The Open Project of Anonymous Identity
– Building the base for an open anonymous online society

The Soothing Coin Team

January 9, 2021

Version 1.0
Downloadable at https://github.com/sthc/AnonyID
Comments are welcome.

Summary

Identity verification is essential for the life in cyberspace. Unfortunately, nowadays identity verification in cyberspace is either virtually non-existent, or has to sacrifice the privacy in our real life. We hereby presents an elegant solution based on the cryptocurrency Soothing Coin (STHCOIN). *The solution allows everybody to establish an* ***anonymous identity (AnonyID)*** *and provides an unprecedented way for universal online authentication.* Like real life identity, a credible AnonyID is established via interactions and connections with other AnonyIDs, and cannot be easily replicated or forged. Each established AnonyID would represent a unique person in the real world and yet would not carry any information from the real world about the represented person. Furthermore, AnonyID is totally transparent, publicly verifiable and thus can be used universally, just like a human face in reality. Since AnonyID is completely separated from the real life identity, when using it for online authentication, one needs not be concerned with leaking his/her identity in the real world. To some extent, the AnonyID system is similar to LinkedIn but everything is anonymous and open to the public. We all need driver licenses and passports to do business in the real society. Soon, just like physical IDs, **AnonyID will be needed by every citizen in the virtual society of cyberspace to prove their identity**. Going above and beyond, AnonyID can be used for equipment and virtual entities as well and support computerized operations (e.g. POS in blockchain). **On top of AnonyID, an online society can be formed that everybody and everything can be a part of anonymously.** Such a society will be the norm in the future cyberspace.

This white paper defines AnonyID, specifies the protocol to implement it on STHCOIN and provides a roadmap. Web functionalities, mobile app and programming APIs for the use of AnonyID are also described. Since both the infrastructure and protocol are open, third parties can participate in the development in their own ways separate from the Soothing Coin team. Furthermore, many interesting issues await the solutions from the public. **The project is open in its nature. Anticipating its broad and deep impacts, we call for the participations of all interested parties.**

Contents

1 Introduction

When it comes to claiming web resources such as social network accounts and cryptocurrency airdrop, identity verification is desired. In practice, the approaches of verification include requiring email address or phone number, or KYC (Know Your Customer). Since email addresses can be obtained at nearly zero cost (e.g. from Google and Yahoo), requiring email addresse without restricting the domain is virtually no identity verification. When phone number is required, if VOIP (voice-over-IP) number is allowed, it is the same as requiring email address without restricting the domain because VOIP numbers are also freely available. When email domain is restricted or non-VOIP telephone number is required, one has to worry about the leak of privacy as the real identity can easily be revealed. When KYC is used, the concerns are similar yet at a much higher level. As we can see, identity verification in cyberspace virtually lies in two extremes: no verification, or sacrificing privacy. Although cyberspace has flourished dramatically during the past few decades of development, somehow a universal identity system has not been established and we have to rely on identities in the real world. That results in the awkward situation of two extremes. As a result, web sites, big or small, have all been long plagued by fake accounts.

With cryptocurrency and the underlying blockchain technology, it is time for a universal identity system to be formed for cyberspace. In the following, we will present such a system that will provide everyone with an *anonymous identity (AnonyID)*. Unlike current web accounts confined to a certain web site, AnonyID is totally transparent and can be verified by anyone on the Internet, no matter which web site is accessed, just like a human face recognizable anywhere. Meanwhile, AnonyID is completely separate from the real life identity and needs to be established within cyberspace independently. To establish and maintain a credible AnonyID, connections to other AnonyIDs must be made and activities need be conducted on the underlying cryptocurrency STHCOIN. As a result, each established AnonyID would represent a unique person in the real world without carrying any information from the real world about the represented person. The system bears some similarities to LinkedIn in that the latter records social connections between users. Nevertheless, every single identity in the AnonyID system is anonymous (i.e. not tied with any real identity), and all the attributes of the identity are transparent to the public and thus can be verified by anyone. Given that, it is practically impossible to forge a credible AnonyID. On the other hand, the system provides ample flexibilities for AnonyID to be used at different levels. For example, a web forum does not need high level credibility of users and can merely check one or two of the AnonyID attributes (e.g. longevity as explained in Section 2.3.1) and set the thresholds low. A social network needs more credibility of users and can scrutinize all the attributes and set the thresholds high. Again, presenting AnonyID for authentication will not reveal any aspects of real identity. Privacy is perfectly protected.

It is important to be noticed that AnonyID is not meant for human use only. Equipment and virtual entities can also be assigned AnonyID and use it for authentication. For example, in Proof of Stake (POS) on blockchain, authentication of the creator of a block is essential. An an example, in the Internet of Things (IoT), authentication of various devices is critical before the data collected from them can be accepted. The transparency of AnonyID will make the processes much more smooth and robust.

In short, AnonyID will fill the gap of identity verification and authentication in cyberspace by making it universally transparent. **On top of that, an online society**

can be formed to have everybody and everything be a part anonymously. In the future, such a society will be vital in cyberspace. The white paper defines the form of AnonyID and its attributes along with how each of the attributes is established and maintained. The operations of AnonyID are realized by a protocol designed on top of the cryptocurrency Soothing Coin (STHCOIN). Every action in the protocol corresponds to one or more special transactions of STHCOIN. As a result, all the information about AnonyID is stored on the underlying blockchain, which guarantees the transparency of AnonyID. The protocol specification is included in this article when the attributes of AnonyID are defined. Web services, mobile app and programming APIs facilitating the use of AnonyID are elaborated as well. The project roadmap shows the expected milestones of the Soothing Coin team. Foreseeing the significance to the cyberspace of the project outcome, we are calling for all parties interested to participate in the development. Both the underlying infrastructure (i.e. the blockchain) and the protocol (specified in this article) are fully open. While utilizing the same infrastructure and implementing the same protocol, the development can be completely separate from that of the STHCOIN team. Furthermore, as to be explained in the rest of the white page, there are many open issues. These issues cannot be properly solved without the input and intelligence from the public and will be very interesting to explore. Only with broad participation can a solid foundation for the better cyberspace be built. Third party development is discussed towards the end of the article.

2 Anonymous Identity (AnonyID)

The AnonyID system is built on top of the cryptocurrency Soothing Coin (STHCOIN). An AnonyID takes the form of a STHCOIN address and its attributes are reflected by STHCOIN transactions. Everything is stored on the underlying blockchain, and are accessible publicly. A protocol is provided to map AnonyID attributes to STHCOIN transactions. The details are explained in the following elaboration.

2.1 The Forms of Anonymous Identity (AnonyID)

Fundamentally, an AnonyID is a STHCOIN address. To get such as address, one visits the Soothing Coin web site (https://soothing.center) and sign up with an email address.[1] The email address does not have to be official and is merely used for sending the second copy of the private keys and important notifications (e.g. coin arrival). Once an email address is entered and password provided, the web site will present an STHCOIN address, for example jMG7wdKsw7bFVSQkGcxvjvSbKZFRwUrfmu. Along with the address, three private keys are provided for the user to download. As a backup copy, the keys are also sent to the email address provided.When operations need to be performed for the address (e.g. sending coins), (any) one of the three keys must be provided. Therefore, it is critical for the user to keep the keys at a safe place. If they are lost, the address can no longer be accessed.

Any activities on the AnonyID (i.e. the STHCOIN address) can be found on the underlying blockchain of Soothing Coin (e.g. through the blockchain explorer at http://chain.soothing.center:8000). Since anybody can access the blockchain, all AnonyIDs are transparent and can be verified publicly.

[1] STHCOIN addresses can be obtained via STHCOIN wallets as well. However, it would be difficult to use them as AnonyIDs because they are provided more for short-term use.

The STHCOIN address for an AnonyID obtained from the Soothing Coin web site is tied to a unique email address. Therefore, the corresponding email address could potentially be used as AnonyID in some situations. Email addresses have the significant advantage that they are much more friendly to human, and is preferred when used by human manually, for example, when one wants to check the credibility of an anonymous online user, only knowing the email address of the latter. The drawback is, though, since email addresses are not stored on the blockchain, they have to be translated to STHCOIN address before verification can be performed with the blockchain data. As we foresee, both kinds of AnonyIDs will be used, depending on the environment and purpose of the usage. If humen need to perform the operations, AnonyID in the email address form will probably be used. On the other hand, if the operations are automatic, e.g. authentication between IoT devices, AnonyID in the STHCOIN address form are more likely to be adopted.

It is possible for a person to create multiple AnonyIDs. However, establishing and maintaining a credible AnonyID consumes much resources (e.g. time, effort and fund) as explained below. It would not be feasible for one to do so, especially if the level of credibility required (by the checking entity) is high.

It should be noted that not all STHCOIN addresses are AnonyID. Only those born as AnonyIDs (Section 2.3.1) are legitimate AnonyIDs.

2.2 STHCOIN Message Exchange Protocol (SMEP)

Some of the attributes of AnonyID are defined by special interactions between AnonyIDs. To perform the interactions, an AnonyID sends a message to another following the STHCOIN Message Exchange Protocol (SMEP) explained below.

When AnonyID X sends a message to AnonyID Y, it must conduct a special STHCOIN transaction. With the transaction, X pays Y a certain amount of STHCOINs. All the inputs of the special transaction must be the outputs (of previous transactions) destined for X, and all the outputs of the special transaction must be destined for Y. The transaction contains two or more outputs specified as follows.

Output 0: The amount must be 0.00000101, and the recipient must be a fixed address. The first version of the protocol uses *jSfM5ZEFM9QaohbrHz6j3GXsHdZeog6qhH*.[2] This output indicates that the transaction is an SMEP message and serves as the message *header* marking the beginning of the message.

Output 1 to n: In each of the outputs, the recipient must the receiver of the message, the amount must be $0.0kkaaabb$, where "kk" (valued between "01" and "99") is the number corresponding to a key and "aaa" (valued between "000" and "999") and "bb" (valued between "00" and "99") are two numbers each corresponding to a different value associated with the key. Therefore, each such output carries a key-value triple. Multiple such outputs means that the message carries multiple key-value triples. The recipient of each output must be unique within the same transaction, but a transaction can carry multiple sub-messages, each to a different receiver.

[2] Other STHCOIN addresses can be used to mark the SMEP header in future versions of the protocol. It may provide an incentive for third party to get involved in the development.

Output $n+1$: This output is also optional, and is used only when excessive coins need to be sent to back X itself.

Output $n+i+1$: If the previous optional output is not present, $i = 0$, otherwise $i = 1$. In this output, the amount must be 0.00000111, and the recipient must be another fixed address, for which *jdjnxpQTQX6RUvz1dDRKsxJiKn6d4vmTZo* is used in the first version of the protocol.[3] This output serves as another indication of this transaction being an SMEP message and marked the end of the message as the *trailer*.

.

STHCOIN's transaction fee is set to no more than 0.00001 (1×10^{-5}) coins per transaction. Typically it is less than 0.0000001 (1×10^{-7}) coins. The smallest unit of STHCOIN is 0.000000001 (1×10^{-8}). One does not need to worry about spending too much on messaging.

2.3 The Attributes of AnonyID and The Implementation

The credibility of an AnonyID depends on its attributes. The more credible an AnonyID, the more likely it is the unique AnonyID owned by the person behind it.

2.3.1 Longevity

The longevity of an AnonyID is the length of the period from the time of the AnonyID's birth to the time when the longevity is measured. An AnonyID is born when any of the following events occurs.

- The AnonyID declares its birth by sending a birth message. The birth message's receiver is the AnonyID itself, and has the key-value triple $(05, 555, 55)$. That is, in the triple, $kk = 05$, $aaa = 555$, $bb = 55$.
- The AnonyID sends an SMEP message of other types (Section 2.3.2, 2.3.3) to another AnonyID.
- The AnonyID receives an SMEP message from another AnonyID.

Once included in the blockchain, the date/time of the block containing the transaction is the birthdate of the AnonyID. When an STHCOIN is first involved in a transaction, it is *conceiving* an AnonyID. Only with one of the aforementioned events can an AnonyID be created (or born).

A newly created STHCOIN address has no balance and thus the associated AnonyID cannot send messages. To help AnonyIDs get started and grow, on the web site, STHCOIN provides a long term lottery program where every STHCOIN address from a unique IP address can do one draw every 24 hours and receive coins. The coins received from the lottery program can be used to perform activities (as shown afterwards) for the associated AnonyID. STHCOIN also provides another long-lasting program where users can tweet on Twitter with specific content to receive coins. The details can be found in the forum posts. Of course, coins can be obtained via other

[3] Similar to header, other STHCOIN addresses can be used for trailer as well in the future.

means as well such as purchases, mining and referral etc as explained in the forum at https://oracle.soothing.center.

Usually speaking, the longer the longevity, the more credible an AnonyID is. However, at the beginning of the project, the longevity of all AnonyIDs are low and other attributes of AnonyID should be used to calculate the credibility until some AnonyIDs have established meaningful longevity.

The birth is the first STHCOIN transaction involving the STHCOIN address associated with AnonyID. Since all STHCOIN addresses start with zero balance, in the first transaction, the address must be receiving coins from others.

2.3.2 Bilateral (Two-Way) Connectivity

Two AnonyIDs may have good relationship with each other. For example, they may have interacted for a long time online, and they may know each other well in the real world. Indicating such relationships can increase the credibility of an AnonyID. Bilateral (or two-Way) Connectivity is provided for such indications.

Request: To initiate the establishment of the two-way connectivity between AnonyID X and Y, a request message with the key-value triple $(03, aaa, bb)$ is sent from X to Y or from Y to X. (Without loss of generality, we will assume X sents to Y.) In the key-value triple, the key 03 $(kk = 03)$ indicates that the triple describes the request to establish a two-way connectivity, the first value aaa indicates the type of two-way connectivity and the second value bb indicates the strength of the connectivity. In the first version of the white paper, only one type of two-way connectivity is used, defined as "acquaintance" (i.e. how well the two AnonyIDs know each other), and $aaa = 01$. For "acquaintance", the level of strength can be from 1 $(bb = 01)$ (weakest) to 10 $(bb = 10)$ (strongest). For example, to indicate acquaintance of the weakest strength, with $kk = 01, aaa = 001, bb = 01$, the coin value for the key-value triple is 0.00300101. For the strongest strength, the coin value is 0.00300110.

In the future, other types of two-way connectivity such as blood and relationship can be defined. The discussion will be opened to the public in the Soothing Coin forum https://oracle.soothing.center.

Confirmation: To complete the establishment of the two-way connectivity between AnonyID X and Y, assuming X sent the request to Y, Y needs to sends a confirmation back to X. The key-value triple in the confirmation message is $(02, aaa, bb)$ where the aaa value must be the same as that in the request. Once both the request and confirmation are recorded on the block chain, the connectivity becomes valid until cancelled. The strength of the connectivity is the minimum of the bb values in the two messages. If no confirmation is received for a request within 5040 blocks (equivalent to approximately one week), the request expires.

Cancellation: Good relationship may end, and a way must be provided to indicate so in the system. For AnonyID X to cancel a bilateral connectivity with Y, a message with the key-value triple $(04, aaa, bb)$ is sent from X to Y. In the key-value triple, the key 01 $(kk = 04)$ indicates that the triple describes the cancellation of a two-way connectivity, the value of aaa must be exactly the same as the aaa value used in the establishment of the connectivity, where the bb value does not matter. For example, if the key-value triple used in the request to establish the connectivity is $(03, 001, 05)$, the corresponding cancellation should be $(04, 001, 00)$ where the only difference is the key.

To cancel a bilateral, either AnonyID may perform the cancellation by sending the message specified above. A single cancellation message is sufficient to end the connectivity. If both entities sends a cancellation message, the outcome is the same as that only one side sends the message.

2.3.3 Unilateral (One-Way) Connectivity / Endorsement

If an AnonyID (X) believes that another AnonyID (Y) is credible, X can endorse Y and thus form a unilateral (or one-way) connectivity from X to Y. Endorsement is uni-directional and can be used when X has certain advantages (e.g. first comers or with higher reputation) over Y. Since it is unilateral, X-to-Y connectivity does not imply Y-to-X connectivity, or X's endorsement of Y does not imply Y's endorsement of X. If X endorses Y, it could be that Y does not endorse X at all, or Y endorses X for a different type and/or at a different level (to be defined below).

Request: In order for X to endorse Y, Y must send a request to X first. The request has the key-value triple $(09, aaa, bb)$. The key 09 ($kk = 09$) indicates that the triple describes a request to establish a one-way connectivity, the first value aaa indicates the type of one-way connectivity and the second value bb indicates the strength of the connectivity. In the first version of the white paper, only one type of one-way connectivity is used, defined as "uniqueness" (i.e. by how much X would believe Y is unique to the person behind it), and $aaa = 001$. The level of strength can be from 1 ($bb = 01$) (weakest) to 10 ($bb = 10$) (strongest). For example, if X is 100

Similar to two-way connectivity, other types of one-way connectivity will also be discussed in the public in the Soothing Coin forum https://oracle.soothing.center. Properly defined one-way connectivities will serve as good indicators of AnonyID credibility.

Confirmation: After a request is received, if X agrees with the endorsement, it sends a message with the key-value triple $(01, aaa, bb)$ is sent from X to Y. Once the transaction is recorded on the blockchain, the connectivity becomes valid until cancelled.

In the key-value triple, the key 01 ($kk = 01$) indicates that the triple describes the establishment of a one-way connectivity, the value of aaa must be the same as the aaa value in the request, where bb should be no more than the value of bb in the request. The bb value in the confirmation decides the final strength of the connectivity. If no confirmation is received for a request within 5040 blocks (equivalent to approximately one week), the request expires.

Cancellation: For AnonyID X to cancel an endorsement to Y, a message with the key-value triple $(08, aaa, bb)$ is sent from X to Y. In the key-value triple, the key 08 ($kk = 08$) indicates that the triple describes the cancellation of a one-way connectivity, the first value aaa must be exactly the same as the aaa value used in the establishment of the connectivity, while the second value bbb does not matter. For example, if the key-value triple used for confirming the connectivity is $(01, 001, 05)$, the corresponding cancellation should be $(08, 001, 00)$.

Circular Endorsement: To discourage cheating, circular endorsement is not allowed. A circular endorsement is formed if X endorses Y, Y endorses C, and so on, and the last one endorses X, and all the endorsements involved are about the same type (i.e. with the same first value in the key-value triple). If a circular endorsement is detected, the last endorsement completing the circle will not be recognized. Moreover, such endorsements will reduce the credibility of the last endorsing AnonyID.

2.3.4 Activeness

The activeness of an AnonyID X is about how much it interacts with other AnonyIDs. It has the following three aspects.

Message frequency is the number of messages sent per unit of time (e.g. day) by X during the most recent period. It is calculated as the total number of messages during the period divided by the length of the period. Depending on the length of the chosen period, the frequency could be short term or long term. Either one or both can be used, depending on the scenario that the calculation is needed for. This aspect shows how active an AnonyID is in the virtual society. The pattern and type of messages can also be analyzed to obtain further insights.

Transaction frequency is the number of non-message STHCOIN transactions conducted per unit of time (e.g. day) by X during the most recent period. It is calculated as the total number of STHCOIN transactions during the period divided by the length of the period. Only the transactions that are not representing SMEP messages are counted. Depending on the length of the chosen period, the frequency could be short term or long term. Either one or both can be used, depending on the scenario that the calculation is needed for. This aspects indicates the finance activeness of the AnonyID.

Company size is the number of unique AnonyIDs that X conducts transactions with during the most recent period. It is calculated as the total number of unique AnonyIDs (excepts X) that are the senders or receivers of the STHCOIN transactions involving X during the period, divided by the length of the period. Again, all types of STHCOIN transactions are counted. However, if the sender of receiver of a transaction is not a registered AnonyID, it should be ignored for the calculation. Its usage is smilar to transaction frequency. Non-AnonyIDs are not included as many cryptocurrency addresses are for one-time use only.

Under certain circumstances, the transaction frequency and company size of an AnonyID may be confined to certain transactions involving certain AnonyIDs, depending on the interest of the party performing the calculation.

2.3.5 Balance

The balance of an AnonyID X is the amount of STHCOINs that X possesses. To obtain a more reliable number, the average balance over the most recent period can be calculated, or the balance can be sampled multiple times during the most recent period and be averaged.

2.4 Authentication of AnonyID

To verify that a user is the owner of a particular AnonyID, it is as simple as asking the user to send some STHCOIN to the verifier. Any amount will be sufficient as long as it is more than the dust value 0.0000003(3×10^{-7}. For reliability, it is recommended that two small amounts are requested to send. The process is as follows.

1. A user provides the AnonyID and asks to be verified.
2. The verifier asks the user to send two amounts (x_1 and x_2) of STHCOIN from the provided AnonyID to the verifier.
3. Within a certain amount of time (up to the verifier), if the two amounts are received from the provided AnonyID, the user is authenticated, otherwise not.

2.5 Credibility Calculation

Once the ownership of an AnonyID is verified, the credibility of the AnonyID itself needs to be checked. Since all the AnonyID attributes take resources to build up, generally the more resources contributed to the establishment and maintenance of an AnonyID, the more credible it can be. The contributions include multiple aspects such as time and efforts, not necessarily just money. Money itself cannot make an AnonyID credible. To obtain a reliable perception of an AnonyID's credibility, it is also important to check multiple (if not all) attributes instead of looking at just one or two.

Longevity is an attribute that no one can cheat on. The longer the longevity of an AnonyID, the more credible it can be. However, it should not be used alone. An inactive AnonyID with an old age probably does not correspond to a user active recently.

Bilateral connectivity and unilateral connectivity are similar in that they both describe relationship between AnonyIDs. The higher the bilateral connectivity or the unilateral connectivity (being endorsed), the more credible an AnonyID is. However, the credibility also depends on the credibility of the AnonyIDs connected with. For an AnonyID X, if the credibility of connected AnonyIDs is low (high), the credibility of X would be low (high). The credibility depends on the pattern of connections as well. If the connections are formed within a closed group with a small number of AnonyIDs, the credibility is questionable. In the contrast, if the connections are with AnonyIDs that are well connected (directly or indirectly) with the rest of the AnonyIDs in the system, the credibility is high. Moreover, according to the well known conclusion of six degree of segregation [4] in social science, any two AnonyIDs should be able to reach each other in no more than six connections. Anything more than that reduces the credibility.

In unilateral connectivity, since circular endorsements are not allowed, the root of the endorsement chain [5] (i.e. the very first AnonyID that endorses another AnonyID in the chain and is not endorsed by any others) is important. Its credibility would significantly impact the credibility of others in the chain. For example, the AnonyID of the creator of Soothing Coin is **jMG7wdKsw7bFVSQkGcxvjvSbKZFRwUrfmu**.

[4] https://en.wikipedia.org/wiki/Six_degrees_of_separation

[5] An endorsement chain is formed where A endorses B, B endorses C, C endorses D and so on.

The endorsement chain rooted at this AnonyID could be considered to have high credibility. Of course, over time multiple AnonyIDs may become famous and can server as the root of widely accepted endorsement chains. Another thing to consider is the length of the endorsement chain. Understandably, the further away an AnonyID is from the root in the chain, the less credibility it can derives from the root. Again, according to the six degree of segregation, we recommend that no endorsement chain should contain more than 7 AnonyIDs. In other words, the endorsement to an AnonyID that is of more than 6 connections away from the root should be disregarded. Furthermore, it is possible for an AnonyID to endorse multiple AnonyIDs. To prevent the abuse of the advantage an AnonyID has, the credibility added by endorsement should decrease or diminish if the AnonyID endorses too many others.

When calculating credibility based on connectivity, as to be explained in Section 2.6, the credibility of connected AnonyIDs must be considered as well. For example, if AnonyID X endorses Y, and Y's credibility decreases because of abuse (Section 2.6), X's credibility should decrease as well. The best way to calculate the propagation will need to be explored during the use of the system.

Activeness is about the frequency and breath of an AnonyID's activity. If social interaction is the focus, message frequency and company size can be used. If finance interaction is the focus, transaction frequency can be used. The mix can be used as well. Balance emphasizes on the finance strength, and will probably be used more for finance related examination.

It should be noted that the above discussion is merely some preliminary thoughts. The exact formulas for calculation will have to be deliberated. Some of them will have to evolve while AnonyID is in use, as many things will be new in a purely online society. While many conclusions about the society in the real world can be leveraged, much more exploration has to be done for the virtual one. Extensive study need to be performed to support the development of reasonable calculation of credibility. Additionally, different situations call for different calculation. For example, a casual forum's calculation could be more relaxed than that of a social network. For academia and industry alike, credibility calculation is an interesting issue to explore.

2.6 Abuse Detection

When AnonyID is used for authentication, abuse could happen. Such events should be recorded and factored into credibility calculation. Should abuse be found for an AnonyID, not only its credibility be reduced, the credibility of those AnonyIDs connected with it (bilaterally or unilaterally) directly or indirectly should also be negatively impacted. Nonetheless, the further away from the abusing AnonyID in connectivity, the less impact there should be. Whether the decrease should be linear or exponential and what should be the coefficients will have to be explored.

However, how abuse is reported has to be carefully considered. Abuse events can only be reported by AnonyIDs because AnonyID is the only valid identity in the system. The reports also have credibility issues, which relies on the credibility of the reporting AnonyID. A loop of impacts is thus formed: AnonyID credibility (partially) depends on abuse reports, and the credibility of abuse reports depends back on AnonyID credibility. When checking the credibility of abuse reports, the calculation needs to be careful to avoid infinitely continuous degradation. More complicated situations can arise. For example, AnonyID X reports abuses of Y and Y does the same on X. The processing of the two reports must be kept indepedent of each other.

3 The Support System for AnonyID

Since all AnonyID operations are performed via STHCOIN transactions, technically everyone can directly use the cryptocurrency and the underlying blockchain to do them. Nonetheless, web sites and mobile apps dedicated for the operations will make it much more convenient.

For users who establish and maintain AnonyID, the functionality of **web services and mobile apps** will include:

- Registration (to create an AnonyID).
- Obtaining STHCOINs for AnonyID operations.
- Declaration of birth.
- Sending requests to establish (one-way and two-way) connectivity.
- Checking the status of requests to establish (one-way and two-way) connectivity.
- Confirming (one-way and two-way) connectivity.
- Cancelling (one-way and two-way) connectivity.
- Retrieving the attributes of an AnonyID (not necessarily of the user's own).

For users (e.g. web sites) who need to verify the credibility of AnonyIDs, a **programming API** will be provided and allow them to authenticate users (as described in Section 2.4). Using the API, the user can delegate the authentication process to the support server and provide a callback point. Once the process finishes, the support server will use the callback to inform the use of the result.

The above functionalities would be sufficient to support the most basic operations of AnonyID. As the system evolves and needs appear, more will be added. The details will be revealed after implementation.

4 Roadmap

The project will follow the approximate timeline given below. Minor adjustments will be made should the situation changes. Meanwhile, the definitions and protocols will keep being refined and augmented.

Completed – Developing the registration web page for creating AnonyIDs.

Completed – Developing the web pages for STHCOIN distribution to support AnonyID operations.

2021 Q1/Q2 – 1) Fundraising (through ICO etc) to have STHCOIN listed on reputable cryptocurrency exchanges. 2) Buiding community.

2021 Q3 – Completing the development of a prototype of web services for birth declaration, connectivity establishment/cancellation and attribute retrieval.

2021 Q4 – Completing the development of a prototype of the programming API for authentication.

2022 Q1 – Completing the development of a prototype of mobile apps for birth declaration, connectivity establishment/cancellation and attribute retrieval.

2022 Q2 and after — Continuous development and refinement of AnonyID.

5 Third Party Development

As explained in the preceding sections, AnonyID leverages the cryptocurrency Soothing Coin (STHCOIN) whereas STHCOIN operates on top of a permissionless blockchain. With the source code of STHCOIN open to the public at https://github.com/sthc/sthcoin, everyone can develop a support system for AnonyID, as long as the protocol given in this white paper is followed. Given that, the support system to be developed by the Soothing Coin team will only be one of them. All the systems will be compatible to each other, because they all follow the same protocol and all the data are stored in the same blockchain. To understand that, consider the example where computers communicate with each other on the Internet owing to the fact that they all implement the same network protocols and use the same network (i.e. the Internet).

There will be many different application scenarios of AnonyID. For different scenarios, the requirements of credibility calculation are likely to be different. There could be different ways to integrate AnonyID into the existing systems as well. People at different places or in different cultures may have different use habits and have different expectations. No single solution is expected to be the panacea. Even for the same application scenario, competition will help to find the best solution. For a healthy eco system, third party development is very much needed.

As explained in SMEP (Section 2.2, third party developers can use their STHCOIN addresses for the message header and/or trailer. When messages are sent, they will receive coins as rewards. That can be an incentive for third party developers to participate. In order for the system to remain universal, new STHCOIN addresses used for message header/trailer must be incorporated into the protocol for the public to follow. That means, the protocol will be revised over time, and the revisions will be published in a future version of white paper, accessible publicly at https://github.com/sthc/AnonyID. Protocol revision and white paper maintenance will be handled by the Soothing Coin team at the beginning. As the project progresses, a consortium will likely be formed and take over the tasks.

If a development team would like to offer STHCOINs for AnonyIDs to be created, negotiation can be made with the Soothing Coin team. All other functionalities can be developed with zero involvement of the Soothing Coin team.

As the project deepens and broadens, it is very likely that other cryptocurrencies/blockchains will join the project with each cryptocurrency/blockchain forming an sub-system to support AnonyID. At that point, how the different sub-systems interact and coordinate with each other will be discussed. Existing protocols may need to be revised and new protocols will need to be designed. At the end, it will be a consortium of cryptocurrencies/blockchains serving the basis for AnonyID.

6 The Vision

Authenticatable identities are the basis for individuals to distinguish oneself from others, and therefore are the basis for various behavior in a society. Online societies are no different. In fact, being virtual in cyberspace, online societies rely more on authenticatable identities as many tangible characteristics of real people are weakened or hidden. Up till now, such identities are virtually non-existent in cyberspace. As a result, online authentication has to rely on real identities or give way to fake accounts. That ties online societies to the real society. In addition, today's online societies are fragmented. Each web site (e.g. Facebook and Twitter) has its own user group that forms a separate society. The authentication process of each site is a blackbox, while every site intends to win over others (by offering OAuth authentication).

The vision of AnonyID is to provide universally accessible authenticatable identities through a completely open process, and keep the identities fully separated from the identities in the real world. The immediate outcome would be to facilitate online authentication without sacrificing privacy and overcome the fake account problem. As a more far-reaching impact, a unified online society can be built on top of that, where everybody and everything is a part with a unique identity. Again, since the identity is independent from that in the real world, the unified online society will become parallel to the one in the physical world. Maybe, a new kind of "parallel universe" will come into our life?

The mist needs to be cleared. The wild needs to be explored. We can only see the beginning. While we are sure that the AnonyID project will not be the end of the move toward the future cyberspace, it will certainly go down in history as a pioneer.

7 Key Pointers

The existing major resources for the discussion and development of AnonyID so far includes:

AnonyID Documentation Github repo: https://github.com/sthc/AnonyID

AnonyID forum: https://oracle.soothing.center/c/anonymous-identity-anonyid

AnonyID Telegram group: https://t.me/AnonyID

The existing major resources for the operations of the underlying cryptocurrency STHCOIN so far includes:

STHCOIN web site: https://www.soothing.center or https://www.soothing.cash

STHCOIN Github repo: https://github.com/sthc/sthcoin

STHCOIN Telegram group: https://t.me/sthcoin

Blockchain browser: http://chain.soothing.center:8000

The pointers will be updated as progress is made.