Digital Inheritance without Intermediate: Securing Crypto Assets after Death

ZINEB IHROUCHEN[1], OMAR SOUISSI[1], RAJAE ABOULAICH[2]
[1]Data Analytics, Operations and Decision (DATA),
Institut National des Postes et Télécommunications (INPT),
Rabat,
MOROCCO

[2]Africa Business School,
Mohammed VI Polytechnic University (UM6P),
Rabat,
MOROCCO

Abstract: With the rise of cryptocurrencies, the issue of crypto-asset's inheritance is becoming a major challenge. Unlike traditional financial assets, these digital assets are secured by cryptographic keys and are independent of intermediaries, making their transfer after the death of the owner complex. Without proper planning, these funds risk being lost forever. This article explores the challenges and solutions associated with inheriting crypto-assets. It also examines smart contract's role in automating asset transfer while ensuring security and compliance. Finally, we propose an AI-DLT-based architecture to ensure the secure and automated transfer of crypto-assets after the death of the owner. This approach aims to prevent the loss of funds and facilitate the reliable and efficient transfer of digital assets to their rightful owners, including heirs who do not possess cryptocurrency wallets.

Key-Words: Crypto-assets, Hashgraph, Inheritance, DLT, Smart contracts, Decentralized finance

Received: November 14, 2025. Revised: February 19, 2026. Accepted: June 13, 2026. Published: July 28, 2026.

1 Introduction

The adoption of cryptocurrencies has increased in recent years, affecting different regions of the world. For instance, in the study, [1], the average global adoption rate in 2022 was 2.6%, though some countries recorded much higher rates. The United Arab Emirates had the highest rate at 28%, followed by Vietnam, Saudi Arabia, and the United States. On a continental scale Asia had the highest average adoption rate at 6%, while North and South America each had an average rate of 3%. This growth is linked to factors such as limited access to traditional banking services, a young and tech-savvy population, and a favourable regulatory environment. These factors have stimulated interest in cryptocurrencies among individual and institutional investors. This mass adoption of crypto-assets has boosted the financial sector by introducing new investment opportunities and promoting financial inclusion. Cryptocurrencies enable fast and low-cost cross-border transactions, offering solutions to unbanked and underbanked populations. In addition, the rise of underlying technologies such as Distributed Ledger Technology (DLT) including Hashgraph, Blockchain.. has increased the transparency and security of financial transactions, reducing the risk of fraud and boosting user confidence.

However, this digital revolution creates major new challenges, particularly when it comes to the succession of digital assets. Unlike traditional assets, crypto-assets are often held in a decentralised manner, without intermediaries, and are secured by private keys known only by their owner. In the event of death, if these keys are not transmitted or accessible to heirs, digital assets may be permanently lost. One notable example is QuadrigaCX, [2], Canada's leading crypto-currency processing platform, which lost around €120 million in crypto-assets after the unexpected death of its founder, Gerald Cotton, in 2018. Cotton was the only person to hold the private keys to access the funds, making them inaccessible after his death Faced with these challenges, the academic world and finance professionals are becoming aware of the importance of finding solutions to ensure the transmission of crypto-assets after the death of their owner. The decentralised nature of crypto-currencies and the absence of traditional intermediaries make it difficult to set up effective inheritance mechanisms. Traditional legal procedures do not readily apply to these digital assets, making their post-mortem transfer particularly complex.

A number of initiatives are emerging to address this issue. Companies such as Safe Haven, [3], and Casa, [4], are developing solutions to facilitate the secure transmission of crypto-assets. For example, Casa offers a combination of multi-signature authorisation and a security protocol using several keys, including one held by a specialist lawyer, enabling bitcoin assets to be recovered after a death. Safe Haven, meanwhile, has launched the Inheriti platform, which allows users to bequeath access to crypto-currencies and social network profiles,

storing encrypted information about the assets in question. However, these solutions can still be improved and are not yet widely adopted. It is therefore essential to develop robust, automated architectures for transferring crypto-assets after the owner's death. Our paper contributes to this thinking by proposing an innovative solution that incorporates automated transfer mechanisms, ensuring that legitimate heirs can access the deceased's digital assets without compromising security or confidentiality even if they do not hold a cryptocurrency wallet. This approach aims to fill the current gap in the inheritance of crypto-assets, by offering a practical and secure solution tailored to the specific features of these new forms of wealth.

Our article has followed this structure: the second section reviews the previous work on the crypto-asset inheritance, analyzing existing solutions, the third section sheds light on the challenges of crypto-asset inheritance, section 4 presents our contribution to a new AI- DLT-based architecture for crypto inheritance, section 5 compares AIAC with traditional solutions, section 6 presents a use case, section 7 include a statistical study with four tests Finally, a brief conclusion is provided.

2 Literature review

In this section, we present previous work related to crypto-asset inheritance by analysing existing solutions and major contributions proposed in recent years. The literature review covers research articles published since 2020 that address the inheritance and estate planning of digital and crypto-assets. We have noticed that the number of published studies and available solutions in this domain remains limited.

In the paper, [5], proposes an Islamic estate planning framework for crypto assets in Malaysia based on interviews with experts (lawyers, estate planners, Shariah specialists, exchange operators and crypto holders). It highlights the key role of the Securities Commission of Malaysia in protecting heirs and aligning the framework with Shariah principles. The study is based on a qualitative approach and requires validation.

Sarcophagus a blockchain-based dead man's switch, [6], system that uses Arweave to permanently store data, and Ethereum to manage the Sarco ERC20 token. Users select archaeologists who are responsible for releasing encrypted data to a final recipient. The data is initially encrypted with the archaeologist's public key and must be re-encrypted by pre-defined dates. If these dates pass without user intervention, the archaeologist decrypts the outer layer and allows the recipient to access the encrypted inner layer. This system guarantees security, immutability and resistance to censorship of sensitive data.

In the work presented in, [7], a solution for dealing with the inheritance of crypto-assets, focusing specifically on the issue of the network acknowledging the death of an individual. This death acknowledgement process could then be used to trigger inheritance transactions and contracts. The proposed solution is called the Tales From the Crypt protocol, which respects user confidentiality and remains decentralised, in keeping with the original spirit of cryptocurrencies. The paper acknowledges that many complex issues related to the inheritance of crypto assets remain unresolved, but hopes that this work will inspire future research and further advances in the field.

Ternoa, [8], a French start-up, offers a death protocol based on a smart contract triggered by local authority APIs that register deaths. However, there are several problems with this system. Firstly, it is centralised, which makes it more vulnerable to attacks than a distributed solution using cryptographic technologies. In addition, there is no common API standard between countries to deal with this problem, so each solution is limited to a single nation state. Finally, there is no guarantee that current APIs will not be changed in the future.

In the work presented in, [9], provides some examples of inheritance of digital assets. It is advisable to include specific instructions for access to funds or private keys in a will or letter of wishes. Some platforms offer API integrations that allow a period of inactivity to be set, after which digital assets are automatically transferred to beneficiaries. A case in point is Hal Finney, who placed his private keys in a safe deposit box so that his family could access his bitcoins after his death. These solutions illustrate different ways of preparing and passing on digital assets in the event of death.

In the paper, [10], proposes a digital inheritance solution via blockchain, allowing a digital executor to recover assets after the death of the testator. An M-of-N system requires the consent of the beneficiaries to confirm the death. A delay period is introduced to ensure the recovery of assets and prevent attacks. The article suggests the development of a 'digital Lego framework' to integrate different blockchain inheritance solutions.

This paper, [11], introduces a formal digital

asset inheritance (DAI) model and proposes a secure inheritance protocol (DAIP), based on certificateless and identity-based cryptography. The protocol ensures reliable posthumous asset transfer, even with limited nominee involvement, and its security and practicality have been proven through comparaison with other solutions such SafeHaven.

In the article, [12], presents the Digital Inheritance Model (DIM), an empirical model for managing digital assets after death, aimed at raising awareness of the importance of digital inheritance among young people and various stakeholders (government, academics, media). It proposes guidelines for managing digital data, taking into account individual rights, confidentiality and sentimental values. The model also encourages a review of technological and legal policies, particularly in the context of Islam.

In the article, [13], NextHeirs a quantum-resistant blockchain framework for securing and decentralising digital inheritance. It relies on verifiable Merkle trees, dilithium signatures and a decentralised death oracle to automate the transfer of assets. It integrates with IPFS to provide secure document storage. This system eliminates the shortcomings of centralised solutions and increases the transparency and efficiency of estates. NextHeirs provides permanent protection for digital assets against post-quantum threats.

Casa, [14], is a company specialises in securing cryptocurrency wallets using a multi-signature scheme, providing greater resilience and protection for digital assets. Its legacy service is based on a secure recovery scheme where multiple keys are shared between the user, trusted contacts and Casa, guaranteeing access to funds in the event of death. This model ensures the secure transfer of crypto-assets without centralisation or risk of loss.

The TrustForWills, [15], project offers a blockchain-based framework for managing digital inheritance, i.e. the transfer of digital assets and profiles upon a person's death. Relying on blockchain technology (Ethereum/Alastria + IPFS), it guarantees immutability, transparency and security through smart contracts. These allow beneficiaries to be designated and transfer conditions to be defined, with execution being automated after death or incapacity.

The article in, [16], proposes a blockchain-based conceptual framework for modernising the distribution of estates in Malaysia, a process which is often slowed down by administrative issues. In this model, several institutions are involved, including the Royal Malaysian Police (RMP), the National Registration Department (NRD), Shariah courts, the central bank and insurance companies. All their data is integrated into a blockchain platform. Once documents such as burial permits, death certificates and information on heirs have been validated, a smart contract automatically distributes assets in accordance with Islamic law.

3 The challenges of crypto-asset inheritance: Between decentralisation and Loss

3.1 Decentralised finance (DeFi)

Decentralised finance (DeFi), [17], refers to a set of financial services and applications built on distributed ledger technologies, which aim to eliminate traditional intermediaries such as banks and financial institutions. It follows on from innovations such as FinTech, RegTech, cryptocurrencies. However, DeFi raises important issues: it can weaken traditional accountability mechanisms and reduce the effectiveness of existing financial regulations. While some parts of the value chain are decentralised, others tend to become concentrated in less visible and less regulated areas. This calls for new approaches to supervision and regulation, including the integration of 'embedded' regulation directly into the design of DeFi protocols.

In short, DeFi does not eliminate the need for regulation: it redefines the means of achieving it, while paving the way for a profound transformation of finance and its modes of governance. In a recent survey study, [18], it appears with qualitative interview findings, only a small minority of cryptocurrency users reported having established any concrete backup or inheritance plan for their digital assets. Even among participants who demonstrated a correct understanding of core security concepts such as seed phrases, inheritance planning behaviors remained rare. The study highlights a substantial gap between technical awareness and actual estate-preparedness practices in the cryptocurrency ecosystem. This gap underline the need for adaptable, jurisdiction-aware solutions such as AICA.

3.2 Technological Applications in Islamic Finance

Technology is playing an increasingly important role in Islamic finance, supporting the

implementation of its principles of fairness, transparency and ethical distribution of wealth. Studies have shown that it is possible to represent Islamic economic rules using quantitative models, enabling more accurate and compliant financial decisions, [19]. Other studies indicate that technological tools can help mitigate financial distortions and strengthen the stability of the system, [20]. Simulation-based approaches have also been successfully applied to model the complexity of financial interactions within Islamic finance, [21]. In this context, DLT and smart contracts appear to be promising technologies for automating inheritance processes, thereby ensuring transparency, efficiency and compliance with Shariah principles.

3.3 Use cases for loss of crypto inheritance

We present a case of loss of crypto assets due to the lack of a prior estate plan. This case illustrates how the lack of appropriate management measures and clear instructions for the transfer of cryptocurrencies can lead to irreversible losses for heirs. In the case, [22], of QuadrigaCX founder Gerald Cotten, his sudden death resulted in the loss of $190 million in cryptocurrency, as Cotten was the only person with the private keys to access the funds. With no process in place to transfer or manage the assets, the heirs suffered irrecoverable losses.

3.4 Inherited practical challenges

The inheritance of cryptoassets after death, [23], refers to the process by which a deceased person's digital assets are transferred to their heirs. As these assets are recorded on the DLT, they can only be accessed using private keys. Inheritance therefore requires the implementation of legal and technological mechanisms that enable authorised heirs to securely recover and manage these assets.

Cryptoassets are digital assets based on DLT that provide a decentralised and secure system for managing and transferring value. They are stored in digital wallets that require a private key to access. This private key, which is essential for the ownership of crypto-assets, poses a major challenge in terms of inheritance: in the event of death, access to funds can be permanently lost if heirs do not have the necessary information. Unlike traditional financial systems (Table 1), the decentralised nature of crypto-assets means that no institution can intervene to recover or redistribute these funds. This constraint creates a trade-off between security and ease of transfer, leading some to explore hybrid solutions with elements of centralisation, such as inheritance management services based on multi-signatures or decentralised recovery protocols. below some pratical challenges.

Risk of loss of crypto-assets: In the absence of clear inheritance mechanisms, the transfer of crypto-assets after death may be impossible, especially if the private key required for access has not been shared or secured.

Centralisation of private keys: Although DLT are decentralised, private key management often relies on one person or entity, making the system vulnerable to loss if that person disappears without an estate plan.

Lack of estate planning: Most users do not take steps to prepare for the transfer of their crypto assets, leaving their heirs without access to the assets in the event of death or incapacity.

Risk of fraud and manipulation: Centralised access to critical information (such as private keys) can create opportunities for fraud or malicious manipulation, further complicating estate administration.

Lack of regulatory and legal frameworks: The lack of clear standards and regulations for the transfer of crypto-assets, [24], creates legal uncertainty, making it more difficult for heirs to access or claim digital assets.

Some Inheritance solutions for crypto-assets exist, but they often centralise the process by involving intermediaries who manage private keys and the transfer of assets.While practical, these solutions work against decentralisation and introduce risks of mismanagement, fraud or loss of control. They require considerable trust in intermediaries, which can compromise the security of crypto-assets.

3.5 Comparaison between digital and traditional inheritance

Table 1: Key difference between Traditional Inheritance and Digital Inheritance

Criteria	**Traditional Inheritance**	**Digital Inheritance**
Centralization	Centralized	Decentralized
Transfer Mechanism	Legal succession	Smart contracts
Security	Limited	High
Asset Management	Institutional management	PrivateKey management
Risk of Loss	Human error	PrivateKey loss

Source: created by the authors

3.6 Inheritance of Cryptocurrencies in Islamic Law

In Islamic law, inheritance (faraid) is a mandatory process for distributing a deceased person's assets among their heirs. distributing a deceased person's assets among their heirs, based on fixed shares, as described in the Quran and Hadith. Wealth, or Maal left by the deceased must be distributed according to these This ensures justice and fairness. As a relatively new form of wealth, cryptocurrencies are becoming increasingly important in this context, [25]. Their treatment under Islamic law requires careful analysis to ensure they comply with the principles of faraid. Islamic inheritance law derives from several key sources:
1. The Qur'an: The Qur'an is the main source of Islamic law. It contains clear injunctions regarding the distribution of property after death.
2. The Hadith: The traditions and sayings of the Prophet Muhammad (peace be upon him) provide further clarification on the application of inheritance laws. The Prophet emphasised the importance of fair and equitable wealth distribution. The Hadith also emphasises the importance of writing a will (wasiyyah) to ensure that assets, including cryptocurrencies, are distributed correctly.

4 Proposed work

This section is dedicated to the presentation of our proposed architecture.

4.1 AICA: Automated Inheritance Crypto-assets Architecture

We propose a new automated architecture that requires no intermediaries for the transfer of crypto-assets. This solution relies on the use of Decentralized Ledger Technology (DLT) and artificial intelligence (AI) to ensure a secure and decentralized process for asset inheritance. With this approach, transactions are carried out autonomously and transparently, thus reducing the risks associated with centralization and ensuring more efficient and reliable management of crypto-assets. This solution is based on the use of smart contracts and smart AI agents to guarantee a secure and decentralised process for inheriting assets. Thanks to this approach, transactions are carried out autonomously and transparently, reducing the risks associated with centralisation and guaranteeing more efficient and reliable management of crypto-assets.

Our proposed solution Figure A1 (Appendix) is based on three key components for the automated and secure transfer of crypto-assets:
AI Agent: The agent acts as a digital twin of the wallet holder, retaining access rights to the wallet and ensuring secure execution of inheritance processes, even in complex scenarios. It monitors user inactivity on the crypto wallet. Prolonged inactivity initiates a user status verification. It is also responsible for selling the crypto-assets to the bank and asking them to send the money received to the heirs according to the rules predefined in the smart contract.
Oracles: Queries external databases (death records, obituaries, etc.) to confirm whether the user is deceased.
Smart contracts: It defines the heirs, their address, the relation with the wallet owner and fully configurable—allowing updates to heirs, shares, and conditions.. Once death is confirmed, they automatically trigger the transfer of assets to designated heirs or witnesses.

The process begins with an AI agent monitoring the user's portfolio activity. If there is a period of inactivity lasting three months or more, the agent triggers a check by interrogating an Oracle, which consults external databases such as death records and obituaries to confirm the user's death using their name and identity ID predefined in the contract. Once the death is confirmed, an inheritance smart contract is automatically activated. This contract, pre-configured by the user during his or her lifetime, verifies the defined conditions, such as the identity of the heirs and the arrangements for the transfer of funds. Once validated, the crypto-assets are sent directly to the designated wallets (in case heirs have crypto wallet), ensuring automatic, tamper-proof execution. In case heirs doesn't have crypto-wallet the AI agent then sells the crypto-assets to the Bank to convert them into fiat currency. Once converted, the agent sends a request to the bank to transfer the money to the heirs according to the instructions in the smart contract. Every step of the process is recorded on the DLT, ensuring transparency, traceability,, and security. Finally, each heir automatically receives their part in their bank account or crypto wallet, guaranteeing secure and decentralised transfer without relying on an intermediary.

Features of the solution

- Total automation with no intermediaries.
- Enhanced security, and traceability.
- Flexibility and customisation
- Reliable verification of death

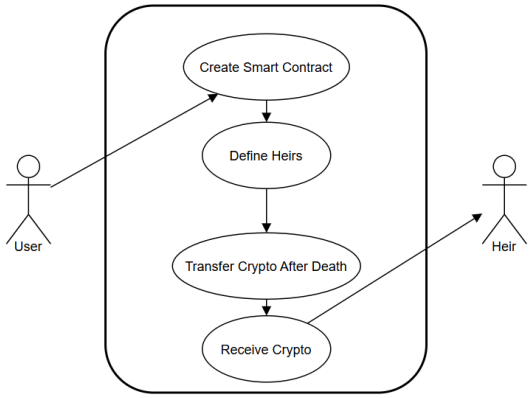

Fig. 1: Use case diagram of our crypto inheritance system
Source: created by the authors

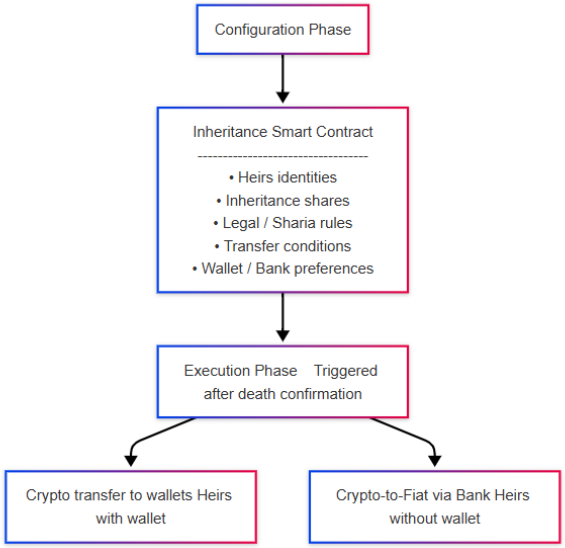

Fig. 2: Conceptual schema of the proposed smart contract for crypto asset inheritance
Source: created by the authors

The use case diagram (Figure 1) illustrates the inheritance process of crypto assets, where a user creates a smart contract specifying the heirs' identities (names and wallet addresses) and share percentages. Upon the user's death, assets automatically transfer to the designated heirs.
The flow diagram (Figure 2) details our smart contract-based crypto inheritance process, starting with the configuration phase where heirs' details (name, address of the wallet, identity ID), and inheritance shares are defined according to Shariah rules. In the execution phase, an oracle verifies the user's death via external data sources such as death certificates, or medical records using identity ID, triggering asset transfers to heirs' crypto wallets; those lacking wallets can convert their crypto assets to fiat currency.

4.2 Entire architecture with different scenarios

This architecture Figure 3 offers a more comprehensive and realistic view, taking into account the multitude of profiles of the heirs. It details two possible scenarios depending on the heirs' ability to directly manage cryptocurrencies.
First, the creation and configuration of the smart contract: the user defines their heirs, their proportions and the transfer conditions.
Second, the detection and confirmation of death: the AI agent monitors the user's activity and consults the oracle in the event of prolonged inactivity. Then the oracle confirms the death via the official register, which triggers the execution of the smart contract.
Scenario 1: (Figure 3)
Heirs without crypto wallets: the smart contract triggers a conversion module via a Crypto-to-Fiat Agent or an exchange platform, cryptocurrencies are automatically converted into fiat currency (USD, EUR, etc.). The bank then transfers the converted amounts to the heirs' bank accounts as defined in the smart contract. This scenario makes the solution accessible even to heirs with no knowledge of cryptocurrencies.
Scenario 2: (Figure 3)
As in scenario 1, the same procedure is followed, except heirs with crypto wallets: the smart contract transfers the funds directly to the heirs' crypto addresses. Each heir receives their share in cryptocurrencies, according to the distribution defined in the contract. This scenario promotes speed and reduces intermediaries.
This architecture is notable for its flexibility and adaptability, covering both heirs familiar with crypto-assets and those who prefer to receive funds directly in fiat currency.

4.3 Materials and constraints

For this work, we have chosen to use Hashgraph technology, renowned for its high performance and minimal transaction, [26]. Integration is achieved through the MetaMask wallet, ensuring seamless interaction. Hashgraph, [27], as a sustainable DLT technology, provides a solid foundation for our approach. This latter is particularly well suited to crypto-asset inheritance thanks to its high security based on Asynchronous Byzantine Fault Tolerance

(aBFT), fast and deterministic finality without forks, and fair timestamping. It guarantees reliable and automated execution of smart contracts after confirmation of death. Its scalability, low latency, and predictable costs make it an effective solution for securely managing multiple assets and heirs. We also plan to explore the use of open source Gemini API (to be confirmed) to leverage LLM to automate certain tasks.

However, we are currently facing a major constraint related to the lack of testnet platforms to simulate banking transactions and the absence of suitable exchange platforms to continue the full simulation of the process. These technical limitations are hampering experimentation, but work is ongoing and will be consolidated as soon as suitable environments become available. Meanwhile, we have initiated preliminary tests on small-scale datasets to evaluate the performance and reliability of the system under controlled conditions. These tests focus on verifying transaction speed, smart contract execution, and error handling, providing valuable insights into potential bottlenecks. The findings will guide future improvements and adjustments, ensuring that when a full testnet and exchange platforms become available, the system can operate efficiently and securely.

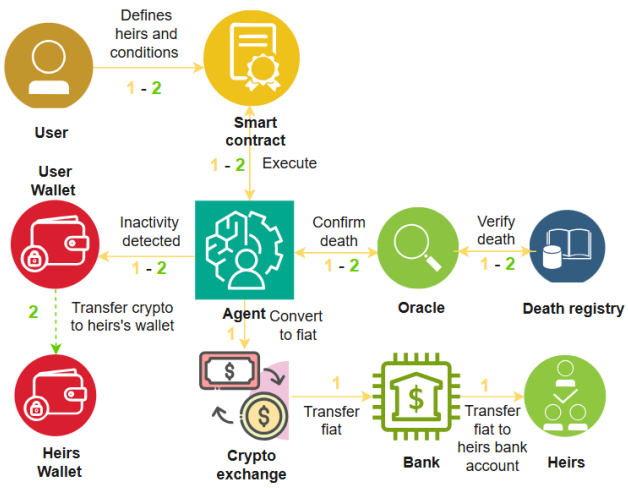

Fig. 3: Architecture of the proposed crypto inheritance system AICA with dual asset distribution options crypto and fiat
Source: created by the authors

5 Comparaison of AICA with traditional practices

5.1 Comparing with NextHeirs

NextHeirs, [13], incorporates a decentralised Oracle of Death, which is something in common with our solution. It is a quantum-resistant blockchain using Merkle trees, Dilithium signatures and decentralised death oracles. It ensures secure, transparent and efficient asset transfers without relying on centralised systems. Transfer automation: execution remains partial as it does not cover heirs without a wallet. Banking compatibility: NextHeirs does not handle crypto-fiat conversion or bank transfers, which limits its applicability in e.g Morocco. Cryptographic security: the use of quantum-resistant signatures is a strong point compared to our current approach.

Our solution retains the advantage in terms of complete automation and hybrid applicability (wallet and bank).

5.2 Comparison with bitcoin time lock inheritance solution

A solution presented in, [28], use Bitcoin time locks, wills or trusts with moderators to transfer crypto-assets. The transfer is carried out via locked contracts or the intervention of a third party who manages keys and documents, exposing the assets to the risk of fraud. Banking compatibility: these solutions already work with notaries, banks and institutions, which is a strong point. Oracle: there is no Oracle integration to verify death, so there is a dependence on paper certificates and notaries. Automation: everything relies on third-party moderators, which increases the risk of fraud, slowness and costs. DLT transparency: often limited or non-existent as it is off-chain. Legal framework: easily integrated into legislation, unlike recent blockchain solutions. Our solution outperforms others (Table 2) in this area thanks to its zero dependence on third parties, AI automation, and blockchain traceability, while maintaining banking compatibility.

6 Use case

We consider a scenario (Figure 4) where we set up a smart contract on Hashgraph network for a father who passes away, holding 1,000,000 HBAR, in accordance with Shariah law. The heirs are his wife, mother, and two sons, and he has no living father or grandparents. He specifies that the wife will receive 1/8 of the inheritance, and the mother 1/6; the remaining amount will be shared equally

Table 2: Comparison of crypto inheritance approaches

Criteria	NextHeirs	Traditional	Our solution
Death notification	Decentralised	No	National register
Transfer automation	Partial (wallet)	No	Wallet + bank
Bank compatibility	No	Yes	Yes
Third parties	No	Yes	No
Cryptographic security	Quantum strong	Medium	AI + Oracle
Practical applicability	Low	Medium	High
Technology	Quantum blockchain	Time lock	Smart contract
Transfer method	Auto on death	Executor	Auto wallet + bank

Source: created by the authors

between the two sons. The mechanism monitors the inactivity of the father's account and, after a specified period of time, automatically triggers the execution of the smart contract. The contract calculates the shares: 125000 HBAR for the wife, 166666.67 HBAR for the mother, and 354166.67 HBAR for each son, then the AI agent buy hbar to the bank, and it transfers the fiat money directly to the heir's bank account. This process ensures automatic, immutable, and transparent execution, complying with Shariah law, without human intervention and guaranteeing secure and automated inheritance.

7 Statistical studies

To support the design work by AICA and address user needs, we conducted a perception survey with 42 participants on their age, their use of cryptocurrency wallets, security practices perceptions of digital asset inheritance mechanisms, from six regions: Europe, Asia, Africa, North Africa, North America, and the Middle East. Although the sample is exploratory, it includes crypto asset holders, DLT practitioners, legal experts, and researchers. This mix offers a varied view on the challenges of digital inheritance.

7.1 Descriptive Statistics

A decentralised Survey application was specially developed for this study to collect responses. This approach ensured the transparency and integrity of the data collected. The responses were recorded directly on the Hedera Hashgraph network to prevent loss of the data, ensuring it

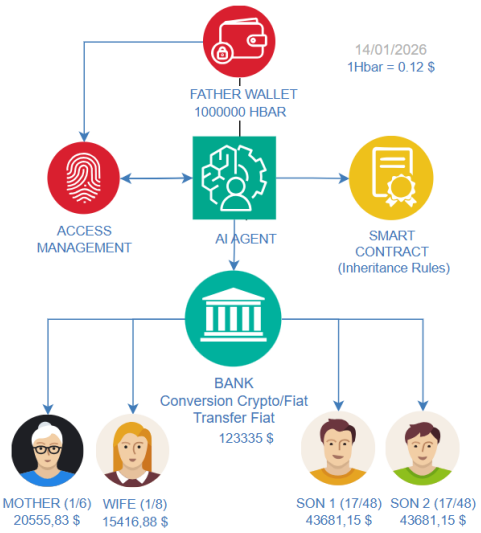

Fig. 4: Use case of crypto inheritance distribution scenario based AICA
Source: created by the authors

was stored immutably. After the collection phase, the data was extracted and analysed tools to identify behavioural trends related to private key management and digital asset estate planning. The descriptive analysis reveals significant trends in users' attitudes towards digital assets and their transfer. The results Table 3 show that most respondents own a cryptocurrency wallet and consider securing mechanisms for inheriting digital assets to be very important. However, few participants have considered planning for these assets, suggesting a potential discrepancy between risk perception and the implementation of practical solutions.

Table 3: Descriptive statistics of survey results

Indicator	Percentage
Wallet holders	73.81%
Never shared private keys	87,09%
Thought about crypto inheritance	40.48%
Aware of asset loss risk	66.67%
Importance of secure inheritance	73.81%
Trust in automated systems	54.76%
Trust in smart contracts	61.90%
Risk-aware preferring automation	33.33%

Source: created by the authors

7.2 Analytical statistics

To further the analysis, four non-parametric statistical tests were applied to the collected data: two binomial test, Mann–Whitney U test and Spearman's correlation coefficient test and

was realised using Python language.

Exact Binomial Test on PrivateKey Non-Sharing:

The exact binomial test was used to determine whether the proportion of participants who do not share their private keys is significantly greater than 0.5. We selected only participants who have a wallet (a Total of 31).

- Null hypothesis (H_0): $p(\text{non-sharing}) = 0.50$ — non-sharing is not more frequent than sharing by chance.
- Alternative hypothesis (H_1): $p(\text{non-sharing}) > 0.50$ — non-sharing is significantly more frequent (Unilateral right test).
- Significance level: $\alpha = 0.05$
- Test result: $X = 27$ successes out of $n = 31$ participants
- Since $p < 0.05$, we reject H_0 and conclude that the proportion of participants who do not share their keys is significantly higher than 50%. This suggests that non-sharing behavior is dominant among participants. (Table 4)

Table 4: Exact Binomial Test on Private Key Non-Sharing

Category	**N**	**Observed Prop.**	**Test Prop.**	**p-value**
Never shared keys	27	0.87	0.50	3.39×10^{-5}
Shared keys	4	0.13		

Source: created by the authors

The results indicate that the majority of users maintain strict control over their private keys, thus confirming statistically that key non-sharing is predominant.

Mann–Whitney test — Trust in Smart Contracts vs Ownership:

The Mann–Whitney U test was used to compare the level of trust in smart contracts between participants who owned a crypto wallet and those who did not. This analysis assesses whether direct experience with blockchain technologies influences the perception of the reliability of automated systems.

- Null hypothesis (H_0): The distributions of trust towards smart contracts are identical for both groups.
- Alternative hypothesis (H_1): The distributions differ (bilateral test).
- Significance level: $\alpha = 0.05$
- Test result: $U = 239$, $n_1 = 31$, $n_2 = 11$
- p-value: $p = 0.04$ *(significant)*
- **Interpretation:** Since $p < 0.05$, we reject H_0 and conclude that trust levels towards smart contracts differ significantly between participants who own crypto assets and those who do not. Ownership appears to influence trust perception. (Table 5)

Table 5: Mann-Whitney U Test: High Trust vs Wallet Ownership

Group	n	Trust Prop.	Mean Rank
Wallet	31	0.419	23.71
No Wallet	11	0.091	15.27

Source: created by the authors

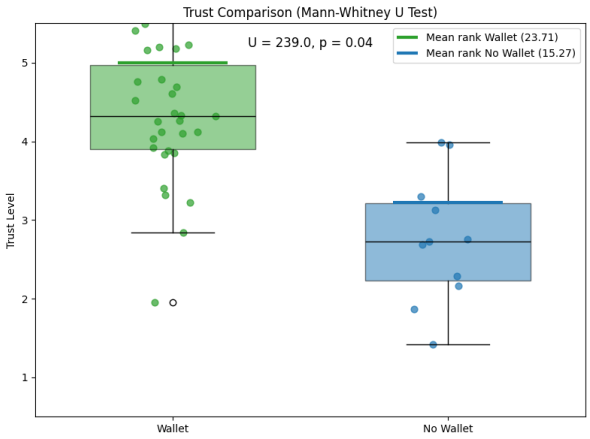

Fig. 5: Boxplot of trust scores towards smart contracts by group, with individual points overlaid.

Source: created by the authors

The Figure 5 presents the distribution of trust scores in smart contracts among owners and non-owners of crypto-assets, the trust score ranges from 1 to 5, where higher values indicate greater trust in smart contract-based systems.

Spearman's correlation — Ordinal Age × Reflection on Inheritance:

Spearman's correlation analysis, Table 6 was applied to examine the relationship between certain ordinal variables in the study, including participants' age and their views on the inheritance of digital assets. The aim of this analysis is to identify possible associations

between demographic characteristics and awareness of issues surrounding the transfer of digital assets.

- Hypothesis: As age increases, individuals are more likely to consider inheritance (ordinal correlation).
- Spearman's $\rho = 0.177$ n = 31
- p-value: $p = 0.340$ *(not significant)*
- **Interpretation:** The positive Spearman correlation indicates that older participants tend to give more consideration to inheritance. Since $p > 0.05$, this relationship is not statistically significant. The lack of significance may be attributed to the limited number of participants in each age group, which reduces the statistical power to detect a meaningful effect. As conclusion Trend observed but not significant, it highlights a potential pattern that could be further explored in larger samples.

Table 6: Spearman Correlation: Age vs Inheritance Consideration

Parameter	Value	Interpretation
Spearman's	0.177	$\rho > 0$ older $\rightarrow$ High inheritance reflection
p-value	0.340	Not significant

Source: created by the authors

Binomial test on the AICA target profile

To further assess the relevance of our inheritance proposed solution, we conducted a *binomial test*, Table 7 focusing on a well-defined target user profile. This profile corresponds to respondents who simultaneously: (i) own a cryptocurrency wallet, (ii) have never shared their private keys, (iii) are aware of the risk of asset loss, and (iv) have never thinked about crypto inheritance. These users represent the primary segment for which AICA addresses a concrete, immediate, and currently unmet need.

Let n denote the total number of wallet owners and k the number of respondents matching the target profile. In our dataset, $n = 31$ and $k = 13$, corresponding to a proportion of 41.9%.

A binomial test was performed to evaluate whether this proportion is significantly higher than a conservative baseline of $p_0 = 0.25$.

- Null hypothesis (H_0) : $p(\text{target profile}) = 0.25$
- Alternative hypothesis (H_1): $p(\text{target profile}) > 0.25$
- Significance level: $\alpha = 0.05$
- Test result: $X = 13$ successes out of $n = 31$
- Exact p-value: $p = 0.029$ (significant)

Interpretation: Since $p < 0.05$, we reject H_0 and conclude that the proportion of users belonging to the AICA target profile is significantly higher than 25%. More than four out of ten wallet owners fall into this category, indicating a situation where users are aware of risks and follow secure practices, yet lack inheritance planning. This provides strong empirical evidence that AICA addresses a substantial and non-negligible unmet need.

Table 7: Binomial Test Summary on the AICA Target Profile

Parameter	**Value**
Target profile size (n)	13
% among wallet owners	41.9%
Binomial test vs $p_0 = 0.25$	$p = 0.029$ (significant)

Source: created by the authors

Overall, these statistical analyses improve our understanding of user behaviour with regard to the secure management of digital assets, highlighting the need to develop reliable transfer mechanisms in the context of DLT technologies.

This research is based on empirical exploration. This survey was created to provide preliminary data on how users see value in our platform and to determine what the long-term adoption of this platform will look like. The sample size of 42 was not meant to allow multivariate inferences to be completed, however, what we have seen is a strong directional consistency across groups and statistically significant results in three key measures that support the assertions we make.

The most impactful evaluation is still to come. In order to do this accurately we will have to acquire real oracle verified death events along with documented latencies for asset transfers on the Hedera mainnet, and jurisdiction specific probate timelines for each jurisdiction. This will be our primary quantifiable goal in our post-deployment research agenda.The two areas we have identified for additional geographic coverage will be Southeast Asia and the Gulf region, as Islamic inheritance frameworks align well with our design and also provide an avenue to align the gap between the preferences declared in our survey and the actual expectations of the target users.

8 Conclusion and Perspectives

The increasing use of cryptocurrencies emphasises the need to reconsider the methods of transferring digital assets upon death. The decentralised nature of crypto-assets makes them complex to manage, so, innovative and adaptable solutions are needed to ensure they can be securely transmitted to heirs. Our contribution follows this approach by proposing an automated architecture that addresses the current and future challenges of crypto-asset inheritance. The proposed architecture can be parametrized to respect the legal and regulatory specifics of different countries. It can be adapted to jurisdictions where cryptocurrencies are restricted or prohibited by enabling conversion mechanisms that facilitate the exchange and transfer of crypto-assets to beneficiaries in compliant forms, including fiat currency. This ensures that all stakeholders, including heirs without cryptocurrency wallets, can receive the inherited value. Future work will include further development of the architecture, as well as applying it to real-world cases to validate its effectiveness and performance further. Additionally, agentic AI could be used to confirm the status of heirs, ensuring that only eligible, living beneficiaries receive the inheritance, even in exceptional or pathological cases.

References:

[1] Ivan Sergio and Jan Wedemeier (2025). Global surge: exploring cryptocurrency adoption with evidence from spatial models. *Financial Innovation*, vol. 11, Issue 1, art. no. 96. DOI: https://doi.org/10.1186/s40854-025-00765-0

[2] Pratama, Dody & Saipudin (2025). Study of Digital Asset Inheritance: A Review of Contemporary Islamic Law in Indonesia. *Istinbath: Jurnal Hukum*, vol. 22, Issue 2, pp. 286-308. https://e-journal.metrouniv.ac.id/istinbath/article/view/11224/4829 [Access Date: 18/05/2026]

[3] Chavali, D. P., Reddy, N. S., Taran, S., & Chandana, S.(2024). Decentralized Intestacy Distribution: Exploring Autonomous Systems Leveraging Blockchain Technology. *International Journal of Scientific Research in Engineering and Management*, vol. 8, Issue 4, pp. 1-5. https://www.researchgate.net/profile/Durga-Chavali/publication/380065517 [Access Date: 18/05/2026]

[4] Korok Ray, Sindura Saraswathi, (2025). Optimal Threshold Signatures in Bitcoin. *arXiv preprint arXiv:2509.25408.* https://doi.org/10.48550/arXiv.2509.25408

[5] A. Wahab, M. Katuk, M. A. Hussain, Z. Zainol, S. Maamor, and N. S. Kamis (2024). A Proposed Framework of Islamic Inheritance and Estate Planning of Digital Assets: The Malaysian Case of Crypto Assets. *ISRA International Journal of Islamic Finance*, vol. 16, Issue. 2, pp. 45–64. DOI: https://doi.org/10.55188/ijif.v16i2.713

[6] Erika Nur Syarifah, DaulayAkhmad Budi Cahyono (2025). Legal Protection for Heirs with Non-Fungible Token Heritage Objects. *Journal of Law Politic and Humanities*, vol. 5, Issue. 3, pp. 2216-2227. DOI: https://doi.org/10.38035/jlph.v5i3.1198

[7] Prost, Frédéric (2022). On the Heritage of Crypto Assets–Tales From the Crypt Protocol. *arXiv preprint arXiv:2209.11194.* https://doi.org/10.48550/arXiv.2209.11194

[8] Dalton Cézane Gomes Valadares, Angelo Perkusich, Aldenor Falcão Martins, Mohammed B. Alshawki and Chris Seline (2023). Privacy-Preserving Blockchain Technologies. *Sensors*, vol. 23, Issue. 16, art. no. 7172. DOI: https://doi.org/10.3390/s23167172

[9] Cristina Carata, Ana-Luisa Chelaru (2024). The Evolution Of The Digital Inheritance: Legal, Technical, And Practical Dimensions Of Cryptocurrency Transfer Through Succession In French-Inspired Legal Systems. *arXiv preprint arXiv:2410.2290.* https://doi.org/10.48550/arXiv.2410.22907

[10] J. Goldston, T. J. Cheffer, J. Osowska, and C. von Gois II (2023). Digital Inheritance in Web 3: A Case Study of Soulbound Tokens and the Social Recovery Pallet within the Polkadot and Kusama Ecosystems. preprint arXiv:2301.11074. https://doi.org/10.48550/arXiv.2301.11074

[11] R. Govind Singh, A. Shrivastava, and S. Ruj (2022). A Digital Asset Inheritance Model to Convey Online Persona Posthumously. *International Journal of Information Security*, vol. 21, Issue. 5, pp. 983-1003. DOI: https://doi.org/10.1007/s10207-022-00593-8

[12] A. Ali, M. A. Mohamad Salleh, and N. Mustaffa (2022). Digital Inheritance Exploration (DIE) Through Digital Inheritance Model (DIM) - A Guideline for Digital Assets Planning After Death. *In APS proceedings. Academica Press*

Solution. https://www.researchgate.net/publication/365315619 [Access Date: 22/04/2026]

[13] S. Ridhorkar, V. Zade, V. Mathane, A. Prince, A. Dhobale, and M. Kamdi (2024). NextHeirs: Blockchain Based Inheritance Management System Using Quantum Resistant, *International Journal of Computer Engineering and Technology*, vol. 15, Issue. 2, pp. 94-103. https://iaeme.com/Home/article_id/IJCET_15_02_012 [Access Date: 22/04/2026]

[14] Prost, Frederic (2022). Inheritance and Blockchain: Thoughts and Open Questions. *ArXiv abs/2212.01194* https://doi.org/10.48550/arXiv.2212.01194

[15] J. Hernando-Corrochano, R. Pastor-Vargas, and R. Hernández-Berlinches (2025). Trusted Wills for Digital Assets Using Blockchain: A Practical Case. *Blockchain: Research and Applications*, vol. 6, Issue. 3, art. no. 100289. DOI: https://doi.org/10.1016/j.bcra.2025.100289

[16] S. B. Anuar, F. A. Md Azmi, and S. N. S. Sidek (2022). Exploring the Potential and Suggesting a New Conceptual Framework of Blockchain Technology in Estate Distribution. *International Journal of Advanced Research in Technology and Innovation*, Vol. 4, Issue. 1, pp. 35-43. https://scholar.archive.org/work/h5hv6qgm3zf5xhdecjzcwl66j4/access/wayback/https://myjms.mohe.gov.my/index.php/ijarti/article/download/17427/9144/ [Access Date: 25/05/2026]

[17] Dirk A Zetzsche, Douglas W Arner, Ross P Buckley (2020). Decentralized Finance. *Journal of Financial Regulation*, Vol. 6, Issue. 2, pp. 172–203. https://academic.oup.com/jfr/article/6/2/172/5913239 [Access Date: 31/05/2026]

[18] Farida Eleshin, Qi Sun, Mengzhe Ye, Sauvik Das, Jason I. Hong. Of Secrets and Seedphrases: Conceptual Misunderstandings and Security Challenges for Seed Phrase Management among Cryptocurrency Users. *in Proceedings of the CHI Conference on Human Factors in Computing Systems*, Yokohama, Japan, 2025, pp. 1–19. DOI: https://doi.org/10.1145/3706598.3713209

[19] R. Aboulaich and M. Tkiouat. Applications of Agent-Based Simulation in Islamic Finance. ISBN: 978-603-8306-29-1, *Islamic Development Bank Institute (IsDBI)*, 2024. https://doi.org/10.55780/Bk24002

[20] Wilson, Rodney (2019). Implications of technological advance for financial intermediation in Islamic finance. *Fintech in Islamic Finance. Routledge*, pp. 33-44. DOI: https://doi.org/10.4324/9781351025584-3

[21] Law, Siong Hook, and Masagus M. Ridhwan (2022). Effect of Islamic financial system stability on economic performance in Indonesia. *Journal of Islamic Monetary Economics and Finance*, vol. 8, Issue.3, pp. 371-406. DOI: https://doi.org/10.21098/jimf.v8i3.1567

[22] Imran Yousaf, Afsheen Abrar, Larisa Yarovaya (2023). Decentralized and centralized exchanges: Which digital tokens pose a greater contagion risk?. *Journal of International Financial Markets, Institutions and Money*, vol 89, art. no. 101881. DOI: https://doi.org/10.1016/j.intfin.2023.101881

[23] Maureen Keisha Yolanda, Chintya Lie Paramitha Moody Rizqy Syailendra Putra (2025). Exploring Digital Assets Inheritance: A Comparative Study of Transnational Legal Frameworks and Practices. *Journal Penelitian dan Pengabdian Masyarakat Indonesia*, vol. 4, Issue. 1, pp. 942-951. DOI: https://doi.org/10.57235/aurelia.v4i1.4483

[24] K. Bajaj, S. Gochhait, S. Pandit, T. Dalwai, and M. S. M. Justin (2022). Risks and Regulation of Cryptocurrency During Pandemic: A Systematic Literature Review. *Wseas Transactions on Environment and Development*, vol. 18, pp. 642-652. DOI: https://doi.org/10.37394/232015.2022.18.61

[25] F. Z. Meskini and R. Aboulaich (2024). Insurance Based on Waqf and Blockchain Technology: A Strong Social Impact & Efficiency. *WSEAS Transactions on Business and Economics*, vol. 21, pp. 741-752. https://www.wseas.com/journals/bae/2024/b265107-2568.pdf [Access Date: 25/05/2026]

[26] Z. Ihrouchen and O. Souissi. A Smart Logistics Architecture Using IoT and Hashgraph. *5th International Conference on Innovative Research in Applied Science, Engineering and Technology* ,Fez 2025, pp. 1-6, IEEE. DOI: https://doi.org/10.1109/IRASET64571.2025.11008100

[27] L. Baird (2016). The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. *Swirlds Tech Reports*, vol. 34, p. 9-11. https://www.hashgraph.com/wp-content/uploads/2024/09/SWIRLDS-TR-2016-01.pdf [Access Date: 22/04/2026]

[28] A. Pokharel and K. Dahal (2022). Crypto Inheritance Planning for HODLers: Methods to Safely Transfer Digital Assets to Beneficiaries. Available at SSRN 4183803: http://dx.doi.org/10.2139/ssrn.4183803

Survey Questions

1. Full/Fake Name 2. Age group
3. Region 4. Country 5. Profession
6. Do you have a cryptocurrency wallet?
7. Do you hold any digital assets?
8. Familiarity with DLT
9. Ever shared private keys (wallet holders)?
10. Comfortable sharing with family?
11. Main reason to keep wallet secret?
12. Most holders keep wallets secret?
13. Thought about crypto inheritance?
14. Could assets be lost without plan?
15. Importance of inheritance?
16. Interested in automated inheritance?
17. Can smart contracts improve security?
18. Prefer automated system or manual sharing?
19. Likely to adopt solution today?
20. Trust decentralized platform?
21. Regulatory environment description
22. Do regulations encourage innovation?

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)
The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself
No funding was received for conducting this study.

Conflict of Interest
The authors have no conflicts of interest to declare that are relevant to the content of this article.

Appendix

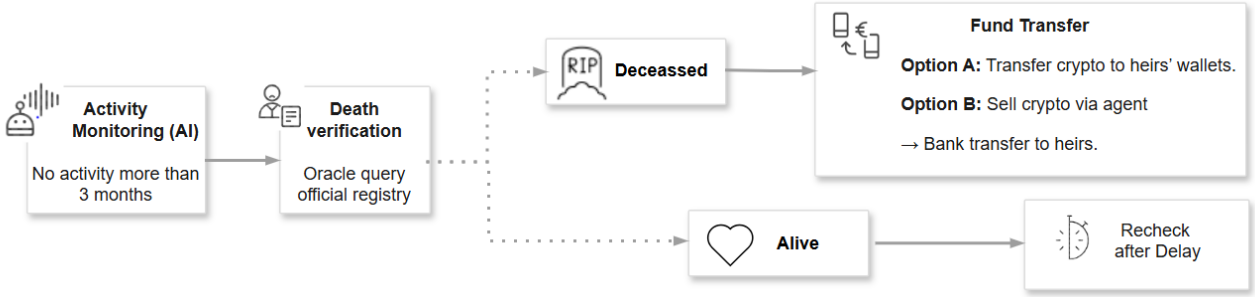

Fig. A1: Overview of the proposed crypto inheritance system AICA
Source: created by the authors