IAME

An Expert System for Blockchain Identity Verification

Nathaniel Tsang Mang Kin
Suryani Chang

www.iame.io

Abstract

A decentralized identification system that would allow parties performing blockchain transactions to verify, on a primary level, the identity of each other without having to disclose non-essential sensitive personal information to the counterparties; and on a secondary level the source of the Cryptocurrencies in the transaction. Identification would be conducted by a multitude of independent third party validators, each verifying fragments of information that together would constitute a complete verification, such that only the original owner of the sensitive personal information retains her/his data in a wholesome and useful way. The result of the identification process would be hashed onto a designated blockchain and made accessible on a public repository such that the identification status and source of the cryptocurrencies associated with specific blockchain addresses can be consulted, without compromising the unique identification data.

Contents

1. Introduction

Current identification systems rely on people having to share their personal information and supporting evidence with counterparties in order to identify themselves and their source of wealth. Those counterparties hold the shared data wholly, and the more data a person shares with those counterparties, the easier it is to identify the person and their source of wealth. If a person is to transact with n counterparties, it results into a topological star network with n nodes, each acting as point of vulnerability to the data sharer. Regardless of security measures, the more data a person surrenders, the more severe the fallout from any potential security breach.

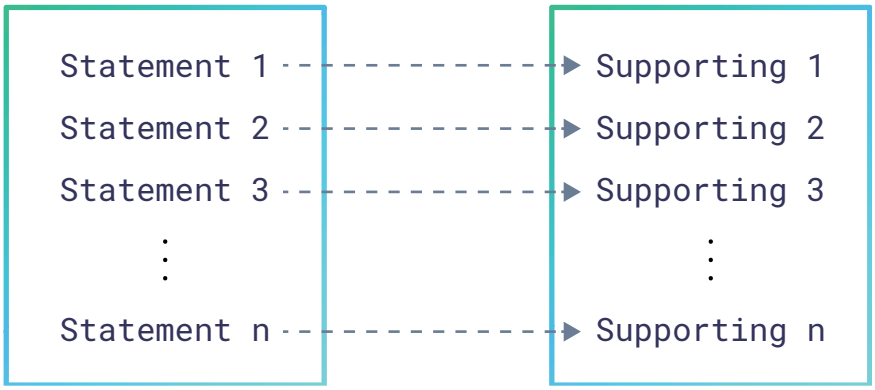
All too often the counterparties/nodes do share the data partially or wholly with third parties, which in turn extends the initial star network, hence increasing the number of points of vulnerability in the former network. Technological innovation in encryption mostly work with regards to securing the transmission of data between two or more nodes in a network, however they do not address the issue of an increase in the number of nodes in a sensible data network. As the number of electronic transactions a person conducts increases in frequency, the number of nodes in their personal data network subsequently increases exponentially, consequently increasing the number of points of vulnerability.

The solution we are proposing is to change the way the identification process is conducted to the point that a person's data is fragmented prior to confirmation by a series of independent third parties, who are not affiliated to any parties within the transaction. The third parties would be assigned the task of confirming fractured pieces of personal data, which by themselves are useless to malicious parties, however, the sum of which would constitute a valid identification to the transactional counterparty. As a result of this, this would bypass the need for any transactional counterparty from having to process or store non-essential data.

The above process would take place on the IAME Identification Network, a purpose-built system to service the fragmented identification process,fueled by the IAM cryptographic token. Functionality of the IAME Identification Network would principally serve Blockchain P2P transactions, however, usage would be extensible to merchant transactions and financial institutions in the provision of blockchain related services.

2. Deconstructing the Identification Process

The conventional identification process starts with a party acceding to a request by a counterparty to identify itself so that that the counterparty may ascertain to a level with whom it is transacting. The party submits a statement filled with data that the counterparty has deemed to be necessary and the corresponding supporting evidence. After mapping the data to the supporting evidence, a decision is reached on whether identification of the party can be ascertained



The process assumes that: if the party is genuine then all provided statements can be mapped onto supporting documentation. In principle, the more data that can be mapped on more supporting documents, the more difficult it is for a party to falsify its identity.

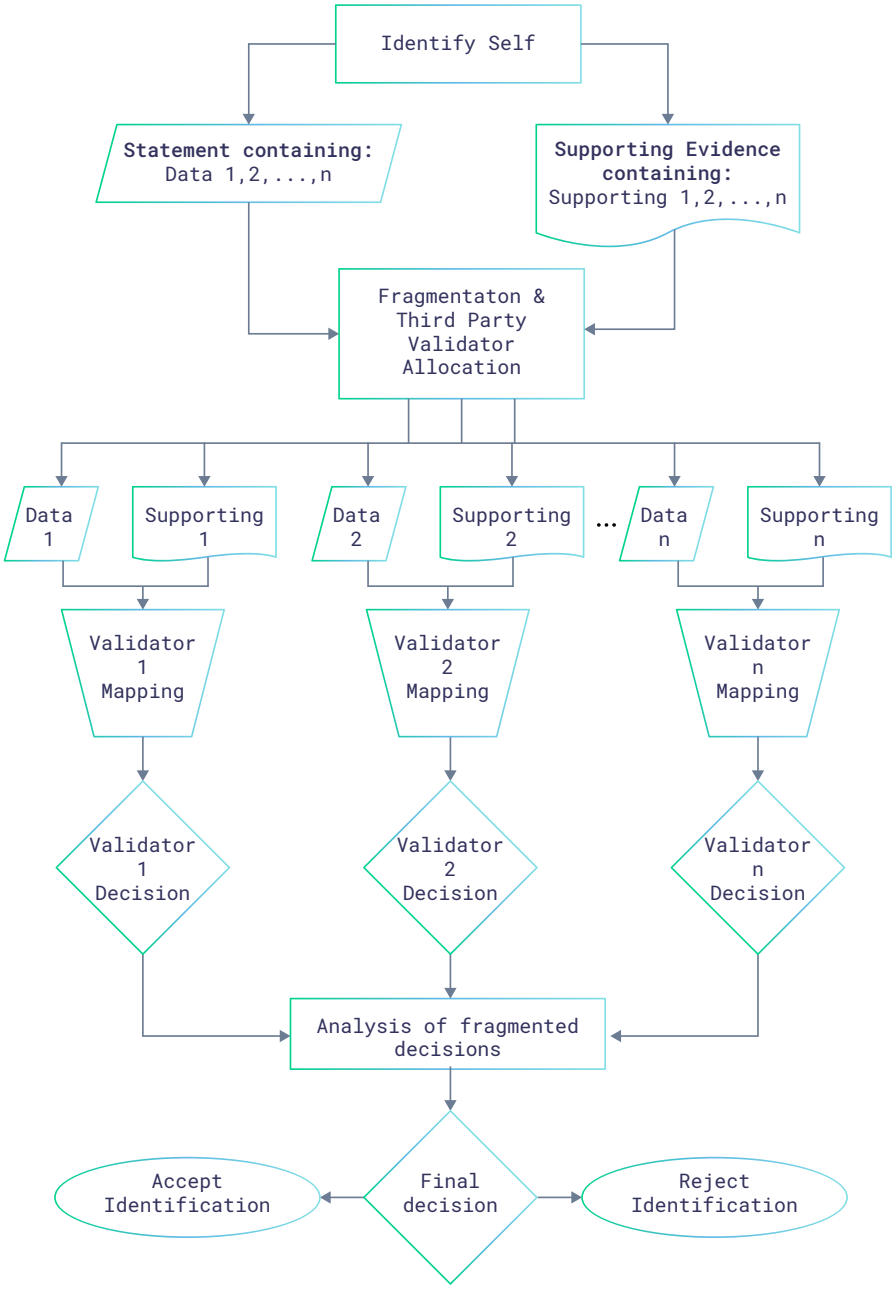
The mapping process itself is quite simplistic and can be categorized as follows:

1. Statement to string confirmation
2. Statement to non-string confirmation
3. Statement to publicly available information confirmation
4. Statement to privately available information confirmation
5. Statement to government records confirmation.

Any identification process that can gather a maximum of the above mapping data is ideal for counterparties to guarantee that they are dealing with a genuine person, however, it can be disastrous for the sharing-party in the event of a security breach.

3. Fragmenting the Identification Process

Building on the previous identification process, the same mapping functions can be achieved without the party disclosing any non-relevant data to a counterparty - by delegating the mapping functions to unrelated third-party Validators. The statement, supporting evidence and functions, would first have to be fragmented in such a way that third-party validators would be confirming fragments of data that, on their own, cannot be used by any malicious third party. However, together, the sum of confirmations would constitute a complete identification process.



Considering a simple scenario whereby a counterparty requires confirmation of 3 string type statements with an identification document as supporting evidence:

1. First Name: "John"
2. Last Name: "Doe"
3. Country: "Mauritius"

From the above information, a simplistic fragmentation can be derived by sending the 3 string type statements to be confirmed with the corresponding section of the identification document string to 3 different third-party validators who would each confirm the content of the string. The summation of their independent validations
would hence be used as the equivalent of the counterparty itself validating the 3 string type statements by itself. Contrasted with a traditional identification process, in the fragmented identification process, the usefulness of the data is exponentially decreasing with the increase in fragmentation.

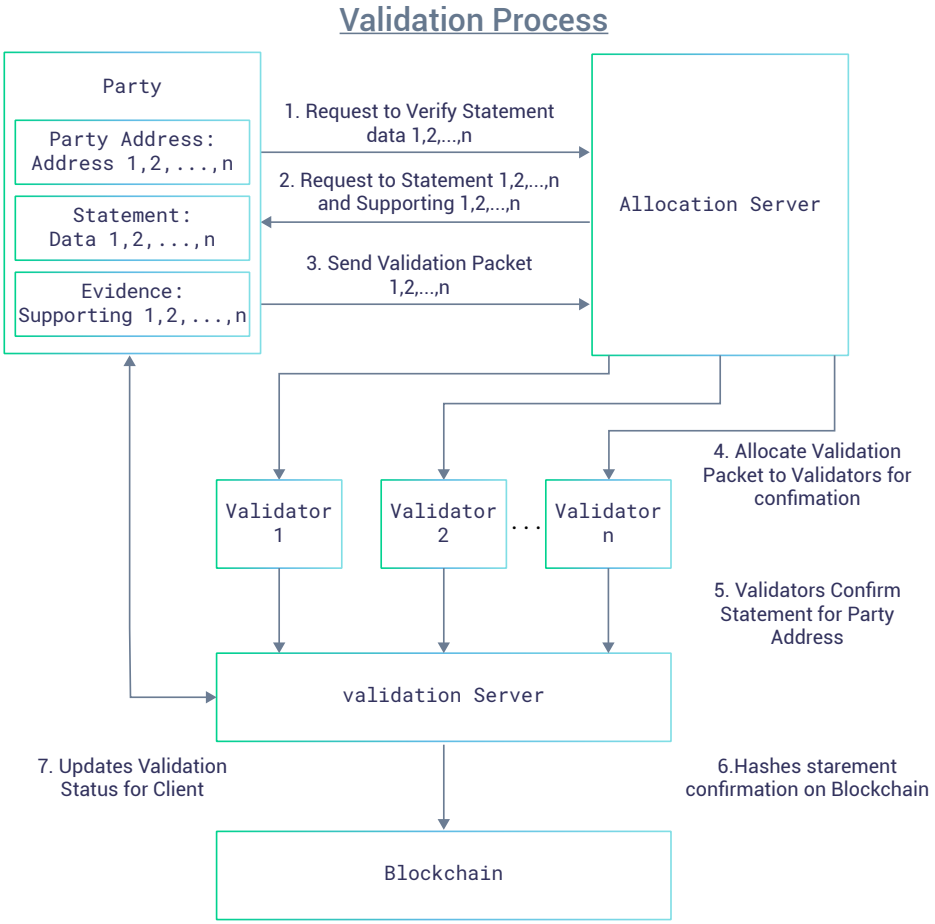
Drawing on on the fragmented identification principle, statements can be further fragmented to transform any useful string type statement into unintelligible data:

1. String Type Statement: John
2. Fragment A: "Jo"
3. Fragment B: "hn"
4. Fragment C: "oh"

Using the above process, we have rendered the string type statement, "John", useless to potential malicious third-party validators.

4. The IAME Identification Network

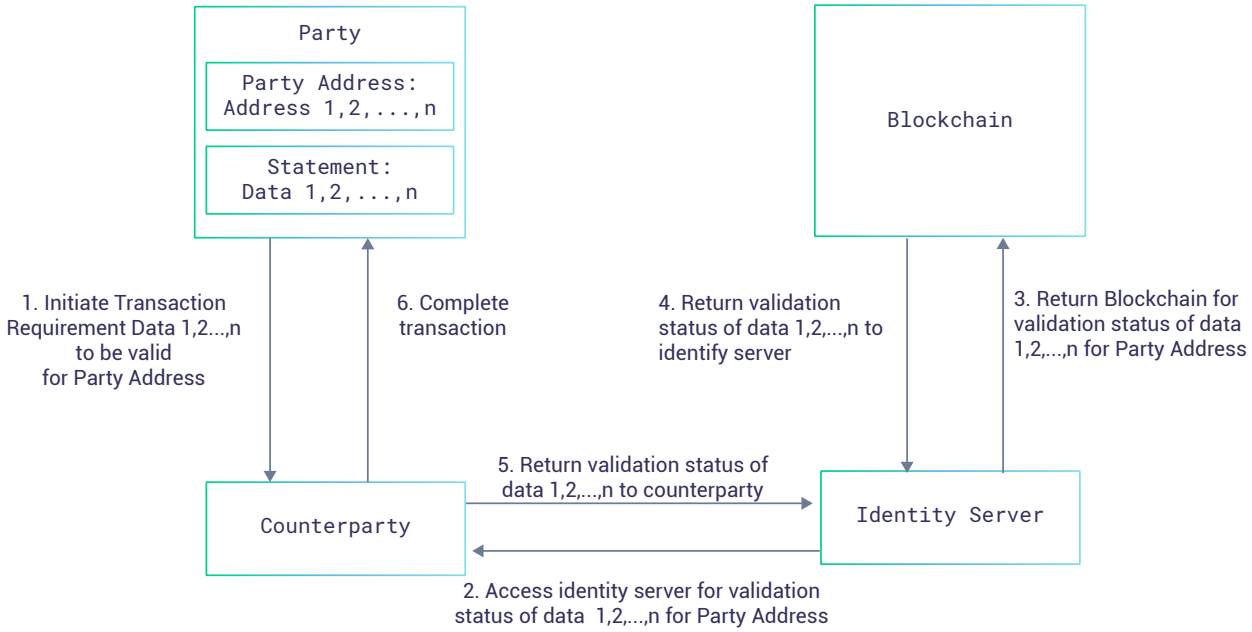
The proposed IAME Identification Network would have a core that consists of 1) a client, 2) an allocation server, 3) a validation server, 4) a writeable blockchain, and 5) an identity server. Each component would carry out specific functions that can be demonstrated in 2 processes - a validation process, and an identification process.



The validation process would be the operation through which the client would have her/his information validated by third-party validators. The process is as shown below:

1. Upon request, statements and their corresponding supporting information would be fragmented at the client level and encrypted into validation packets to be sent to the allocation server.
2. The allocation server would control the random allocation of validation packets to third-party validators, who would return the result of their validations to the validation server.
3. Once the above is completed, the validation server would evaluate the validations from the third-party validators, and hash numeric or boolean confirmations paired to specific statements on a designated writeable blockchain.

Identification Process



For a counterparty to transact with a client, an identification process has to be completed. This process is based on the counterparty's own specific requirements.

1. Assuming that the counterparty requires Data 1,2,.. n to be validated for a specific transaction with a party, the counterparty sends a request to the Identity Server for the validation status of Data 1,2,.. n.
2. The Identity Server reads the blockchain for validation status of Data 1,2,..n for the party, and returns the validation data to the counterparty, and from thereon the counterparty can complete the transaction.

As per the previous diagram, a party can self-identify her/his statements for transactional counterparties, while the wholesomeness of sensitive data is retained solely by the owner of the data, rendering acquisition of sensitive data by malicious third-party validators pointless.

While the IAME Identification Network would not be a bypass for data sharing between transactional counterparties, it would serve to segregate the distribution and validation of non-essential sensitive personal information.

5. The IAM Token

To operate the IAME Identification Network, a functional token will be issued, known as the IAM Token, which would operate as a validation token to initiate confirmation requests for validation packets on the IAME Identification Network. Parties would spend the token through the IAME Identification Network client and after deduction of equivalent blockchain hashing costs, the balance of IAM token would be paid out as reward to third-party validators who operate the validation processes on a for-profit basis.

This would attribute not a store of value to the token but a market value based on natural demand and supply for identification processes. The value of the IAM Token would be, in essence, determined by 2 factors:

1. The cost of validation, which would be proportional to the financial cost of hashing the requested amount of data on the designated blockchain, setting a price floor for the token
2. Market demand, which would be proportional to the demand for blockchain identification based on the IAME Identification Network

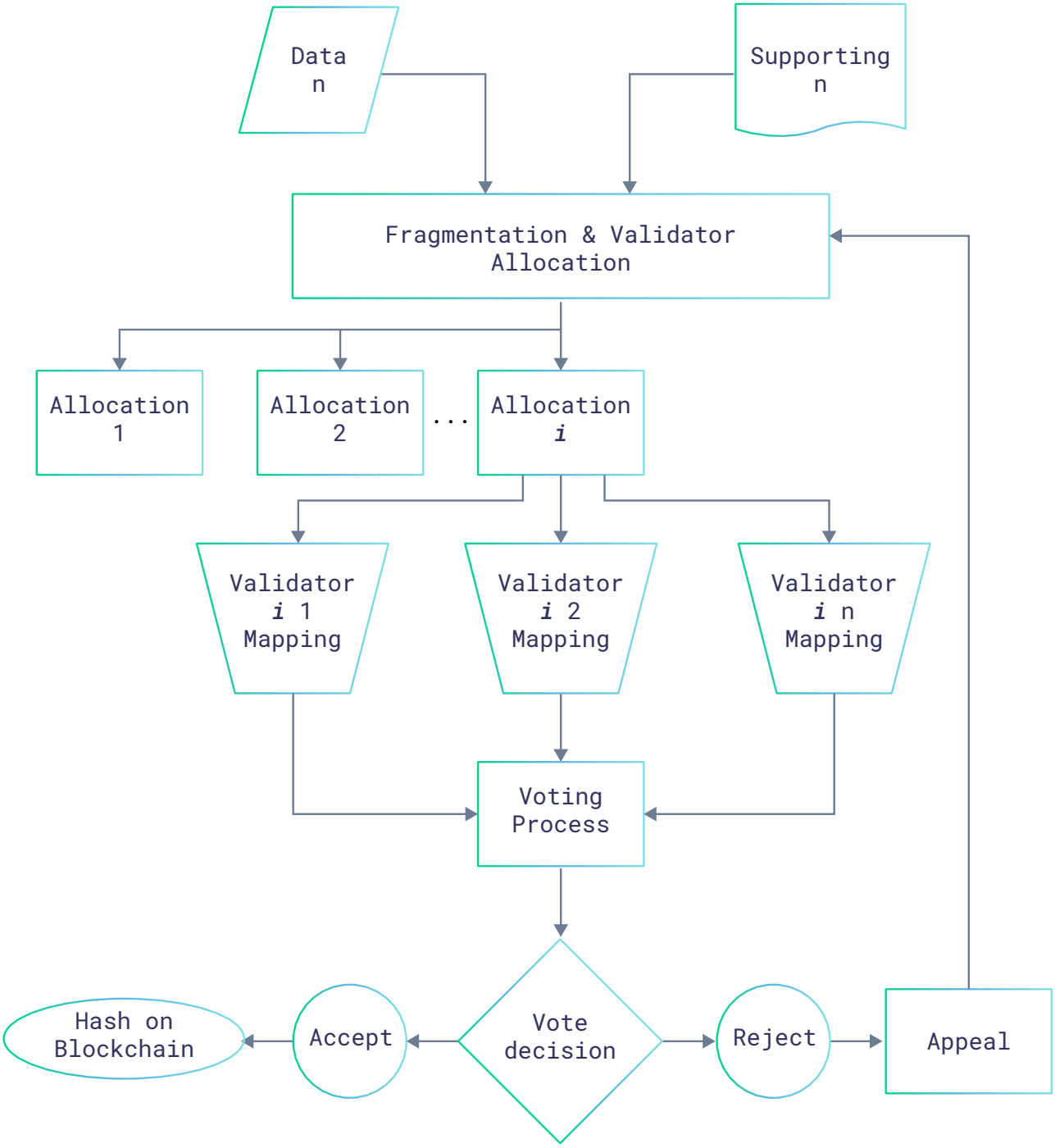
Because of the the ephemeral aspect of data validation in the field of identification, market demand would remain recurring and would only increase with an increased adoption of the IAME Identification Network.

6. Third Party Validation

Pursuant to the concept of the IAME fragmented identification system, there is a requirement for a system of decentralised third-party validators under the rational that an identification validation conducted by a multitude of third-party validators is more dependable and less susceptible to the risk of fraud than an identification validation conducted by a single institution or party. However, having a system that runs on a for-profit basis, where the third party is "paid" to validate information, creates a natural tendency for participants to game the system and collectively approve a validation process to receive a payout. The solution we propose is a symmetric game model that will encourage truthful validation that is analogous to the Byzantine Fault Tolerance - the Trial Algorithm.

Aspects of the Trial Algorithm:

1. Each statement and their corresponding supporting information are processed as fragments ("Evidence");
2. Evidence is validated not by single third-party validators ("Jury"), but by a Jury (a "Tribunal");
3. Each jury validates in a designated method on whether the Evidence matches the statements
4. The Tribunal validations are counted and a majority rule consensus is reached
5. If there is a non-majority consensus on an evidence, the evidence is sent through a second tribunal ("Appeal")
6. If the appeal jury votes to a majority consensus identical to the initial tribunal,the decision is upheld, or else the initial tribunal decision is rejected



The purpose of the trial algorithm is to support truthful validation and, most importantly, genuine dissent in the event a significant portion of the third-party validators are corrupted in their validation mechanism. In the proposed technical implementation, it is intended that the third-party validators are blindly assigned tribunals, appeals, and control tribunals("Control Tribunal"). Control tribunals are an allocation of non-matching statements to evidence, and to third-party validators, such that the third-party validators are randomly subjected to double blind procedures.

7. Reward and Ranking Mechanism

As a continuation to the Trial Algorithm, there is a need for a reward and a ranking mechanism in such a way that good third-party validators are rewarded and bad third-party validators penalized. **For this mechanism, two reward systems are proposed: a token reward system and a node ranking system.**

1. The token reward system allocates a pool of IAM Tokens to the third-party validators for completing the fragmented validation process akin to mining
2. The ranking system attributes an internal ranking system to third-party validators within the IAME Identification Network, such that higher ranked validators receive a higher proportion of the tokens, which is indicative of their ranks..

In principle, the determination of the allocation of any IAM token pool would be a function of the outcome of the Tribunal, while the ranking system would be a function of the outcomes of the Appeal and the Control Tribunal. Due to the application of a double blind procedure, the third-party validators would not be at any time aware of whether they are in a Tribunal, an Appeal, or a Control Tribunal - further reducing any risk of gaming the system. Third-party validation would be open to the public and, in the long-run, poorly ranked third-party validators would be banned from acting as nodes.

8. An Identification System for Blockchain P2P Transaction

With a functional IAME Identification Network, the primary application would be the facilitation of blockchain P2P transaction, such as online merchant transactions. Taking into consideration a simple online purchase where a customer purchases a physical good from an online merchant with Cryptocurrencies, the amount of personal data that is communicated from the customer to the merchant can be segregated into two categories: essential to the transaction and non-essential to the transaction.

1. Essential information would be a name and an address without which the transaction and the delivery of the good cannot occur
2. Non-essential information would include, for example, an identity document to prove the name of the customer, a utility bill to prove that the address belongs to the customer, and the specific date of birth of the customer

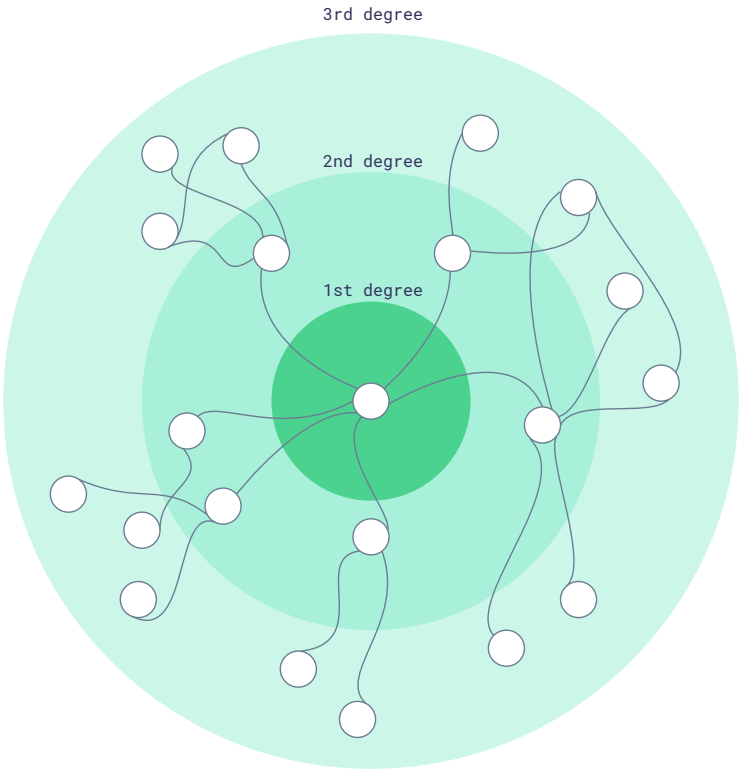
The logic behind the conveyance of non-essential information is based out of regulatory need. But with an alternative identification system, the same goal can be achieved without disseminating the non-essential information, decreasing security risks for the customer and decreasing the burden of security breaches for the merchant.

In the P2P scenario, the merchant would consult the public repository of the IAME Identification network to verify whether non-essential information associated with the customer's blockchain address has been undertaken on the identification network. This could be either out of a regulatory basis or for her/his own comfort level.

9. A Platform for Financial Institutions

As the regulatory classification of Cryptocurrencies converges towards currencies, securities, and/or software, there will be a need for some form of anti-money laundering procedures to be applied, which can trace the source of the Cryptocurrencies - up to a level that can ascertain that they are not from the proceeds of criminal activities. The use of public ledgers, though being able to create an electronic trail up to the mining/creation of Cryptocurrencies, does not identify the transitory wallets through which the Cryptocurrencies have been.

As an extension of the IAME Network and its public repository, the identification system would be used in the construction of identified topological spaces that would provide financial institutions with the tools to identify, to the nth degree, the origin of the Cryptocurrencies they are handling.



The creation of a partially meshed system would provide financial institutions handling Cryptocurrencies a level of comfort, to the nth level, on the source of Cryptocurrencies, which would still constitute a more efficient anti-money laundering tool than current procedures for Cryptocurrencies.

10. Conclusion

The biggest source of security risk to persons identifying themselves is through the sharing their personal data with counterparties. Encryption and conventional security measures can work only to the extent that counterparties that handle the information are secure. However, in an economy where the number of electronic transactions a person conducts is constantly increasing, the number of points of potential vulnerabilities increase exponentially, decreasing any advantage gained from security innovations.

Using the proposed IAME Identification Network laid out in this white paper, we seek to resolve the problem parties face in blockchain transactions by having to identify themselves with a multitude of counterparties, while both preserving the anonymity of the transacting party, and satisfying the need for counterparties to conduct a certain level due diligence on clients.

There is both a practical imperative and commercial need for a non-invasive identification system for decentralised blockchain technology and we believe that the IAME Identification Network will be the bridge that will link blockchain technology to the regulated world.