Quantum-AI-Guarded Cyber Currency for intangible tokens (Part I)

Pedro J. Navarro Vera

Cybersecurity Lead Consultant info@cybereu.eu

# Abstract

The global economy undergoes a seismic shift, with the use of advanced technologies such as the power of artificial intelligence, quantum computing and distributed ledger. This paper is part (I) of a proof of concept (PoC) on monetary transactions based on a new currency named @mo. The second part of this paper [1] Navarro Vera, P.J. In the Book Quantum-AI-Guarded Cyber Currency for Intangible Tokens (Part II) focuses on data visualisation by means of Python and Power BI tools, related to this proof of concept (PoC) on monetary transactions based on a new currency named @mo. This new currency, likewise, money is fungible, which means that one @mo banknote is interchangeable with any other genuine @mo banknote like it. This new currency holds fungible, non-tangible, digital tokens applied to relevant scenarios under test. Such domains include for instance healthcare, nursing homes, peacekeeping, and humanitarian aid domains. This paper also describes how the combination of these advanced technologies, together with defined processes, enhances the overall security of those transactions. As an example of security controls, the use of applicable processes such as Know Your Client (KYC) best practices, strong cyber security measures based on Security testing methodology such as the Open Web Application Security Project (OWASP) and MITRE ATTACK Frameworks and a registry with a special flag to signal hacked or stolen coins to indicate they are not to be traded or used.

This paper includes an analysis of a sample of the population of @mo transactions by means of Python and Power BI tools. This analysis leads to the main findings, results, and conclusions.

This article’s main finding relates to the contribution of Dijkstra's algorithm to the stabilization of the volatility of this new currency, limiting the risk of this currency being used as a speculative investment. In the second place, it describes the contribution of AI together with quantum computing to the improvement of the security of these currency transactions and limiting the risk of these coins being hacked.

The main conclusion is that both the volatility and security of this new currency for intangible tokens can be proportionally reduced under the application of an adaptive sequence of key security strategies identified in this paper.

**Keywords:** Quantum Encryption; AI; Open Web Application Security Project (OWASP); MITRE ATTACK; Blockchain; Dijkstra's algorithm; Know Your Client (KYC); OpenID Connect and Oauth 2.0 (Open Authorization).

# 1. Introduction

Intangible assets, unlike physical ones, have no tangible form yet hold significant value both now and in the future. Traditional currencies like USD or Euros fall short when it comes to acquiring the most precious and intangible things—what we call “the unbuyable.”

A high-level introduction to this topic can be found in [2] Priceless Exchange: The Rise of AMO (Part I): Quantum-AI-Guarded Cyber-currency for the Unbuyable.

This work presents a proof of concept (PoC) on how such intangible assets can be exchanged, challenging the conventional limitations of traditional money.

Currently, no universal laws govern the valuation of intangible assets, highlighting the need for innovative approaches in this evolving financial landscape. The following publication stated that “there are no corresponding universal laws of nature that relate to intangible assets valuation” [3] Valuing Intangible Assets (McGraw-Hill Library of Investment and Finance) Robert F. Reilly.

Moreover, the concept of goodwill, a typical intangible asset, in business has sparked debate for over a century. A striking example is Facebook’s (now Meta) 2010 purchase of the domain fb.com for USD 8.5 million—an amount recorded as goodwill on its balance sheet, and at this point we cannot include it in the scope of what we call “the unbuyable.” Yet, before the sale, the American Farm Bureau Federation, the original owner, could not recognize its value. This highlights a key financial principle: goodwill must come from an external source.

Historically, goodwill represented the lasting value of a company’s reputation and customer connections. However, modern accounting standards, like IFRS’s IAS 38, strictly define it as an asset only when acquired externally, excluding internally generated goodwill such as brand value or customer loyalty."

Finally, the main aim of the work is proof of concept (PoC) on how such intangible assets can be traded among each other, challenging the conventional limitations of traditional money transactions. The conclusions highlight two key contributions of advanced technology to the stability and security of this new currency. First, AI-driven cybersecurity measures, combined with Dijkstra's algorithm, help stabilize volatility, preventing the currency from becoming a speculative asset. Second, the integration of AI and quantum computing enhances transaction security, reducing the risk of hacking and ensuring a more resilient financial system.

# 2. Materials and Methods

The Materials and Methods section that follows describes the testing steps, including relevant screenshots with sufficient details to allow others to replicate and build on the published results.

There are no restrictions on the availability of materials or information. Please note that the publication of this manuscript includes references to all materials, data, computer code, and protocols associated with this publication available to readers in a reserved DOI. The DOI is registered when the upload is published: **10.5281/zenodo.15017650** and

<https://zenodo.org/records/15017650?preview=1&token=eyJhbGciOiJIUzUxMiJ9.eyJpZCI6IjRkNjJiMmI1LTJhZWMtNDQ4OC1hMGFiLThmYjdjYWI2YjVlZSIsImRhdGEiOnt9LCJyYW5kb20iOiIxMDFiMzc2ZTA2YTE4YWZkMzg0NTJjYzdjZmZlYmI2NCJ9.F5KK366RTed0v21XTaQzzlwno0XOS6qiswPTCZ3cyDqfe_E1xkn6rqxhB0Sr4-LAv5iqyb6-N2Ju1hY1QiW6qw>

also here[**https://drive.google.com/file/d/1eneKrHeid-Zo6w17pdJZ2VGQ69wBuU5g/view?usp=drive\_link**](https://drive.google.com/file/d/1eneKrHeid-Zo6w17pdJZ2VGQ69wBuU5g/view?usp=drive_link).

## 2.1. Steps to replicate and build on the published results of the proof of concept (PoC) under test

A high-level summary can be found in [3] Priceless Exchange: The Rise of @mo (Part II): Future Quantum-AI-Guarded Cyber Currency for the Unbuyable.

The protection of digital assets via cryptographic private keys or secrets typically involves the secure storage and use of a private key or secret to gain access to the asset. In cases where assets are protected by a private key, if the key is lost, the protected assets may be permanently lost. Owners of assets protected by private keys may wish to ensure their assets are not lost in the event of their death or incapacitance by providing some level of access or backup to their heirs while not relinquishing control of their assets until the right time.

The tool under test includes the above concepts; Those concepts like merging process or merge authority simply describe how your digital assets should be distributed (merging process) among your chosen beneficiaries and the executor (merge authority or notary), the person responsible for executing your wishes and ensuring the distribution of your assets as outlined in your plan.

### 2.1.1. Step 1- Sign-up on the tool.

The first step consists of a simple sign-up on this specific website link:

<https://inheriti.com/?via=pedro-juan> .The screenshot below (Figure 1) describes the first step to sign-up on the tool. Note that the following link <https://docs.inheriti.com/> includes key vendor documentation.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a phone  AI-generated content may be incorrect. |
| (a) | (b) |

Figure 1. This figure shows the sign-up page of the proof of concept (PoC) under test: (a) The sign-up page is contained in the first panel; (b) The link to create an account is contained in the second panel.

The screenshot below (Figure 2) describes how the sign-up form is filled out on the tool. This step creates a so-called SafeID Account.

Note that it is also possible to leave the authentication process to other platforms playing the role of Identity Providers (IdPs) such as Apple, Facebook, Google or X. Those platforms can confirm our identity by using an existing account and redirecting us back to the tool (OpenID Connect and Oauth 2.0 protocols).

Sign-up using OIDC protocol allows external Identity Providers where Multi-Factor Authentication (MFA) and several MFA strengths can be defined.

|  |  |
| --- | --- |
| A screenshot of a sign up and sign up form  AI-generated content may be incorrect. | A screenshot of a login form  AI-generated content may be incorrect. |
| (a) | (b) |

Figure 2. This figure shows the sign-up form of the proof of concept (PoC) under test: (a) The sign-up form is contained in the first panel; (b) An example of the sign-up form completed is contained in the second panel by setting up a username and password.

The screenshot (Figure 3) below describes the email verification step after completing the sign-up form on the tool.

|  |  |
| --- | --- |
| A close-up of a email  AI-generated content may be incorrect. | A screenshot of a phone  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 3. This figure shows the email verification process of the proof of concept (PoC) under test: (a) The email verification page is contained in the first panel; (b) The email address verification confirmation is contained in the second panel. This confirmation takes place after the user clicks on the verification link received by email.

The screenshot (Figure 4) below describes how to log in to the tool.

|  |  |
| --- | --- |
| A screenshot of a login page  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 4. This figure shows how to log in to the tool of the proof of concept (PoC) under test: (a) The login page is contained in the first panel; (b) The initial page, the dashboard of the tool is contained in the second panel.

### 2.1.2. Step -2. Display your @mo bank accounts and account balance using so-called Plan Shares (PS).

Plan Shares (PS) can be of two types: Mobile Plan Shares (MPS) and Cold Plan Shares (CPS), depending on where they are stored, in a mobile app for Mobile Plan Shares or stored in a specific USB device (also known as Safe ID Key) for Cold Plan Shares.

Mobile Plan Shares (MPS) require setting up an email address to link a set up the app before the protection plan can be created. By contrast, Cold Plan Shares (CPS) can be stored in a physical device that can be handled to the right person at any moment or when needed without the need to install a mobile app nor setting up an email.

These cold shares can be useful for certain scenarios. The screenshot (Figure 5) below lists the information on the Mobile Plan Shares (MPS) and Cold Plan Shares (CPS) of Digital Inheritance Plans (DIPs) you hold.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 5. This figure shows the Mobile Plan Shares (MPS) and Cold Plan Shares (CPS) of Digital Inheritance Plans (DIPs) of the proof of concept (PoC) under test: (a) The Mobile Plan Shares (MPS) are contained in the first panel; (b) The Cold Plan Shares (CPS) are contained in the second panel.

Your Plan Shares (PS) list all the Digital Inheritance Plans (DIPs) you hold and all the ones you are appointed as a beneficiary by their respective Plan Owner (PO).

You have access to the intangible digital assets defined in the DIPs described in the merge process: When the merge process takes place, you have a temporary time window to access the encrypted data stored under the DIPs for which you are appointed as a beneficiary.

A so-called Digital Inheritance Plan (DIP) is a vendor-specific type of Protection Plan (PP) to safeguard digital assets, for instance, the @mo currency. This DIP is designed to cater to specific needs regarding data security and digital legacy management, providing users with specific options to safeguard their digital assets.

Furthermore, in this type of PP, the plan owner (PO) by default plays a passive role, as he cannot hold shares nor be a merge authority (MA), his beneficiaries are defined as heirs, and in this type of PP the PO also provides a passive approval to open the digital inheritance plan simply by not taking specific actions defined in the plan, for instance, login within a defined period.

The creation of Digital Inheritance Plans (DIPs) includes the tasks described in the following sections.

### 2.1.3. Step -3. Select the Protection Plan type and create the Plan with the type Inheritance Plan.

The screenshot (Figure 6) below describes the step to create a DIP on the tool.

|  |  |
| --- | --- |
| A screenshot of a blue box  AI-generated content may be incorrect. | Screens screenshot of a computer screen  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 6. This figure shows how to create a DIP in the proof of concept (PoC) under test: (a) The button “create a protection plan” is contained in the first panel; (b) The two types of PP are contained in the second panel.

The screenshot (Figure 6) below describes the entry form to create a DIP on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | Screens screenshot of a computer screen  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 6. This figure shows how to create a DIP in the proof of concept (PoC) under test: (a) The DIP form page is contained in the first panel; (b) The link to create an account is contained in the second panel.

### 2.1.4. Step -4. Define your Plan

This includes the following sub-steps:

#### 2.1.4a. Step -4a. Define your Plan Details

This includes the title and description (visible to all beneficiaries, so-called heirs, and the merge authority) so that they all understand what data is within the shares that this protection plan holds.

The screenshot (Figure 7) below describes how to enter the details that define your PP on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 7. This figure shows the JSON format used to enter the PP details in the proof of concept (PoC) under test: (a) The JSON formatting page is contained in the first panel; (b) The formatted data entered is contained in the second panel.

This includes the title and description (visible to all beneficiaries, so-called heirs, and the merge authority.

Within the data message, there is certain information that needs to be visible and certain information that can be encrypted for the intended audience:

Id, Creditors (Beneficiaries), Debtor (Plan Owner), Merge Authority (Notary), Domain, Title, Value: These are fields visible by the Merge Authority and the algorithm to find the shortest path between creditors and debtors. The value can be added to the title to facilitate better visibility.

Note that the Merge Authority may publish a so-called Revocation List which includes all ids whose value is zeroed by the Merge Authority. Merge Authority shall zero all assets that have been stolen or hacked and shall also prevent the initiation of any merging process where those assets are involved.

The confidential data included in the asset entry form dedicated to that purpose is only visible to beneficiaries when the merging process takes place. If applicable, consider including instructions for your digital assets, such as clear instructions for the Merge Authority on the action a beneficiary should take to confirm the acceptance of the value of the asset. Otherwise, the Merge Authority (MA) may revoke the value of the asset by publishing the id of the asset in the revocation list.

The Creditors (Beneficiaries) and Debtor (Plan Owner) need to have a unique code being used in the different PPs managed by the different Plan Owners. This unique identifier facilitates the creation of the adjacent matrices that define the shortest path from one account to another.

The value of an asset for this PoC is a whole number that ranges between 1 and 100. This is like the different banknotes of a currency.

{

"id": "000001",

"Title": "1.00@mo - Safe my life during medical emergency in a plane",

"Data": "XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",

"Merge Authority": [

{

"type": "@mo",

"Merge Authority Number": "000001",

"Domain": "healthcare"

}

],

"Beneficiaries": [

"Mila",

"Manuel",

"Pilar"

],

"Currency": "@mo",

"Value": "1.00",

"KYC": "Passport",

"cyber security measures": null

}

The screenshot (Figure 8) below describes how to enter some private notes visible to the PP owner on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 8. This figure shows the private notes form of the proof of concept (PoC) under test: (a) The private notes form is contained in the first panel; (b) The next step is to add heirs as shown in the second panel.

### 2.1.5. Step -5. Define your *address book* with so-called *trusted beneficiaries or heirs* (transfer recipients).

The screenshot (Figure 9) below describes the step to set up trusted beneficiaries on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 9. This figure shows the list of beneficiaries of the proof of concept (PoC) under test: (a) The set-up page is contained in the first panel; (b) A sample of beneficiaries is contained in the second panel.

In this step, you decide who your transfer recipient is and their @amo bank account numbers, using the above-mentioned trusted beneficiaries concept. The screenshot (Figure 10) below describes the entry form for beneficiaries on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer screen  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 10. This figure shows the entry form to add beneficiaries on the proof of concept (PoC) under test: (a) The setup page is contained in the first panel; (b) A sample beneficiary account is contained in the second panel.

The screenshot (Figure 11) below describes an additional entry form for beneficiaries on the tool.

|  |  |
| --- | --- |
| A screenshot of a phone  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 11. This figure shows the entry form to add beneficiaries on the proof of concept (PoC) under test: (a) The set-up page is contained in the first panel; (b) A sample beneficiary account is contained in the second panel.

It is required that only one beneficiary is set per asset and per protection plan together with the merge authority.

If more beneficiaries are needed, this can be accomplished by setting up different assets and different protection plans. This facilitates finding the shortest path from one account to another, as defined later.

Note that the tool may allow setting up several beneficiaries, but this scenario shall be only used by the Clear Authority to settle the accounts once the shortest path from one account to another has been found.

The screenshot (Figure 12) below describes how to select the beneficiaries and add them to the PP on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a chat  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 12. This figure shows the add button of the proof of concept (PoC) under test: (a) The add button is contained in the first panel; (b) The added beneficiaries are contained in the second panel.

The screenshot (Figure 13) below describes how to add the Merge Authority (MA) to the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a chat  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 13. This figure shows the merge authority designation on the proof of concept (PoC) under test: (a) The heir or beneficiary is contained in the first panel; (b) The heir is designated merge authority in the second panel.

Beneficiary Shares are all shares distributed among the individuals you designate as beneficiaries. These shares contain parts of your encrypted data but are not sufficient on their own to access the information. They ensure that no single beneficiary can access the information alone, safeguarding against unauthorized data retrieval. The (Figure 14) below describes the two options to store the Beneficiaries shares defined on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 14. This figure shows the two options to store the heir’s shares defined on the proof of concept (PoC) under test: (a) The option to use a mobile app to store the shares is contained in the first panel; (b) The the requirement to have an email address set up for the mobile app shares is contained in the second panel.

Merge Authority Share vs Regular Plan Shares: In your protection plan, one of the critical roles is that of the Merge Authority, the individual designated to initiate the merging process.

This distinction creates two specific types of beneficiary shares within your plan:

Merge Authority Share: This share is uniquely assigned to the Merge Authority. It empowers them to start the merging process of all shares, facilitating access to the protected data. This share is essential for activating the retrieval of encrypted information.

Regular Plan Shares: Held by other beneficiaries, these shares are crucial for data recovery but do not have the authority to initiate the merging process. They can only participate in the recovery process when the Merge Authority activates the merge.

These roles ensure a balanced distribution of power within the plan, safeguarding against unauthorized access and ensuring that the merging process is executed under controlled and intended conditions.

The Validator Share acts as a critical security mechanism within your protection plan. It remains securely stored on the blockchain and is only released under the specified conditions of a plan's activation methods, ensuring that plan activation follows your predefined criteria.This share helps validate the merging process of other shares, ensuring that all actions are authorized and in line with the owner's intentions.

The screenshot (Figure 15) below describes the steps to select the validator shares on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screen shot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 15. This figure shows the types of validator shares of the proof of concept (PoC) under test: (a) The type of shares based on cost, security and speed are contained in the first panel; (b) The details of the distinct types are contained in the second panel.

**2.1.6. Step -6. Choose where your data messages will be stored, from blockchain to physical devices and mobile phones.**

The screenshot (Figure 16) below shows information about the technology to store the encrypted data on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A close-up of a text  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 16. This figure shows the different blockchain technologies embedded in the proof of concept (PoC) under test: (a) Vechain and Ethereum information is contained in the first panel; (b) Information on Optimism is contained in the second panel.

**2.1.7. Step -7. Define your asset transfer schedule and select how your intangible asset should be accessed using so-called advanced activation methods and Dead Man Switch (DMS).**

The merging process begins when the Merge Authority, a designated beneficiary within the protection plan, initiates the merge. This triggers the countdowns for the activation methods tied to the plan.

The so-called Dead Man Switch (DMS) is employed in inheritance plans and automatically triggers if the plan owner fails to take the necessary action within the set time frame. For instance, if the plan owner fails to log in within a period of 30 days.

Once the activation methods are successfully triggered, the validator share is released from the blockchain. The Merge Authority, together with the selected beneficiaries, then combines all the required plan shares, reconstructing the data to make it accessible. This is referred to as “Combining All Shares.”

Then, the merged shares reveal the original, unencrypted data. This is referred to as “Reveal the Data.” This data is now visible -for a selected maximum amount of time- on the screen of the Merge Authority and, thus, to all beneficiaries present.

The merging process ensures that the plan owner’s data remains secure and inaccessible until all the correct conditions are met. This process adds an extra layer of security by making sure that no single person or entity can access the data on their own, without permission from the plan owner and other beneficiaries. It is a crucial part of both protecting and eventually retrieving valuable digital assets.

By carefully configuring the protection plan, selecting trusted beneficiaries, and choosing the right activation methods, the merging process becomes the secure bridge between encrypted data and the moment it is needed.

The screenshot (Figure 17) below describes the so-called Dead Man Switch (DMS) on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 17. This figure shows the different activation methods embedded in the proof of concept (PoC) under test: (a) A list of activation methods such as login days or sms are contained in the first panel; (b) The selection of several activation methods is contained in the second panel.

**2.1.8. Step -8. Define your intangible assets using so-called data messages. You are securing your intangible assets in the same way you secure other data messages or digital assets such as your message or instructions.**

Your intangible assets need to be defined so that only the merge authority has the capability to initiate the merging process and either transferring the asset value to the beneficiaries or the publication of the assets in a revocation list based on the instructions of the plan owner written on the data message.

The definition of your intangible assets requires data messages with specific information.

Your intangible assets need to be defined so that they can be traded considering all the domains or within the domain in scope e.g., healthcare.

The definition of your intangible assets requires data messages with specific information like accounting terms to be included such as:

Assets that are held by a person. These are balance sheet accounts that can be used to pay liabilities. Obligations of a person that are payable are called liabilities. They are settled by current assets transferred to the creditor. A person to whom money is owed is known as a creditor.

A data message includes the following information: Source or Creditor, Destination or Debtor. If known, value of the debt signed by the creditor, however if that is not known, the value can be set to by default to the highest possible value e.g. 100@mo and then what action expected from the Creditor to prove for the Merge Authority of the debt being paid.

In addition, (optional) the signature of the debtor using a private key for signature. The public key pair is then shared with the Merge Authority.

This information included in the data message is necessary for finding the shortest paths between nodes in a weighted graph, which represents the nodes from source to destination.

The segments of the graph are weighed with the value with the aim of calculating the total value from source to destination. This total value is expected to be lower than the default value setup e.g., 100@mo.

Finding the shortest paths between nodes in a weighted graph facilitates that the value is the minimum feasible within the existing network of nodes.

Once the shortest paths between nodes in a weighted graph, then it is possible for the Merge Authority to set up a new PP and merge process for which all intermediary nodes participate as beneficiaries, being involved also the merge authorities.

The initiation of this new Merging process allows all shareholders to agree on the initiation of the merging process for each segment of the path. Once the new merging process is completed, all subsequent merging processes within each segment must be completed, otherwise, the Merge Authority may publish a so-called Revocation List, which includes all ids whose value is zeroed by the Merge Authority.

Merge Authority shall zero the assets of those creditors which have not completed the merging process in the same way as if they were stolen or hacked and also shall prevent the initiation of any merging process where those assets are involved.

The screenshot (Figure 18) below describes how to set up the assets or data messages on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 18. This figure shows the set-up for assets or data messages in the proof of concept (PoC) under test: (a) The single asset set up is contained in the first panel; (b) The multi-asset set-up is contained in the second panel. This multi-asset set-up allows defining a “Plain text” asset fit for purpose for each domain e.g., healthcare, care homes etc.

The (Figure 19) below describes how to set up the assets or data messages on the tool.

|  |  |
| --- | --- |
| A screenshot of a phone  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 19. This figure shows the entry form to set-up the assets or data messages on the proof of concept (PoC) under test: (a) The name of the asset which includes the value as well as the data you want to protect such as the instructions for the Merge Authority are contained in the first panel; (b) The maximum number of secret characters e.g. 256 allowed in the data to protect is contained in the second panel.

In the step above, include not only your own intangible assets but also those intangible assets you are a trusted beneficiary as well, so that ownership and the right to receive @amo currency from the party you are beneficiary can be passed through you towards your heirs or beneficiaries.

The encryption of a data message, if required for the application, is a process that requires the public key of the destinatary of the message. This public key is needed to encrypt data that only the destinatary can decrypt with his own private key.

The signature of a data message, if required for the application, is a process that requires the private key of the person that signs the message so that anyone can verify using the public key of that person that the data message was signed by him.

The (Figure 20) below describes how to generate a so-called self-signed certificate that can be used to sign or to encrypt data messages on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 20. This figure shows the selected page to generate self-certificates of the proof of concept (PoC) under test: (a) The self-certificate generation page is contained in the first panel; (b) The output once the certificate is generated is contained in the second panel.

X.509 cert:

-----BEGIN CERTIFICATE-----

MIICljCCAf+gAwIBAgIBADANBgkqhkiG9w0BAQ0FADBnMQswCQYDVQQGEwJiZTER

MA8GA1UECAwIQnJ1c3NlbHMxEDAOBgNVBAoMB0N5YmVyZXUxEzARBgNVBAMMCmN5

YmVyZXUuZXUxHjAcBgkqhkiG9w0BCQEWD2luZm9AY3liZXJldS5ldTAgFw0yNTAy

MDcxNjExMjFaGA8yMTI1MDExNDE2MTEyMVowZzELMAkGA1UEBhMCYmUxETAPBgNV

BAgMCEJydXNzZWxzMRAwDgYDVQQKDAdDeWJlcmV1MRMwEQYDVQQDDApjeWJlcmV1

LmV1MR4wHAYJKoZIhvcNAQkBFg9pbmZvQGN5YmVyZXUuZXUwgZ8wDQYJKoZIhvcN

AQEBBQADgY0AMIGJAoGBAPJHHYv0V8/tlfEEjtZtfQm2c7DTrvSbxP5TK5ZPwE36

obNunF5QE7RzlekWhjF59UqWBO6uhj7FdHK/tTVBNJyJm0H9P+7TqoajYIHam9uS

MTdFgRUc3KTBTyDtjVolPQnVhTns1xlKSG+hESySaA6u1+DWMk4nH2OwW3P1FZut

AgMBAAGjUDBOMB0GA1UdDgQWBBSkwJ1LeVzxae4h8q7OA/plejF2WzAfBgNVHSME

GDAWgBSkwJ1LeVzxae4h8q7OA/plejF2WzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3

DQEBDQUAA4GBAMsODfvOPZXmkSsAm+byifw6v3rXBapKDKgn3Q5miK51+qpA/KJa

6IxASMhXurevCzveUyIsrIa/cYB9IIhTdfEowADlDXpiD5kBXTdWMsoj4l56n4pg

3EieGFjHvqZJ9XLQeGU3pImBGssBGxYlf4RgTWXAB6n4XANbaqKfPFG9

-----END CERTIFICATE-----

Private Key:

-----BEGIN PRIVATE KEY-----

MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAPJHHYv0V8/tlfEE

jtZtfQm2c7DTrvSbxP5TK5ZPwE36obNunF5QE7RzlekWhjF59UqWBO6uhj7FdHK/

tTVBNJyJm0H9P+7TqoajYIHam9uSMTdFgRUc3KTBTyDtjVolPQnVhTns1xlKSG+h

ESySaA6u1+DWMk4nH2OwW3P1FZutAgMBAAECgYBtCoTJ0JcVBiFN8Hc5Gt4D2RII

q706akEnFdewNwSeFAdi8o1+BRxZQwxdc73B1toHT624nuPcrJHUc2PjLA245hqj

VQK7pBt92zSnYIX1zyk3M6V/mXcMMFLCIMVMGP4I8juFLp0Cak0mabWpEwefDwda

0coZWbkxdgXVKeKSIQJBAP6iZ4AmALkHjEcU1vPbHpCDH96t0ZxYvdeQPVRf/Oiv

0FEwn8KZ6Zhnj4+Aot0KnEXycTpAPxs7l7QLjryDYwMCQQDzk78QzWi7qNzc3S1S

Qi0YvYUQVxbLyuIO5sq17XGGnknU1YttORSw+sSDeBLDdDPuf9bYqCeXtMNQMYaE

QW+PAkEAhshsRLbY9xf5tr5fMWExAomF2xbitwF6K5pb/Ed61agKeo9kYVua/GME

6I7MpngxVA0KxiyvuriGinT7rulVBQJAW2c5DsQWJj2iy9rP1AtzQtJzqYMU0drL

Y84liYmVzW9+wzhzPsRpyFQCBFe9qszjY/9jDyBi4yH5HRHIqb6obwJBALXV8WC9

d+0alsJqbJWgKG8JT0BL5Wcp4vBhMQvE+CfIt0IBx8H6nAjfehYFZ4qj1qB7HYjW

oV(intentionally deleted)

-----END PRIVATE KEY-----

CSR:

-----BEGIN CERTIFICATE REQUEST-----

MIIBpzCCARACAQAwZzELMAkGA1UEBhMCYmUxETAPBgNVBAgMCEJydXNzZWxzMRAw

DgYDVQQKDAdDeWJlcmV1MRMwEQYDVQQDDApjeWJlcmV1LmV1MR4wHAYJKoZIhvcN

AQkBFg9pbmZvQGN5YmVyZXUuZXUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB

APJHHYv0V8/tlfEEjtZtfQm2c7DTrvSbxP5TK5ZPwE36obNunF5QE7RzlekWhjF5

9UqWBO6uhj7FdHK/tTVBNJyJm0H9P+7TqoajYIHam9uSMTdFgRUc3KTBTyDtjVol

PQnVhTns1xlKSG+hESySaA6u1+DWMk4nH2OwW3P1FZutAgMBAAGgADANBgkqhkiG

9w0BAQ0FAAOBgQCsr+ndyYy4RuOqjdF8CqOTGeDb6vbwM3152DwnKl0PfbcxDwci

AM34ri2Qah6y/bAORJnajJ4JwkJU8bBwlT34ORMn5d9MXsBAAiMKpDuBV2xkaVR6

dr1qCQ8Y4DPX1jhn/OlRG1G+y3MOfFpfwQXdJngx+wLCOXzUpD4AK4SQSw==

-----END CERTIFICATE REQUEST-----

The (Figure 21) below describes how to calculate a short string known as “fingerprint” that designates the certificate on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. |  |
| (**a**) | (**b**) |

Figure 21. This figure shows the fingerprint calculation page of the proof of concept (PoC) under test: (a) The sign-up page is contained in the first panel; (b) The fingerprint detail is contained in the second panel.

FingerPrint:

62c36c99c1dd6b5e303db9c48dd583dc612e04e5b9198786e52f13e0db22a403

The (Figure 22) below describes how to encrypt the data message on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 22. This figure shows the steps to encrypt using the proof of concept (PoC) under test: (a) The step to convert the JSON message into XML format to be encrypted is contained in the first panel; (b) The step to encrypt the XML format of the data message is contained in the second panel.

Encrypted XML:

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" Type="http://www.w3.org/2001/04/xmlenc#Element"><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/><dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"><xenc:EncryptedKey><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1\_5"/><xenc:CipherData><xenc:CipherValue>8Mfg9dvHvI5j+2X4CZpIjzQhiFn8Fl6d7cwjoiZmaC/ONgJNr9FpDo7R+ZhHTOpNuK6rbpntpkBxEhT41cZ5WVC3dNrFeQ3jF/3v1SavTB4ovfuPJWHuhks/8R91YNZEyKER7deeDNWdle5j1uB3hLxeWhDF5+oF95r/vzcwHZ4=</xenc:CipherValue></xenc:CipherData></xenc:EncryptedKey></dsig:KeyInfo>

<xenc:CipherData>

<xenc:CipherValue></xenc:CipherValue>

</xenc:CipherData>

</xenc:EncryptedData>

The (Figure 23) below describes steps to decrypt a data message on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 23. This figure shows the sign-up page of the proof of concept (PoC) under test: (a) The sign-up page is contained in the first panel; (b) The link to create an account is contained in the second panel.

Decrypted XML:

<root>

<id>000001</id>

<Title>Safe my life during medical emergency in a plane</Title>

<Data>XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX</Data>

<Beneficiaries>Mila</Beneficiaries>

<Beneficiaries>Manuel</Beneficiaries>

<Beneficiaries>Pilar</Beneficiaries>

<Currency>@mo</Currency>

<Value>10.00</Value>

<KYC>Passport</KYC>

<Merge\_Authority>

<type>@mo</type>

<Domain>healthcare</Domain>

<Merge\_Authority\_Number>000001</Merge\_Authority\_Number>

</Merge\_Authority>

<cyber\_security\_measures/>

</root>

Note: It is possible to include additional fields such as a binary timestamp for instance, 181022 in binary <Timestamp>101100001100011110</Timestamp>

### 2.1.9. Step -9. Review of Inheritance Plan.

The screenshot (Figure 24) below describes the step to review the PP on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a chat  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 24. This figure shows the final review of the plan to be created using the proof of concept (PoC) under test: (a) The first part of the review plan page is contained in the first panel; (b) The second part of the review plan page is contained in the second panel.

The screenshot (Figure 25) below describes the step to review the PP on the tool.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a cell phone  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 25. This figure shows the final review of the plan to be created using the proof of concept (PoC) under test: (a) The third part of the review plan page is contained in the first panel; (b) The fourth part of the review plan page is contained in the second panel.

### 2.1.10. Setting up the route for the asset transfer using the so-called Dijkstra's algorithm

This step describes how accounts are interconnected so that it is possible to find the chain of accounts that establish a route between two accounts considering all the domains or within the domain in scope e.g., healthcare.

This step is detailed in [1] Navarro Vera, P.J. In the Book Quantum-AI-Guarded Cyber Currency for intangible tokens (Part II), 1st ed; Publisher: F1000 journal (Feb 2025), Brussels, Belgium, 2025.

Interestingly, Edsger Dijkstra, in an interview stated that this algorithm was designed in about twenty minutes. One morning I was shopping in Amsterdam with my young fiancée, and tired, we sat down on the café terrace to drink a cup of coffee, and I was just thinking about whether I could do this, and I then designed the algorithm for the shortest path. As I said, it was a twenty-minute invention - [6] "An Interview with Edsger W. Dijkstra."

The screenshot (Figure 26) below describes how to define the route between all accounts by using a graph and an equivalent adjacent matrix.

|  |  |
| --- | --- |
| A diagram of a number  AI-generated content may be incorrect. | A screenshot of a computer code  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 26. This figure shows the Dijkstra's Algorithm applied to the solution under test: (a) The implementation of the network graph that interconnect all accounts; (b) The equivalent adjacency matrix used by the Dijkstra's Algorithm for finding the shortest paths between nodes in a weighted graph is contained in the second panel.

### 2.1.11. Setting up the asset transfer or payment using a so-called merging process.

The (Figure 27) below describes an example of four assets of value 10,20,30 and 1000 that need to be set up in the merging process. Each asset is behind its own Protection Plan (PP). Assets behind a protection plan (PP) are managed by the plan owners e.g., 0,1,2,3. Plan owners can also be beneficiaries of assets managed by another plan owner. The accounts in the diagram are 0,1,2 and 3. The arrow in the diagram shows the direction from the PP creditor to the debtor, so that 2 is beneficiary of 3, and 1 is beneficiary of 1, and 0 is beneficiary of 1 and so on.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 27. This figure shows the Dijkstra's Algorithm applied to the solution under test: (a) The implementation of Dijkstra's Algorithm for finding the shortest paths between nodes in a weighted graph; (b) The sign-up form is contained in the second panel.

The assets are created only by the debtors.

The only route to settle the accounts is to follow the arrows.

The merging process is set to provide an agreement for all shareholders.

The merging process applied to this graph can be initiated once that 3 agrees to settle the account with 0 when 2 settles the account with 3, and this will happen in the same moment that 1 settles the account with 2 as a result that 0 settles the account with 1.

This merging process can be expressed under the following notation:

The (Figure 28) below describes the way this merging process can be expressed under the following notation:

|  |  |
| --- | --- |
| A white background with black text  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 28. This figure describes the notation for the merging process applied to the solution under test: (a) The notation of Dijkstra's Algorithm for the shortest paths between nodes 0 and 3 in a weighted graph; (b) The shortest path length (60) from node 0 to node 3 is contained in the second panel.

Note: The assets have different values by default. If assets are divided into several ones, then it is possible a partial settlement of the accounts. Otherwise, by default, the merging process can be set to clear the values of all involved assets by default, no matter if the value of each asset is different. All the Plan Owners involved can agree to clear the values of the assets by default if they are willing to do so.

The Clear Authority, upon request, can create an overarching PP with value zero that holds the information needed to initiate manually or automatically all PPs behind the plan owners. The overarching plan is set up with the same merge authorities as the one involved in the PPs behind the overarching PP.

The screenshot (Figure 29) below describes the way this merging process can be expressed under the following equations:

|  |  |
| --- | --- |
| A white background with black text  AI-generated content may be incorrect. | A white background with black text  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 29. This figure describes the notation for the merging process applied to the solution under test: (a) The notation of Dijkstra's Algorithm for the shortest paths between nodes 0 and 3 in a weighted graph; (b) The route equation for the shortest path length (60) from node 0 to node 3, the simplification equation considering the same value, and the PP overarching clearing equation is contained in the second panel.

All Plan Owners are shareholders of this overarching PP that once created by the Clear Authority it can only be initiated by the Merge Authority. The Plan owner of the overarching PP is in fact the so-called Clear Authority and the beneficiaries are the rest of Plan Owners involved.

Once the merging process is completed and data retrieval happens, all creditors must confirm as per the instructions created by the debtors of all PPs involved in the merging process so that assets are cleared.

**Only the merge authority has the capability to initiate the merging process of the overarching PP and, afterwards, each of all PPs that form the overarching PP.**

Furthermore, in this type of PP so-called Digital Inheritance Plan (DIP), the *plan owner (PO)* by default plays a passive role, as he cannot hold shares nor be a merge authority (MA), his beneficiaries are defined as heirs, and in this type of PP the *PO* also provides a passive approval to open the digital inheritance plan simply by not taking specific actions defined in the plan, for instance, login within a defined period.

The (Figure 30) below describes the first step to initiate the merging process on the tool. To initiate the merging process and unveil the protected data, the Merge Authority needs to connect their SafeKey device that holds the Merge Authority shares. You must click the selector “I’m the Merge Authority and have my SafeKey device with Merge Authority shares available” and then you can either scan a QR code or insert a usb device so-called SafeKey Device.

|  |  |
| --- | --- |
| A screenshot of a phone  AI-generated content may be incorrect. | A screenshot of a phone  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 30. This figure shows the merge process of the proof of concept (PoC) under test: (a) The merge page is contained in the first panel; (b) The link to create an account is contained in the second panel.

By combining the so-called **encrypted plan shares** using the predefined **conditions of the activation methods**, the data is reconstructed safely and accurately, just as intended.

## 2.2. Fungible non-tangible digital tokens applied to relevant scenarios under test such as healthcare, nursing home, peacekeeping, and humanitarian aid domains

### 2.2.1. Healthcare domain.

For this scenario, the healthcare domain of each asset behind each protection plan can be defined as in the following example.

The screenshot (Figure 31) below describes how to enter the details that define your PP on the tool for this scenario.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 31. This figure shows the JSON format used to enter the PP details in the proof of concept (PoC) under test: (a) The JSON formatting page is contained in the first panel; (b) The formatted data entered is contained in the second panel.

{

"id": "000001",

"Title": "1.00@mo - Safe my life during medical emergency in a plane",

"Data": "XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",

"Merge Authority": [

{

"type": "@mo",

"Merge Authority Number": "000001",

"Domain": "healthcare"

}

],

"Beneficiaries": [

"Mila"

],

"Currency": "@mo",

"Value": "1.00",

"KYC": "Passport",

"cyber security measures": null

}

Note: It is possible to include additional fields such as a binary timestamp for instance, 181022 in binary "Timestamp": "101100001100011110". This timestamp can be written in a physical coin, which might be transferred as well to better symbolize the digital transaction.

### 2.2.2. Nursing home domain.

For this scenario, the nursing home domain of each asset behind each protection plan can be defined as in the following example.

The screenshot (Figure 32) below describes how to enter the details that define your PP on the tool for this scenario.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 32. This figure shows the JSON format used to enter the PP details in the proof of concept (PoC) under test: (a) The JSON formatting page is contained in the first panel; (b) The formatted data entered is contained in the second panel.

{

"id": "000004",

"Title": "1.00@mo - Took care of my hubsband's life during humanitarian emergency as he was in the ICU with COVID and already on the ventilator and there was nothing I could do from 3000 miles away",

"Data": "XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",

"Merge Authority": [

{

"type": "@mo",

"Merge Authority Number": "000004",

"Domain": "nursing home"

}

],

"Beneficiaries": [

"Kathleen Bartholomew"

],

"Currency": "@mo",

"Value": "1.00",

"KYC": "Passport",

"cyber security measures": null

}

Note: It is possible to include additional fields such as a binary timestamp for instance, 181022 in binary "Timestamp": "101100001100011110". This timestamp can be written in a physical coin, which might be transferred as well to better symbolize the digital transaction.

### 2.2.3. Peacekeeping domain.

For this particular scenario, the pacekeeping domain of each asset behind each protection plan can be defined as in the following example.

The screenshot (Figure 33) below describes how to enter the details that define your PP on the tool for this scenario.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 33. This figure shows the JSON format used to enter the PP details in the proof of concept (PoC) under test: (a) The JSON formatting page is contained in the first panel; (b) The formatted data entered is contained in the second panel.

{

"id": "000002",

"Title": "1.00@mo - Safe my life during humanitarian emergency in the yugoslav war in the city of Konjic in 1993",

"Data": "XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",

"Merge Authority": [

{

"type": "@mo",

"Merge Authority Number": "000002",

"Domain": "pacekeeping"

}

],

"Beneficiaries": [

"Monterde"

],

"Currency": "@mo",

"Value": "1.00",

"KYC": "Passport",

"cyber security measures": null

}

Note: It is possible to include additional fields such as a binary timestamp for instance, 181022 in binary "Timestamp": "101100001100011110". This timestamp can be written in a physical coin, which might be transferred as well to better symbolize the digital transaction.

### 2.2.4. Humanitarian aid domain.

For this scenario, the humanitarian aid domain of each asset behind each protection plan can be defined as in the following example.

The (Figure 34) below describes how to enter the details that define your PP on the tool for this scenario.

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 34. This figure shows the JSON format used to enter the PP details in the proof of concept (PoC) under test: (a) The JSON formatting page is contained in the first panel; (b) The formatted data entered is contained in the second panel.

{

"id": "000003",

"Title": "1.00@mo - Safe my life during humanitarian emergency as I was one of the displaced persons and returnees who had escaped the conflict that the Horn of Africa nation has experienced since the collapse of the central government in 1991",

"Data": "XXXXXXXXXXXXXXXXXXConfidencialXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",

"Merge Authority": [

{

"type": "@mo",

"Merge Authority Number": "000003",

"Domain": "humanitarian aid"

}

],

"Beneficiaries": [

"Father Vincenzo Barbieri"

],

"Currency": "@mo",

"Value": "1.00",

"KYC": "Passport",

"cyber security measures": null

}

Note: It is possible to include additional fields such as a binary timestamp for instance, 181022 in binary "Timestamp": "101100001100011110". This timestamp can be written in a physical coin, which might be transferred as well to better symbolize the digital transaction.

### 2.3. The use of applicable Know Your Client (KYC) best practices.

Every Merge Authority has a unique view of how to balance speed, conversion, and fraud mitigation during the identity verification process. As best practices, Document & Identity Verification for Streamlined Onboarding is recommended.

This means that at least the user is asked to take a photo of their government-issued identity document and a simple selfie. This can be completed on a device and platform of their choice. The government-issued identity document is in the field <KYC>Passport</KYC> included in the data message. Please be aware that the setup of the KYC on-boarding and the credit assignment procedure are beyond the scope of this guide.

The screenshot (Figure 35) below describes how to upload the verification ID photo onto the tool.

|  |  |
| --- | --- |
| A close up of a person's face  AI-generated content may be incorrect. | A screenshot of a chat  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 35. This figure shows the uploaded verification ID on the proof of concept (PoC) under test: (a) The beneficiary verification ID uploaded is contained in the first panel; (b) The pool of beneficiaries is contained in the second panel.

## 2.3. Setting up your browser security

This step focuses on your data’s safety which begins in your browser and stays intact throughout the data storage and data transfer.

The screenshot (Figure 36) below describes the Mobile Plan Shares (MPS) and Cold Plan Shares (CPS) of Digital Inheritance Plans (DIPs).

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 36. This figure shows how to check the security of the browser connection to the proof of concept (PoC) under test: (a) The lock indicating a secure connection is contained in the first panel; (b) The analysis results of the link used for the connection are displayed in the second panel.

Secure website connections rely on encrypted communication, but server certificates are just one part of the process. Key exchange mechanisms, from RSA (Rivest–Shamir–Adleman) to Diffie-Hellman to Elliptic-curve Diffie–Hellman (ECDHE), ensure a balance between security and performance. While ECC is gaining traction for encryption, RSA remains dominant due to its widespread compatibility with existing systems.

However, cryptographic standards continue to evolve. Quantum computing poses potential threats to both RSA and ECC encryption, highlighting the need for future-proof security solutions. One such innovation is the QKD (Quantum Key Distribution) network, which enhances communication security by generating and managing cryptographic keys through multiple specialized layers. See <https://community.citrix.com/tech-zone/build/tech-papers/key-exchange-in-ssl-tls#_=_>

The screenshot (Figure 37) below describes an example of a QKD network as an add-on technology and service to conventional telecommunications networks.

Note that the following link includes key documentation <https://www.qkdnetsim.info/models/build/html/qkd.html>

|  |  |
| --- | --- |
| A diagram of a computer network  AI-generated content may be incorrect. | A diagram of a computer network  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 37. This figure shows an example of a QKD network: (a) The sole purpose of the QKD network is to generate, manage, and distribute cryptographic keys among arbitrary QKD nodes and to provide keys as a service to standard communications network users or applications; (b) The general purpose of cryptographic applications. Data communication is unidirectional; the applications function in a master/slave paradigm. The master is the application that sends confidential data to the peer-slave, and the slave is a simple receiving application. Protected user data is encapsulated with a QKD Application Header and sent over a public, unsecured channel. The QKD Application Header contains key information (e.g., the applied cryptographic algorithms and the unique key identifiers of the cryptographic keys used for processing data) that assists the receiving applications in processing the protected (encrypted/authenticated) packets.

Every Merge Authority has a unique view of how to balance speed, conversion, and fraud and how to balance speed and fraud mitigation when accessing the application.

As best practices, regular security testing by the Merge Authority is recommended. Note: Please be aware that the setting up of the cloud environment and the credit assignment procedure are beyond the scope of this document.

For instance, AI- web application scanning is recommended; Integrating OpenAI's advanced models and leveraging the vast repository of over 120,000 open-source Language Model Models (LLMs) available on the Hugging Face Model Hub. As an example, AI- web application scanning such as BurpGPT stands as an innovative extension to the industry-standard Burp Suite, introducing a revolutionary paradigm to web application security.

As best practices at least the Protection Plan Owner is asked to take a photo of their device compliant report. This can be completed on a device and platform of their choice. Their device compliant report is in the field <cyber\_security\_measures/> included in the data message.

The recommended security testing methodology is based on the Open Web Application Security Project (OWASP) and MITRE ATTACK Frameworks. MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

As best practices, a special flag for hacked or stolen coins is recommended. This means that at least the Merge Authority can flag those assets that have been stolen.

The Merge Authority issued flag is in the field <Hacked flag>Value</Hacked flag> included in the data message. Please be aware that the setup of the Hacked flag management and the asset zeroed procedure are beyond the scope of this guide.

# 3. Results

This section is divided by subheadings, each of them provides a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

## 3.1. Experimental results

### 3.1.1. The stabilization of volatility

The experimental results on the stabilization of volatility are described in [] Navarro Vera, P.J. In the Book Quantum-AI-Guarded Cyber Currency for intangible tokens (Part II), 1st ed; Publisher: F1000 journal (Feb 2025), Brussels, Belgium, 2025.

* In a network of 100 users, interconnected randomly, it was analised a sample of 989901 transactions, with path values between (1 and 100 units), resulting that there is a peak of the transactions via the shortest path with a value of 7 units; This means 7 jumps of 1 unit each or alternatively 3 jumps of 1,1, and 5 units each…
* The confidence level of the results is 95%.
* The margin of error for the results is 5%.

Table 1 shows 2 out of 9801 rows analysed in the first sample.

Table 1: Table representative of all the data analysed using the tool, Power BI.

|  | Transaction | Origin->Destination | Value | Shortest Path |
| --- | --- | --- | --- | --- |
| Row 1 | 1 | 0->1 | 7 | 8 83 94 1 |
| Row 2 | 1 | 0->1 | 71 | 0 83 93 11 |

1 The whole table contains 9801 rows, which are fully available in the download area. (file: proofofconcept\_output100 (1).txt)

The screenshot below shows all the data analysed using the tool Power BI (Figure 38).

|  |  |
| --- | --- |
| A screenshot of a computer  AI-generated content may be incorrect. | A screenshot of a computer  AI-generated content may be incorrect. |
| (**a**) | (**b**) |

Figure 38. This graph shows the count of @mo transactions by value: (a) The graph includes the data related to all transactions including transaction, origin and destination, value and shortest path. It includes a slicer graph to select one or all transactions, the max value of a transaction and the number of transactions by value which has a peak at value 7. All is contained in the first panel; (b) The graph includes the count of all samples; this is the count of all transactions 9801. This is included in the second panel.

The source of data for analysis is generated using a Python code that simulates a number of transactions. The transactions consider the shortest path from source to destination calculated using the Dijkstra algorithm.

### 3.1.2. The improvement of the security of these currency transactions.

In second place, the following cybersecurity measures that improve the transaction security have been identified:

* Authentication via a Sign-up form that creates a so-called SafeID Account including email verification step; Alternatively, using OIDC protocol which allows external Identity Providers where Multi-Factor Authentication (MFA) and several MFA strengths can be defined.
* Shares storage distributed across blockchain, mobile app for Mobile Plan Shares and/or stored in a specific USB device (also known as Safe ID Key) based on a patented method for transferring control of an asset private key from an initiating user to a group of users by use of a key management system. The method includes splitting, with the initiating user computing device, the asset private key into a plurality of subkeys;
* The Merge Authority may publish a so-called Revocation List which includes all ids whose value is zeroed by the Merge Authority. Merge Authority shall zero all assets that have been stolen or hacked and shall prevent the initiation of any merging process where those assets are involved.
* Verification ID process.
* Security check of their browser connection by the user.
* Security testing by the Merge Authority
* Periodic review of the device compliance report by the Protection Plan Owner.
* Security testing methodology is based on the Open Web Application Security Project (OWASP) and MITRE ATTACK Frameworks.
* As cryptographic standards continue to evolve. Quantum computing poses potential threats to both RSA and ECC encryption, highlighting the need for future-proof security solutions. One such innovation is the QKD (Quantum Key Distribution) network, which enhances communication security by generating and managing cryptographic keys through multiple specialized layers.

# 4. Discussion

These results open the discussion whether they can be interpreted in the way that each account owner can interact clearing @mo transactions with anyone in the @mo network along a chain of 7 jumps, no matter how far they are located physically. This improves the coverage of the interactions.

Future research directions may be how to deal with a batch of transactions involving different user accounts at the same time and achieve more complex interactions which may have the same common goal.

# 5. Conclusions

The conclusions highlight two key contributions of advanced technology to the stability and security of this new currency. First, Dijkstra's algorithm helps stabilize volatility, preventing the currency from becoming a speculative asset. Second, the integration of AI and quantum computing enhances transaction security, reducing the risk of hacking and ensuring a more resilient financial system.

# 6. Patents

The tool selected for the proof of concept is based on the following patent [4] Schouppe, J. Methods and Systems for cryptographic private key management for secure multiparty storage and transfer information. This patent information is available in the following link:

<https://patentimages.storage.googleapis.com/07/6f/86/d1cd53a5f07d49/US20200162246A1.pdf>

# Data Availability Statement

Data supporting reported results do not pose any Data Privacy concern as they can be randomly generated for the purpose of simulation using Python code available.

# Acknowledgments

I would like to thank the “Terracotta” members for your support during the review and discussion of this document.

# Conflicts of Interest

The author declares no conflicts of interest.

# Authors' Biography

Pedro Navarro completed his university degree in Telecommunications at ETSIT (UPM) and University of Ulm. He holds several certifications such as CISSP, CISA, CCSP and developed his career at different international organisations such as Telefonica, Indra Sistemas, Santander UK, ING Bank BE and European Parliament.

# References

1. Navarro Vera, P.J. In the Book Quantum-AI-Guarded Cyber Currency for intangible tokens (Part II), 1st ed; Publisher: f1000 journal (Feb 2025), Brussels, Belgium, 2025;
2. Navarro Vera, P.J. In the Book Priceless Exchange: The Rise of @mo (Part II): Future Quantum-AI-Guarded Cyber Currency for the Unbuyable, 1st ed; Publisher: Independently published (Dec 9, 2024), Brussels, Belgium, 2024; Volume 2. ISBN-13:979-8303202313
3. Navarro Vera, P.J. In the Book Quantum-AI-Guarded Cyber Currency for intangible tokens (Part II), 1st ed; Publisher: f1000 journal (Feb 2025), Brussels, Belgium, 2025;
4. Reilly, Robert F. Is the discipline a science or an art? In the Book Valuing Intangible Assets. Publisher: McGraw-Hill Library of Investment and Finance.
5. Navarro Vera, P.J. In the Book Priceless Exchange: The Rise of AMO (Part I): Quantum-AI-Guarded Cybercurrency for the Unbuyable, 1st ed; Publisher: Independently published (Dec 9, 2024), Brussels, Belgium, 2024; Volume 1. ISBN-13:979-8303208933.
6. Frana, P. L. Misa, T. J. In the Book "An Interview with Edsger W. Dijkstra". Communications of the ACM. (August 1, 2010). Volume 53 Issue 8 (pp 41–47). doi:10.1145/1787234.1787249
7. Schouppe, J. In the Book Methods and Systems for cryptographic private key management for secure multiparty storage and transfer information. Patent Application Publication. May 21, 2020, Brussels, Belgium, 2021. Pub. No.: US 2020/0162246 A1

# Disclaimer/Publisher’s Note

The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of F1000 and/or the editor(s). F1000 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

  Licensed under [Creative Commons Attribution-ShareAlike 4.0 International License](http://creativecommons.org/licenses/by-sa/4.0/)