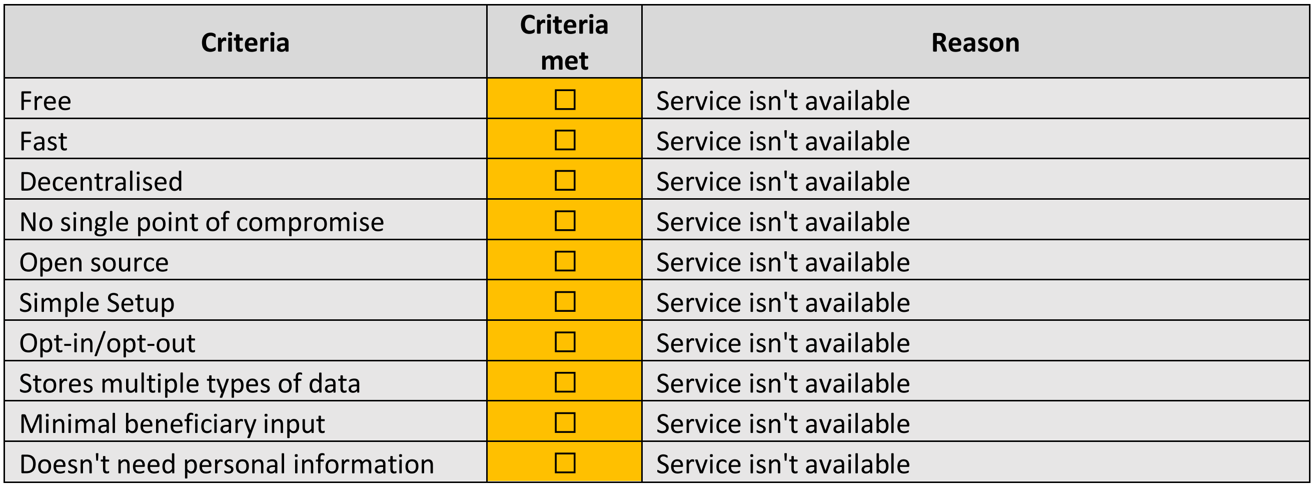
Criteria: Safehaven.io



Criteria	Criteria met	Reason
Free	X	Service will cost business clients money
Fast	□	Service isn't yet available
Decentralised	□	Service isn't yet available
No single point of compromise	□	Service isn't yet available
Open source	□	Service isn't yet available
Simple Setup	□	Service isn't yet available
Opt-in/opt-out	□	Service isn't yet available
Stores multiple types of data	□	Service isn't yet available
Minimal beneficiary input	□	Service isn't yet available
Doesn't need personal information	□	Service isn't yet available

Figure 5.

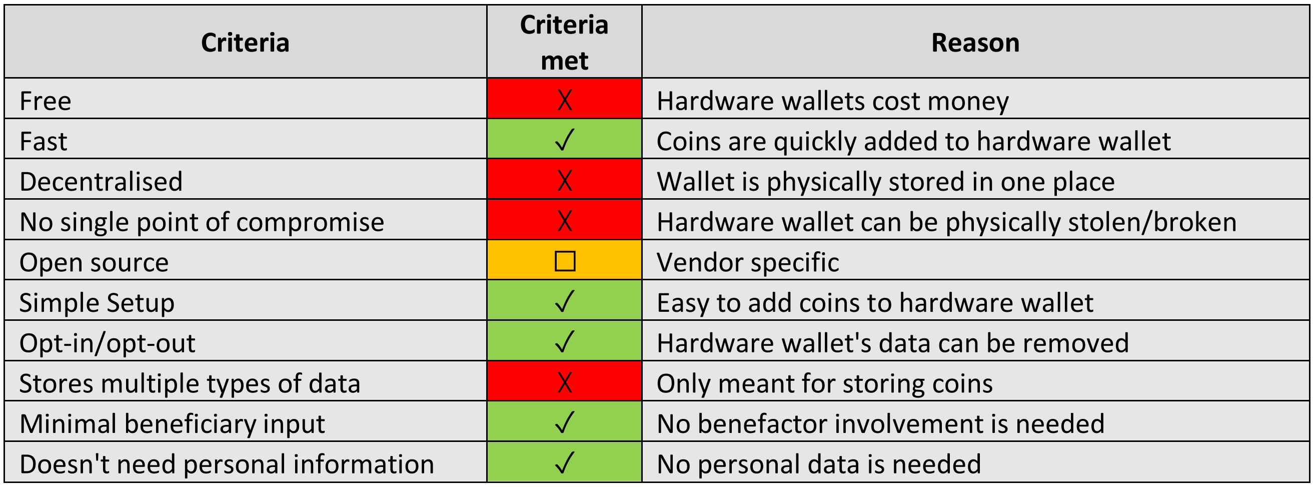
Criteria: Digiplus



Criteria	Criteria met	Reason
Free	□	Service isn't available
Fast	□	Service isn't available
Decentralised	□	Service isn't available
No single point of compromise	□	Service isn't available
Open source	□	Service isn't available
Simple Setup	□	Service isn't available
Opt-in/opt-out	□	Service isn't available
Stores multiple types of data	□	Service isn't available
Minimal beneficiary input	□	Service isn't available
Doesn't need personal information	□	Service isn't available

Figure 6.

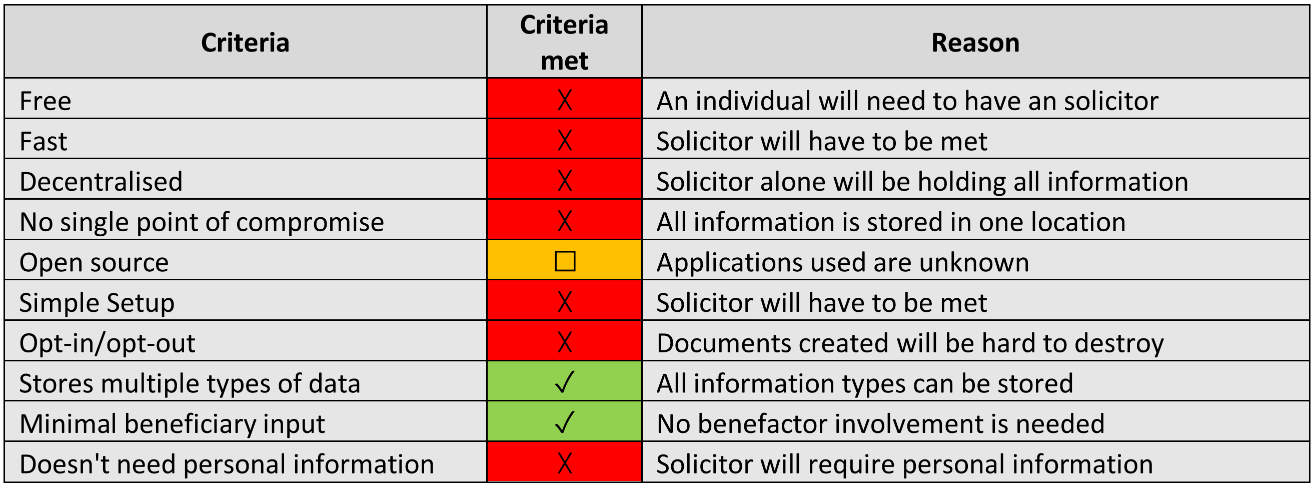
Criteria: Hardware wallet



Criteria	Criteria met	Reason
Free	X	Hardware wallets cost money
Fast	✓	Coins are quickly added to hardware wallet
Decentralised	X	Wallet is physically stored in one place
No single point of compromise	X	Hardware wallet can be physically stolen/broken
Open source	□	Vendor specific
Simple Setup	✓	Easy to add coins to hardware wallet
Opt-in/opt-out	✓	Hardware wallet's data can be removed
Stores multiple types of data	X	Only meant for storing coins
Minimal beneficiary input	✓	No benefactor involvement is needed
Doesn't need personal information	✓	No personal data is needed

Figure 7.

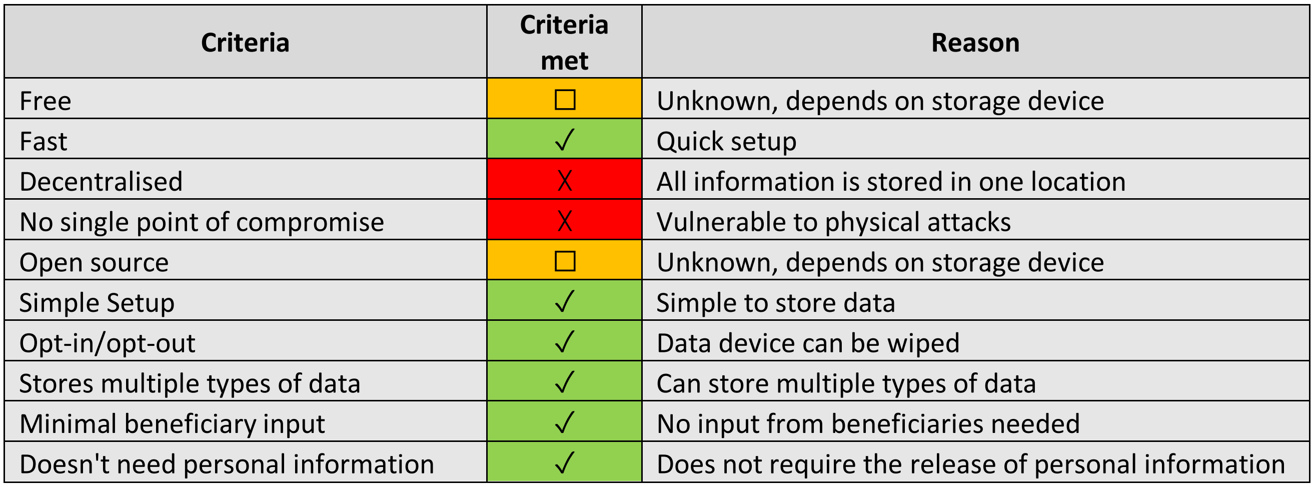
Criteria: Legal document



Criteria	Criteria met	Reason
Free	X	An individual will need to have an solicitor
Fast	X	Solicitor will have to be met
Decentralised	X	Solicitor alone will be holding all information
No single point of compromise	X	All information is stored in one location
Open source	□	Applications used are unknown
Simple Setup	X	Solicitor will have to be met
Opt-in/opt-out	X	Documents created will be hard to destroy
Stores multiple types of data	✓	All information types can be stored
Minimal beneficiary input	✓	No benefactor involvement is needed
Doesn't need personal information	X	Solicitor will require personal information

Figure 8.

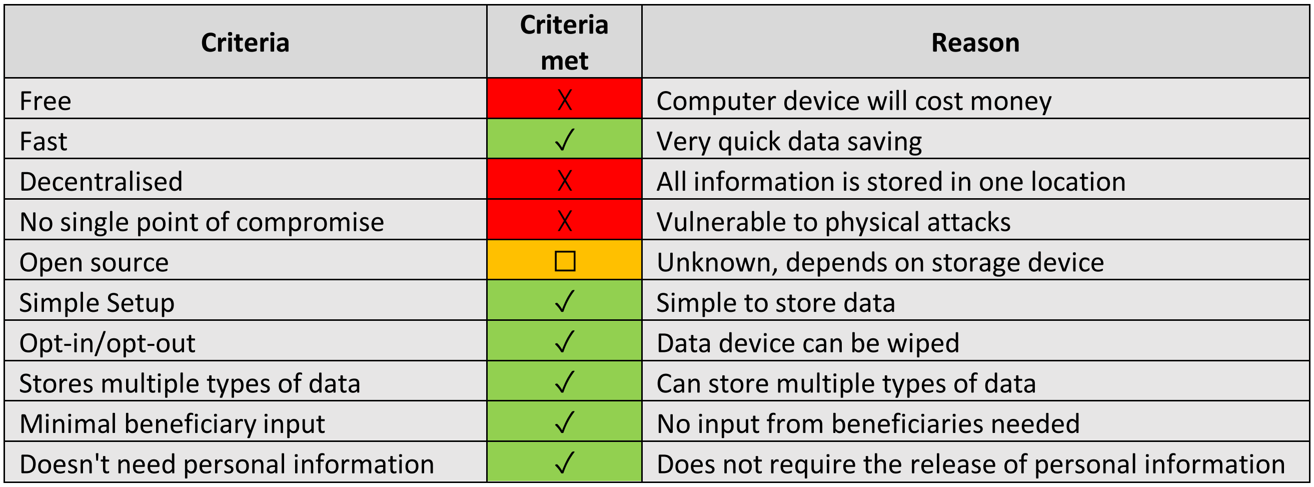
Criteria: Cold storage



Criteria	Criteria met	Reason
Free	□	Unknown, depends on storage device
Fast	✓	Quick setup
Decentralised	X	All information is stored in one location
No single point of compromise	X	Vulnerable to physical attacks
Open source	□	Unknown, depends on storage device
Simple Setup	✓	Simple to store data
Opt-in/opt-out	✓	Data device can be wiped
Stores multiple types of data	✓	Can store multiple types of data
Minimal beneficiary input	✓	No input from beneficiaries needed
Doesn't need personal information	✓	Does not require the release of personal information

Figure 9.

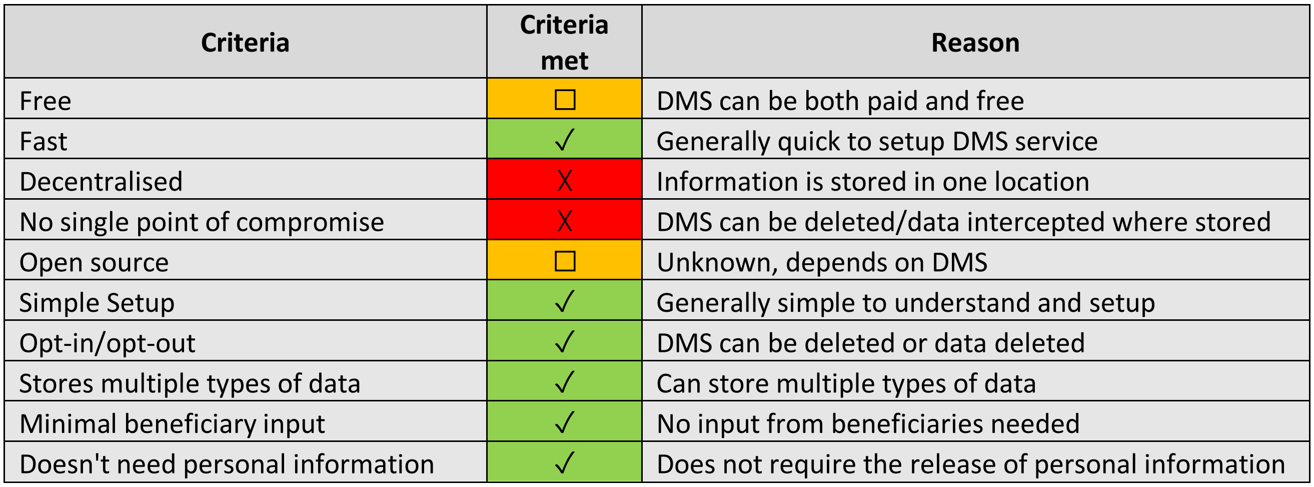
Criteria: Computer storage



Criteria	Criteria met	Reason
Free	X	Computer device will cost money
Fast	✓	Very quick data saving
Decentralised	X	All information is stored in one location
No single point of compromise	X	Vulnerable to physical attacks
Open source	□	Unknown, depends on storage device
Simple Setup	✓	Simple to store data
Opt-in/opt-out	✓	Data device can be wiped
Stores multiple types of data	✓	Can store multiple types of data
Minimal beneficiary input	✓	No input from beneficiaries needed
Doesn't need personal information	✓	Does not require the release of personal information

Figure 10.

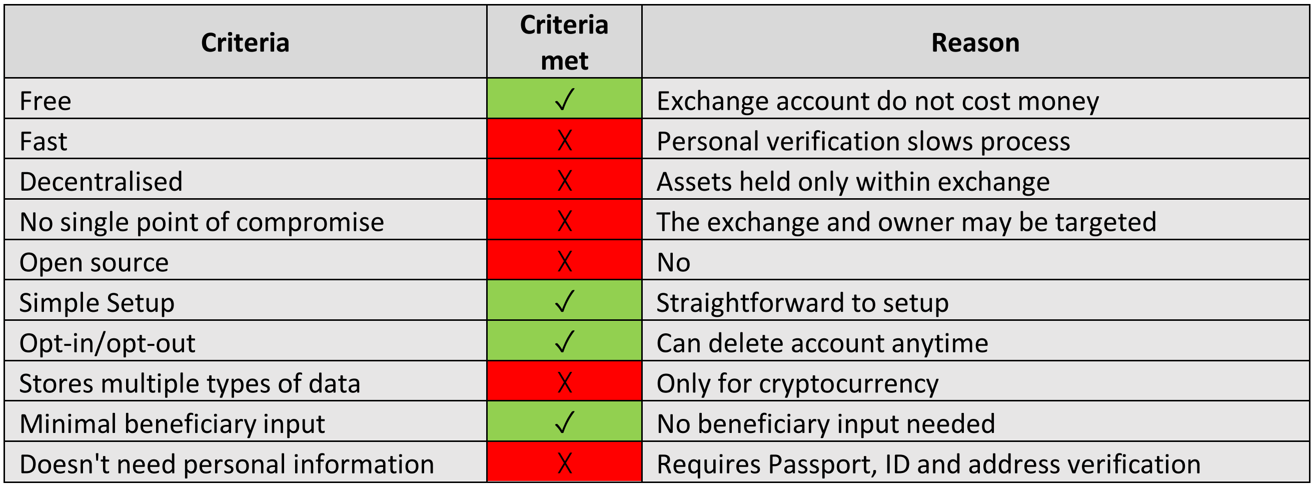
Criteria: Dead man's switch



Criteria	Criteria met	Reason
Free	□	DMS can be both paid and free
Fast	✓	Generally quick to setup DMS service
Decentralised	X	Information is stored in one location
No single point of compromise	X	DMS can be deleted/data intercepted where stored
Open source	□	Unknown, depends on DMS
Simple Setup	✓	Generally simple to understand and setup
Opt-in/opt-out	✓	DMS can be deleted or data deleted
Stores multiple types of data	✓	Can store multiple types of data
Minimal beneficiary input	✓	No input from beneficiaries needed
Doesn't need personal information	✓	Does not require the release of personal information

Figure 11.

Criteria: Cryptocurrency exchange



Criteria	Criteria met	Reason
Free	✓	Exchange account do not cost money
Fast	X	Personal verification slows process
Decentralised	X	Assets held only within exchange
No single point of compromise	X	The exchange and owner may be targeted
Open source	X	No
Simple Setup	✓	Straightforward to setup
Opt-in/opt-out	✓	Can delete account anytime
Stores multiple types of data	X	Only for cryptocurrency
Minimal beneficiary input	✓	No beneficiary input needed
Doesn't need personal information	X	Requires Passport, ID and address verification

Figure 12.

Secret Sharing

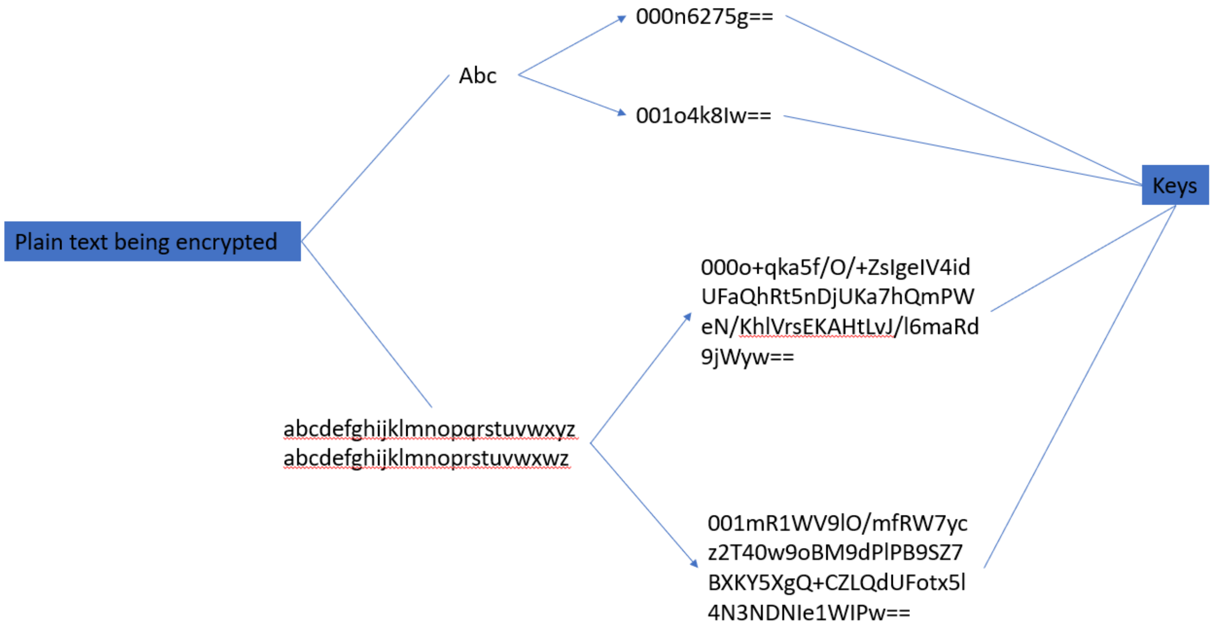


Figure 13. *In the case of an attacker controlling one key, it would be much simpler to crack the second key of 11 characters then in the second example where the keys are 51 characters long.*

References

[1] Andrew.R. 2019. What Is Digital Inheritance And The Future Of Your Assets After Death? [ONLINE] Available at: https://www.forbes.com/sites/andrewrossow/2018/04/03/what-is-digital-inheritance-and-the-future-of-your-assets-after-death/. [Accessed 29 October 2019].

[2] The Telegraph. 2019. Rise of 'digital inheritance' as YouGov poll shows quarter of people plan to hand social media to loved ones. [ONLINE] Available at: https://www.telegraph.co.uk/news/2018/11/06/rise-digital-inheritance-yougov-poll-shows-quarter-people-plan/. [Accessed 29 October 2019].

[3] Wikipedia. 2019. Digital inheritance - Wikipedia. [ONLINE] Available at: https://en.wikipedia.org/wiki/Digital_inheritance. [Accessed 29 October 2019].

[4] Chainalysis Blog | Bitcoin's $30 billion sell-off. 2019. Chainalysis Blog | Bitcoin's $30 billion sell-off. [ONLINE] Available at: https://blog.chainalysis.com/reports/money-supply. [Accessed 29 October 2019].

[5] CoinMarketCap. 2019. Cryptocurrency Market Capitalizations | CoinMarketCap. [ONLINE] Available at: https://coinmarketcap.com/. [Accessed 29 October 2019].

[6] BBC News. 2019. Quadriga: The cryptocurrency exchange that lost $135m - BBC News. [ONLINE] Available at: https://www.bbc.com/news/world-us-canada-47203706. [Accessed 29 October 2019].

[7] Coin Thud | Bitcoin & Cryptocurrency News. 2019. Mathew Mellon: $500 Million in Ripple Lost as Billionaire Dies Suddenly. [ONLINE] Available at: https://cointhud.com/500-million-ripple-lost-billionaire-mathew-mellon-dies/. [Accessed 29 October 2019].

[8] CryptoPotato. 2019. $500 Million Of Ripple Lost After Owner Dies Suddenly. [ONLINE] Available at: https://cryptopotato.com/500-million-worth-of-ripple-lost-after-owner-dies-suddenly/. [Accessed 29 October 2019].

[9] Bloomberg. Bitcoin Industry Grapples With Age-Old Problem of Inheritance [ONLINE] Available at: https://www.bloomberg.com/news/articles/2018-02-13/bitcoin-industry-grapples-with-age-old-problem-of-inheritance?srnd=cryptocurriences. [Accessed 29 October 2019].

[10] Google Trends. 2019. Have I been Pwned?. [ONLINE] Available at: https://trends.google.com/trends/explore?date=all&q=%2Fg%2F11c3yr69mm. [Accessed 29 October 2019].

[11] Google Trends. 2019. GDPR. [ONLINE] Available at: https://trends.google.com/trends/explore?date=all&q=GDPR. [Accessed 29 October 2019].

[12] Bloomberg. Bitcoin Industry Grapples With Age-Old Problem of Inheritance [ONLINE] Available at: https://www.bloomberg.com/news/articles/2018-02-13/bitcoin-industry-grapples-with-age-old-problem-of-inheritance?srnd=cryptocurriences. [Accessed 29 October 2019].

[13] Google Trends. 2019. Bitcoin. [ONLINE] Available at: https://trends.google.com/trends/explore?date=all&q=%2Fm%2F05p0rrx. [Accessed 29 October 2019].

[14] Google Trends. 2019. Cryptocurrency. [ONLINE] Available at: https://trends.google.com/trends/explore?date=all&q=%2Fm%2F0vpj4_b. [Accessed 29 October 2019]. Bloomberg. Bitcoin Industry Grapples With Age-Old Problem of

Inheritance [ONLINE] Available at: https://www.bloomberg.com/news/articles/2018-02-13/bitcoin-industry-grapples-with-age-old-problem-of-inheritance?srnd=cryptocurriences. [Accessed 29 October 2019].

[15] Google Trends. 2019. Digital Inheritance. [ONLINE] Available at: https://trends.google.com/trends/explore?date=all&q=%2Fg%2F120qknj4. [Accessed 29 October 2019].

[16] Home - PassOn – Inventing Digital Inheritance. 2019. Home - PassOn – Inventing Digital Inheritance. [ONLINE] Available at: https://passon.com/en. [Accessed 31 October 2019].

[17] TrustVerse - The Universe Of Trust. 2019. TrustVerse - The Universe Of Trust. [ONLINE] Available at: https://trustverse.io/#/. [Accessed 31 October 2019].

[18] CRYPTO360. 2019. Compra/vendi Criptovalute - CRYPTO360. [ONLINE] Available at: http://crypto360.it/. [Accessed 31 October 2019].

[19] SAFE HAVEN. 2019. HOME - SAFE HAVEN. [ONLINE] Available at: http://safehaven.io. [Accessed 31 October 2019].

[20] DAN.COM. 2019. The domain name digipulse.io is for sale | DAN.COM. [ONLINE] Available at: https://digipulse.io/. [Accessed 31 October 2019].

[21] Coinranking. 2019. Coinranking: Cryptocurrency prices, charts & lists. [ONLINE] Available at: https://coinranking.com/. [Accessed 31 October 2019].

[22] CoinGecko: 360° Market Overview of Coins & Cryptocurrencies. [ONLINE] Available at: https://www.coingecko.com. [Accessed 31 October 2019].

[23] The National Law Review. 2019. Cryptocurrency: Investment, Inheritance, Wallet Transfers . [ONLINE] Available at:

https://www.natlawreview.com/article/cryptocurrency-current-investment-future-inheritance. [Accessed 31 October 2019].

[24] Ledger. 2019. Hacks Timeline | Ledger. [ONLINE] Available at: https://www.ledger.com/academy/crypto/hacks-timeline/. [Accessed 31 October 2019].

[25] Bitcoin and me (Hal Finney). 2019. Bitcoin and me (Hal Finney). [ONLINE] Available at: https://bitcointalk.org/index.php?topic=155054.0. [Accessed 31 October 2019].

[26] Bitcoin News. 2019. Crypto Users Are Still Scared to Pay With Bitcoin in 2019 — FIO Protocol Aims to Fix That - Bitcoin News. [ONLINE] Available at: https://news.bitcoin.com/crypto-users-are-still-scared-to-pay-with-bitcoin-in-2019-fio-protocol-aims-to-fix-that/. [Accessed 31 October 2019].

[27] Secret Sharing - an overview | ScienceDirect Topics. 2019. Secret Sharing - an overview | ScienceDirect Topics. [ONLINE] Available at: https://www.sciencedirect.com/topics/computer-science/secret-sharing. [Accessed 01 November 2019].

[28] Secret Double Octopus. 2019. What is Secret Sharing? | Security Wiki. [ONLINE] Available at: https://doubleoctopus.com/security-wiki/encryption-and-cryptography/secret-sharing/. [Accessed 01 November 2019].

[29] Secret sharing - Wikipedia. 2019. Secret sharing - Wikipedia. [ONLINE] Available at: https://wikipedia.org/wiki/Secret_sharing. [Accessed 01 November 2019].

[31] Netlify. 2019. Netlify: All-in-one platform for automating modern web projects. . [ONLINE] Available at: https://www.netlify.com/. [Accessed 01 November 2019].

[32] Jamstack.org. (2019). JAMstack | JavaScript, APIs, and Markup. [online] Available at: https://jamstack.org/. [Accessed 01 November 2019].

[33] Fauna. (n.d.). The database built for serverless. [online] Available at: https://fauna.com/. [Accessed 01 November 2019].