GlobalVille Web of Trust

A Decentralized Identity, Reputation & Communication Network

Abstract

We present a distributed ledger application which provides the ability to create unique digital identities based on the web of trust principle as well as principles of game theory. The main goal of the application is to address the Proof of Individuality problem by ensuring that individuals can create only one verified digital identity and that each verified identity belongs to a real individual. The identities are community issued and decentralized so that no central entity is in charge of issuing or revoking identities. Once unique digital identities are established it provides a foundation for additional features such as authentication, reputation, direct communication and distribution of unconditional basic income. Many other organizations will be able to make use of this public infrastructure to enhance their own services.

1. Motivation

Identity is the foundation of a civilized society. Without identity, one cannot establish property rights. Without property rights, one cannot participate in markets and commerce. The root source of identity for individuals is currently provided by government organizations. If an individual does not have an identity with any government then there is no source of identity for this individual. As a result over 2.4 billion people in the world do not have an identity [1]. These people are not able to properly participate even in their local economies and are usually left unbanked and unable to own physical property such as land. Proving that you are a unique individual on this planet should not require any government involvement. The world needs a permissionless, decentralized, global identity system based on community issued identities.

Most government issued identities are only useful in the physical world and can only be verified by privileged organizations that have access to the central identity database. They are not suitable for transferring over the Internet and cannot be used by individuals to verify each other's identity. Yet the world is becoming more globalized and individuals from different countries are interacting with one another over the Internet. It would be ideal to have an identity system which is accessible to all individuals and can be used to verify one another not only in the physical world but also over the Internet.

Governments, out of a need for patrolling their borders and providing benefits to their citizens have had to implement their own identity systems. However, this has put individuals in a situation where they are dependent on governments to provide the root source of identity. This necessity has also burdened governments with an ongoing additional expense to implement, maintain and secure these identity systems. Since each government has its own identity system, this has created walled gardens of incompatible identity. If an individual moves from one country to another, they must re-establish their identity under the government of the new country. This not only burdens the individual, but also the government. Ideally governments should not be providers of identity, but rather consumers of an identity system that spans not only their borders, but the globe.

Such a global identity issuing system should not be under the control of a centralized corporation, a government agency or even an international organization. It needs to be a decentralized system with no single point of control and permissionless access.

2. Overview

When we enter a public place in the real world, we are able to see faces, but do not know additional information about a person unless that person chooses to disclose it. We can always communicate with the person to exchange more information. GlobalVille tries to preserve these features in the digital world. GlobalVille is based on the notion of a global village where everyone can see each other's face and communicate directly with each other.

Users can install the GlobalVille app on a mobile device and use it to send transactions to the GlobalVille distributed ledger; also referred to as the GlobalVille network. Through this app users can get registered to establish a unique verified account. The verification step requires endorsements from friends and relatives who are already registered. Once verified the user begins receiving daily stipends of the GETCoin crypto token. The user will also be able to search and browse other users, send GETCoin to other users, and send direct messages to other users. The app can also be used to prove one's identity to any requesting party, website or mobile app.

3. Identity

To be useful for a broad number of applications a system that provides the root source of identity must prevent the creation of fake accounts and duplicate accounts. To prevent fake accounts the system needs to ensure that each individual associated with an account really does exist. To prevent duplicate accounts the system must ensure that one individual is not able to create multiple accounts.

To ensure that the individual really does exist, other individuals who are already part of the system must attest to the joining individual's existence. To ensure that an individual has created only one identity in the system, the joining individual must attest to creating only one account to other individuals who are already part of the system. In addition, facial images of the joining individual are linked to the account and can be compared against the images of all other accounts to find possible duplicate accounts. Facial images are chosen over other biometric data because faces are a biometric feature that is already exposed publicly, can be acquired easily without contact, and are biometric identifiers that can easily be processed by humans.

Monetary disincentives are also used to discourage fraudulent accounts. If an account is proven to be fake or duplicate then the individuals involved with the creation of the account must pay a fine to continue using their own account. If an individual does not pay the fine then the status of the account will be marked as delinquent and other services which use the identity system to provide benefits to the individual will not be able to function. Monetary incentives are used to encourage finding and reporting fake or duplicate accounts as described later.

Account Creation

At the core of the identity system each participating individual has ownership of a unique digital identifier. This ownership is provable using a digital signature. In its simplest form an account consists of a globally unique id (GUID) and an associated public key. The individual retains possession of the private key and can use it to prove ownership of the account linked to the GUID. A digitally signed transaction that contains the GUID and is verifiable using the associated public key initially creates the account, unless it already exists. The GUID determines the account address and the public key is stored as a field in the account record. However the GUID could also be created and assigned by the distributed ledger application to ensure uniform distribution of the ids across the address space. Many more fields can be added to this account record as the user builds the credibility of the account. A person can create any number of accounts. However, such accounts will be pseudo-anonymous and not linked to any person. Only when biometric data is added to an account and endorsed by others does the account become verified and linked to an individual. The key pair used to control the account can be changed in the future while the address of the account will always be the GUID. The fee for submitting account creation and key change transactions is paid using a proof-of-work.

All accounts verified or not can have a username linked to the account. This makes it easier for users to enter the username instead of an account address.

Account Verification

To create a verified account, facial images of the individual must be added to an account in order to link the account to a specific individual in the real world. After the images are added the account

may be endorsed by other users who already have a verified account. The endorsement attests to the fact that the images match a real person who is well known to the endorser, that the endorsee has testified to the endorser that another verified account has not and will not be created, and that the endorsee is aware that both the endorsee and endorser will be fined if the endorsee creates another verified account. The endorsement must include an image of the endorser with the endorsee. An account must have at least 3 endorsements to become a verified account. An account is limited to receiving no more than 4 endorsements. Once verified the account will be able to give up to 6 endorsements. The endorsements are irrevocable so they cannot be retracted and given to someone else. Once an endorsement has been given, it is used up.

Accounts of minor individuals below some age limit like 18 are verified by having two adult verified accounts endorse them as dependents. The adult supporters are not using up their 6 endorsements by supporting a minor. A verified adult has up to 10 supporter endorsements that can be given out irrevocably. Accounts of minor individuals will not receive the 6 endorsements that can be given out; nor can they become supporters for other minor accounts. Once a minor individual reaches the age limit mentioned earlier the account can receive 3 peer endorsements to become a verified adult account capable of endorsing others. The age limit is a parameter that can be voted on and changed in the future. The number of endorsements available to give out can also be changed in the future by voting amongst the verified adult accounts. All fees for verification transactions are paid with a proof-of-work.

Seed Party

When the network initially starts the first 400 accounts created do not need any endorsements for the account to be active. A seed party event is held where 100 groups of 4 individuals each come together to create the initial accounts. The 4 individuals in each group should know one another and will endorse each other so that each account has 3 endorsements before more accounts are added. Yet, each account receives 6 endorsements which can be given out so each individual will still have 3 unused endorsements. Once the number of accounts in the network is 401 or more, the network will require all accounts to receive 3 endorsements before the account is active. The 100 groups will come from each of the 100 largest cities. When the 4 members from each group return to their city they will endorse 4 new members, who will each have 6 unused endorsements and will be able to endorse 8 new members. These members can endorse 16 members, then 32 and so on. This will help the network spread across the globe faster and more evenly. Even if only one group of 4 individuals seeded the network, after about 35 endorsement iterations, every individual will be part of the GlobalVille network. Assuming each endorsement iteration takes one month, it would take about 3 years for the network to reach every individual.

Account Information

A user may add personal and contact information to any account. The information is added in a hashed and symmetrically encrypted form so that it can only be verified by those to whom the original information along with a encryption key is provided. For example let's say the user wants to add their name and address to the account. The user presents strings like:

- “Name: Joe Smith | 3821738”
- “321 Main Street | 9228315”

to the endorsers of their account to certify this information is correct. The endorsers ignore the numbers at the end of the strings and certify that the information is correct by signing the hash of the string. The numbers at the end of the strings are only there to prevent the hash from being easily guessable. The digitally signed certificate from the endorser contains the field name (like

“name” or “address”) and the hash of the presented data for this field. After collecting the certifications from 3 endorsers the user can submit them to the network along with a different encryption key for each field. The network verifies the certificates and stores only the hashes. The hashes are encrypted before being saved. The user can periodically change the encryption keys. Changing the encryption key requires submitting a request with only the current and new key and does not need to involve the endorsers. By changing the encryption key periodically the user can ensure that any requestors that were shown the information previously cannot show the information to others. There is a fee for adding information to an account or making changes to the information. The fee is burned.

Account Renewal

All verified accounts must be renewed annually by paying a renewal fee and uploading new facial images to the account. The endorsers and endorsees of the account are notified about the renewal and given the chance to verify that the image is still of the same person. Otherwise, anyone can file a false information report as described later.

Fake Account Report

Anyone can anonymously report a fake or duplicate account by sending the report from a non-verified account. There is a fee to submit the report, but if the report turns out to be right, the reporter will be rewarded much more than the cost of reporting. Otherwise, the reporter will lose the amount paid to submit the report. The report is voted on by endorsers and endorsees that are up to 3 links away from the user being reported. The user being reported and the immediate endorsers of the user being reported cannot vote on this report. In the case of a “duplicate account” being reported, both the users cannot vote as well as the endorsers of these users. There is a fee to submit a vote. The votes are submitted in a symmetrically encrypted form so that during the voting period the result of the voting cannot be determined. After the voting period is over the encryption keys are submitted so the result of the voting can be determined. Although it would be good if the voting could be anonymous, it does not seem this would be possible; so the votes are not anonymous. The users on the side which receives more votes get to equally divide up the total collected fees. The users who voted on the side that received less votes or did not release the encryption key get nothing back and lose the amount paid to vote. In case of a tie the total collected fees are divided among all the voters. If more than 50% of the votes confirm the report then the reporter is given a reward equal to the maximum fines that would be collected. This reward amount is created and the fines collected are burned. If the account was reported as fake, the account becomes inactive and each endorser is fined 10 times the cost of submitting a report. Also the endorsers lose any unused endorsements. The maximum reward in this case would be 30 times the cost of submitting a report. If the account was reported as duplicate, then both reported accounts become inactive and only one can be reactivated by paying a fine of 20 times the cost of submitting a report and causing the other account to permanently be deactivated. The endorsers of both accounts are each fined 10 times the cost of submitting a report. The maximum reward in this case would be 80 times the cost of submitting a report.

Deceased Account Report

Anyone can report an independent account as dead. Meaning that the individual associated with the account has died. The identity of the reporter is not anonymous and there is a fee to submit the report. If the account that is reported as dead or any of the endorsers of the account does not refute the report within a time limit of two weeks, the account becomes inactive and the reporter is

awarded two times the cost of submitting the report. But if the report is refuted then the endorsers and endorsees of the account may vote on the correctness of the report. The voting process is similar to that defined above for fake or duplicate accounts. If the report is confirmed then the account becomes inactive and the reporter is awarded two times the cost of submitting the report. The reward amount is created. If no voting is required the fee to submit the report is burned.

False Information Report

Anyone can anonymously report a verified account having false information. The report would include at least one or more field names that are believed to have false information. The report is voted on by endorsers and endorsees that are up to 3 links away from the user being reported. The part of the report with details of the false and correct information would be posted in a symmetrically encrypted form and the key would be shared only with users that can vote as well as the user being reported and the endorsers of the user. The encryption key would be sent as a direct message to the users from the user filing the report. The voting process, costs, rewards and fines are the same as for reporting a fake account.

Maintaining Endorsements

If any endorser of a verified user becomes inactive, the user will need to find another endorser within 30 days. Otherwise the user will not have the required minimum of 3 endorsers and the account will become inactive. A fee will need to be paid to activate the account again for 30 days. The account can be repeatedly activated for periods of 30 days, but the fee will double each time.

4. Authentication

There are many times when one needs to present their identity. For example when boarding an airplane or when logging into a website or mobile app. There are also many times when one needs to verify the identity of another individual. For example when interviewing candidates for a job or renting a property. The process of authentication should be very easy for both the presenter and requestor.

The requestor can show the presenter a QR code specifying what information needs to be presented. Showing a QR code is optional and the information to present can be specified verbally or in another way. The presenter is able to use an app on a mobile device or a browser to select what information will be presented to the requestor. The presenter can only present information that was previously certified by endorsers and submitted to the network to be added to the profile of the presenter. The app displays a QR code or a text string which can be presented to the requestor. The requestor can use this information to query the network and verify the presenter.

As an example let's say that the requestor wants to know the full name of the presenter and if the presenter is above the age of 21. The presenter previously had presented strings like:

- "Name: Joe Smith | 3821738"
- "Age above: 25 | 9228315"

to the endorsers to certify they are correct. The endorsers ignore the numbers at the end of the strings and certify that the rest of the string is correct by signing the hash of the string. The numbers at the end of the strings are only there to prevent the hash from being easily guessable. After collecting the certifications from all the endorsers the presenter can submit them to the network to be stored in the profile of the verified account. Only the hash of each string is stored. A

symmetric encryption key can be provided with each field so that data is encrypted before being saved.

When the presenter is asked by the requestor for the name and proof of age above 21 the QR code or string given by the presenter contains the account id of the presenter, the symmetric encryption key and the above strings. The account id is also signed with the private key linked to the public key of the presenter's account. The data provided to the requestor is encrypted with the public key of the requestor. In case the public key of the requestor was not provided, the presenter can query the username of the requestor to obtain the public key from the network. Using the account id the requester can obtain the profile of the presenter. This profile can be unencrypted with the key provided by the presenter. The profile will contain hashes of the above strings along with hashes of other strings. The requestor can verify that the strings given by the presenter are correct by checking that the hash of those strings are included in the set of hashes received from the network.

By changing the symmetric encryption key used to encrypt the profile data in the network, the presenter can prevent the requestor from being able to prove these credentials about the presenter to anyone else using the same data that was given to the requestor.

To authenticate to a web site or a mobile app the presenter can scan the QR code or copy and paste it into the client app. The data presented by the requesting web site or app will contain the data that is being requested and a URL where the response can be posted. The client app will display to the user the data being requested and if the user accepts, it will present the same set of information as described earlier. The web site or mobile app can verify that the data given by the presenter is correct by checking it against the data received from the network.

5. Multisig Payments

The client app can be used to send GETCoin from one account to another. All accounts verified or not can have a username linked to the account. This makes it easier for users to enter the username instead of an account address.

In addition to user accounts which usually require only one digital signature, the network will support accounts which require multiple signatures for spending funds.

An account can also have multisig turned on for a limited amount of time, so that many micro payments between two parties can be done without actually submitting the transactions to the network. These are referred to as tab accounts. For example an account that normally requires only the signature of A to spend funds can be setup to require the signatures of both A and B until some time in the future when it reverts back to only requiring the signature of A. During this multisig period A can send micro payment transactions to B which are only signed by A. At any time during the multisig period B can sign and submit the most recent transaction (most likely the one which gives B the most coins) to the digital ledger to have the payment take effect. B can only submit one of the transactions that was provided by A since all transactions will have the same sequence number which must match with the sequence number in the account for the transaction to be valid. After a transaction is applied the sequence number in the account is incremented, thus other transactions with the same sequence number become invalid.

6. Communications

The client app can be used to send messages directly to a recipient specified as a username. The messages are time limited so that if not viewed by the recipient within 1 week they are lost. If the message was viewed by the recipient, a delivery confirmation is sent to the sender.

A user can place a fee on the account for receiving messages. The sender would need to include this fee as GETCoin tokens to have the message delivered. The payment is sent as an off chain transaction against a tab account. Thus, the recipient will have to read the message to receive the payment. If the message expires and is not read, the sender will be able to recover the payment for sending the message.

7. Storage

The client app can make use of decentralized redundant storage provided by the network of nodes. This storage is used to hold images and other data for the accounts. This storage is provided to reduce dependency on other external applications for critical data needed by GlobalVille. The client app may use other external data storage services for noncritical data.

The data storage model is a simple key value distributed hash table. The key also serves as a public key such that even to store the initial data, the transaction must prove ownership of the public key. Transactions to modify or delete the data must also prove ownership of the public key. Requests to retrieve the data do not need any proof.

The fee for data storage is prepaid using GETCoin tokens. The fee is burned. The amount prepaid sets the number of days into the future the storage will be maintained. The daily storage fee per 1 megabyte is a parameter that is voted on by the community. The fee at the time the data was stored and the size of the data determines how long it will be stored. Even if the storage fee is changed in the future it does not affect the expiration time of data that is already stored. However, if the data is updated the current rate along with the size of the new data is used to determine the new expiration time.

8. Account Protection

Lost Password

The ability to recover an account easily even if one forgets the password or loses the mobile device with the client app is crucial for mass adoption of the GlobalVille system. The GlobalVille identity is controlled by a private key which must be secured and remembered. Losing the private key would lock one out of their GlobalVille account with no way to recover the identity. Since this is likely to happen with a high probability, it is vital for the GlobalVille application to provide a way for users to recover the private key without needing to depend on any third party.

To recover the private key, the user is asked to provide the same image file that was provided when the user first setup the app. The file does not need to be an image file and can be any type of file as long as the size of the file is at least 100KB. The user can also provide a pin with the file. The hash of the file combined with the pin is key stretched using a high memory usage key stretching algorithm such as Equihash so that it requires about a minute of processing time to recover the

private key. The file provides a high level of entropy and is easy for the user to remember. The pin provides additional entropy and key stretching increases the time for each guess attempt.

Robbery Attempt

When funds are stolen from a user in a distributed ledger, there is no way to recover them since there is no third party that can reverse the transaction. There is a greater chance that a user may be forced to reveal the password and give access to the account to an adversary who has the intention of stealing resources from the account. In such a case the user can provide a fake password which causes the account to become frozen. This fake password is setup beforehand to trigger the app to send a transaction that will freeze the account and also alerts all the endorsers and endorsees of the account by sending an automated alert message. The user will need to meet with two endorsers or endorsees to produce a transaction signed by them to unlock the account. The possibility that the victim can lock the account and alert others should help deter this type of attack.

Estate Settlement

When the owner of an account has died, it becomes impossible to access the resources protected by the account. Being able to give an executor access to the resources controlled by the account after the owner of the account has died is crucial for mass adoption of the GlobalVille system. A user can specify another verified user as an executor for the account through the app. This just sends a message to the executor with a transaction that can later be used by the executor to gain access to the account of the user. Who the executor of an account is will not be known publicly since this transaction is not submitted to the distributed ledger; it is only known to the user and the executor. The transaction contains the id of the executor and a timestamp; the transaction is signed by the user. When the account has been marked dead and the executor submits the transaction to the account, the id specified in the transaction becomes the executor of the account. If another transaction is submitted to the account but with a more recent timestamp theallown the id specified in that transaction becomes the executor of the account. The transaction submitted by the executor must be signed by the executor and have a current timestamp (to a few minutes) to prove that the transaction is being submitted by the executor. All transactions to set the executor must be submitted within 5 days of the first transaction to set the executor. Thus, even if a transaction to set the executor was given a more recent timestamp by the user, but the transaction is submitted after the 5 day limit, it will not be accepted and change the executor of the account. This allows the user to setup a main executor and backup executors with priority given to the executor with the most recent timestamp. It also allows the user to change the executor in the future. It also does not let any executor know that they are for sure the main executor until and unless all potential executors compare the transactions they have received from the user.

Once the executor of the account has been set, the executor can use their own private key to submit transactions against the account for a limited time of about one week to settle the account. The endorsers of the account will be notified of this change of control. During this time the executor would be able to transfer funds and gain access to other accounts on behalf of the deceased.

When setting up an executor the user may also want to setup a will to guide the executor. An encrypted copy of the digitally signed will is placed with all the endorsers and endorsees. The symmetric key to decrypt the will is distributed as fragments to the endorsers and endorsees such that 3 of the endorsers or endorsees are needed to decrypt. The will would be signed by the account owner, so it cannot be modified by anyone else. Special precautions should be taken to ensure the will cannot be changed by the executor.

Change Public Key

There may be times when the user needs to change the public key used to control the account. The simple solution is to have the new key specified in a transaction signed by the current key. However, if the current key has been compromised it would be easy for an adversary to lock out the user. To protect the user from such a possibility, the transaction specifying the new public key must be signed by not just the user, but also at least two endorsers. This requires the user to communicate with the endorsers to request having the transaction signed.

Withdrawal Protection

In order to prevent a major loss of funds in case the private key is compromised there is a default upper limit on the amount of funds that can be spent from the account within a 24 hour period. Any transaction that would exceed this limit will be ignored. Once set, the limit can only be changed with a transaction signed by not just the user, but also at least two members from the set of endorsers and endorsees. The change transaction can also specify a time after which the change reverts back to the previous limit.

9. Reputation

An important lesson learned from the online shopping revolution is that ratings and reviews are essential for establishing buyer and seller reputation and facilitating online commerce more safely.

Deterring Buyer Fraud

Chargebacks are not possible in decentralized payment networks. Once a customer has sent funds to a merchant, it is up to the merchant to keep the promise of delivering the goods or service which the customer paid for. In this situation it is very easy for a merchant to fraud customers and never deliver the goods or service. It would be useful in helping to deter such fraud if customers could view some rating metric of the merchant before transacting.

Any account, verified or not, can choose to enable merchant status for the account. There is an initial fee to enabling this feature on an account and a yearly renewal fee for maintaining it. The fees are burned. Enabling this feature will track how many payment transactions the account has received from unique independent accounts over the past one year. Whenever a payment is received by a merchant account from an independent account, the account id and timestamp is added to a list. If there is an older entry from the same independent account, it is removed from the list. A user viewing such a merchant account would be able to see the number of payments from unique independent accounts over the past one year.

An independent account that has sent a payment to a merchant account can submit a fraud report against the account for up to one year. The report would also include a message describing the problem encountered by the customer. This report would be added to the merchant account with the same timestamp as the entry for this user in the list of payments sent to the merchant account. The report would be removed after the timestamp is one year old or if the account that filed the report chooses to remove it. Another fraud report cannot be filed by the same independent account until the first one is removed. There is a fee to submitting such a fraud report, but no fee to remove the report. The fee is burned.

The client App can make a query to receive all the fraud reports filed against a merchant account and the number of unique independent accounts that sent payments to the merchant account over the past one year. This information can help a user decide on the credibility of the merchant and thereby deter buyer fraud.

Deterring Creditor Fraud

A customer may have received goods or service from a merchant and has agreed to make payments for it in the future. However, the customer may fraud the merchant by not making the expected payments. It would be useful in helping to deter such fraud if merchants could see a credit rating for the buyer's account.

When a customer enters into a future payment agreement with a merchant, the customer gives the merchant a digitally signed certificate which allows the merchant to submit a fraud report against the customer until a specified future time. This time would typically be a few months longer than the time given to the customer to complete the future payments. If a merchant chooses to submit a fraud report during this time, the merchant would have to submit this certificate along with a message describing the problem. There is a fee for submitting a fraud report, but not for deleting it. The fee is burned. The report is automatically deleted after five years or earlier if the merchant submits a request to delete it. However, the merchant can pay another fee before the report expires to extend the expiration for another five years. This can be done repeatedly, but the fee will double each time. Note that the customer and merchant accounts could be of any type and are not limited to interaction between a merchant and independent account. However, a merchant would want the customer account to be a verified account or another merchant account rather than an anonymous account.

The client App can make a query to receive all the fraud reports filed against an account. This would help a creditor in deciding to extend credit to a customer and thereby deter creditor fraud.

10. Parameters

The following parameters can be voted on by independent accounts as described in the paper “Global Electronic Trading Coin Economic Model”. Some initial values for these parameters are proposed here.

$A = 18$	the age in years at which an individual is considered independent
$E_v = 3$	the number of endorsements needed for an account to become a verified account
$E_g = 6$	the number of endorsements an independent account can give
$F_{ar} = 10$	the yearly fee for verified account renewal
$F_{ar} = 2$	the fee for adding or changing the account information
$F_r = 500$	the fee for submitting a report against an account
$F_{rv} = 5$	the fee for voting on a report
$T_{rv} = 7$	the time in days for voting on reports
$T_{rr} = 7$	the time in days for revealing votes on reports
$F_e = 50$	the fee for activating account short of endorsements for 30 days
$S_d = 1000$	the default max amount which can be spent in 24 hours
$F_c = 100$	the fee to extending the expiration of a credit fraud report by 5 years
$F_{mi} = 250$	the fee to initially enable a merchant account
$F_{mr} = 50$	the yearly fee to renew a merchant account
$F_{mf} = 10$	the fee for submitting a fraud report against a merchant account

F_{cf} = 100 the fee for submitting a credit fraud report against a customer account
F_s = 0.01 the fee for 1MB of storage per day

11. Economic Model

The economic model for the crypto token used by GlobalVille is defined in the paper “Global Electronic Trading Coin Economic Model”.

12. Distributed Ledger Technology

The Distributed Ledger Technology being developed for GlobalVille is defined in the paper “Unblocked Sharded Ledger”. However, we will also be evaluating other DLT systems such as IOTA, EOS and Toda-Algorand which are currently in development.

13. Contributors

The following individuals provided ideas, comments and feedback to make this paper possible. They are listed in last name alphabetical order. The list is not yet complete.

Osman Ali, Adrian Armaselu, Peter Chapman, Derrick Farris, Marc Mattox, James Ross, Aaron Sullivan, Aamir Syed, Omar Syed

14. References

[1] M. Dahan, A. Gelb. The Identity Target in the Post-2015 Development Agenda. https://openknowledge.worldbank.org/handle/10986/25001

Version 20220315
Original 20170814