VerifyUnion

WHITEPAPER

DISCLAIMER

This document and any other VerifyUnion documents do not constitute a prospectus of any sort and are not a satisfaction for investment. The UC Coin does not represent an ownership or share in ANY public or private corporation, or other entity in any jurisdiction. Acquisitions of UC Coins through the Crowdsale are non-refundable. UC Coins are only to be used in connection with VerifyUnion under the Terms & Conditions. Any acquisition and use of UC Coins carries significant financial risk, including the use of experimental software.

Version 1.17
September 15th, 2017
Written by the VerifyUnion Team
www.verifyunion.io

CONTENTS

ABSTRACT

Hacks, identity theft, leaks of personal data, password breaches, and document fraud are just a few reasons why current online safety measures are not trusted.

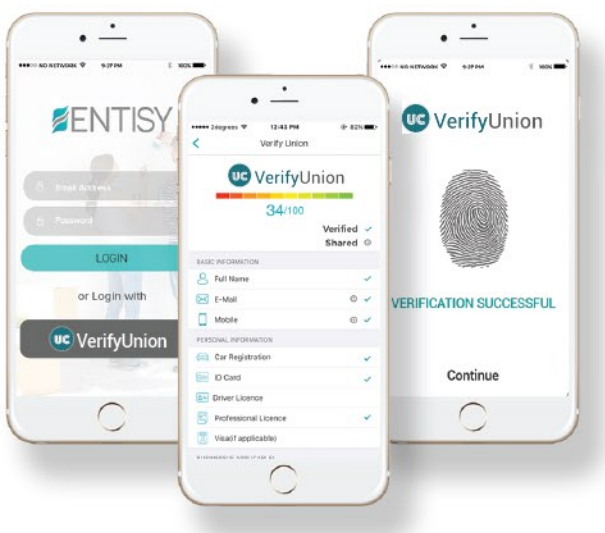
We introduce a new system to users which takes the benefits of Blockchain and the Ethereum Network and applies them to help our users in a world where Privacy and Security are at stake.

When we use a digital service, and upload our personal documents and information, most of us are unaware of who is using those identification details and for what specific purposes. The inefficiency and significant risk of the current system is that, once the documents or personal details are transferred, the authority of the owner of the information is cut out and they cannot track or trace the flow of their details.

VerifyUnion has developed a unique portfolio for all users, which returns a "True Value". True Value comprises the combined values derived from verifying digital identification, social & public profiles, as well as financial details linked to the User's unique profile. Users portfolio value benefits by gaining higher authenticity for their Trust and Verification services. This methodology allows users to provide essential information for required verification to be completed, and they can increase their portfolio True Value by providing additional data that the User and Evaluator agree upon.

The Blockchain can offer a solution by decentralizing the ownership of credentials and offering a universally available protocol for verifying one's record in an immutable chain of data. This data, rather than being stored on a per app basis, is stored in a shared ledger. This shared ledger is downloaded by each individual user of the Blockchain and is a record of every transaction ever made.
VerifyUnion offer a hybrid version of advantages of both during the transition phase while we complete the development of the fully Decentralized solution. By using Blockchain technology we aim to give full authorization of the Digital Verification Process to the personal user.

VerifyUnion is an Integrated Platform where users can register to safely achieve all their secure Digital Identification needs. Personal information is kept in the user's personal storage only rather than sending it to an anonymous person or company, and the user can then decide to share that information without sending to the centralized authority. Personal details will be sent to the requesting person with the user maintaining full authority over the information being transferred.



ABSTRACT

VerifyUnion proposes the broader concept of Trust Verification, and is not limited to Digital Identity Verification. This facilitates users and requesting authorities to exchange a handshake to verify the individual including social profile, social influence, interests and digital identification at the same time.

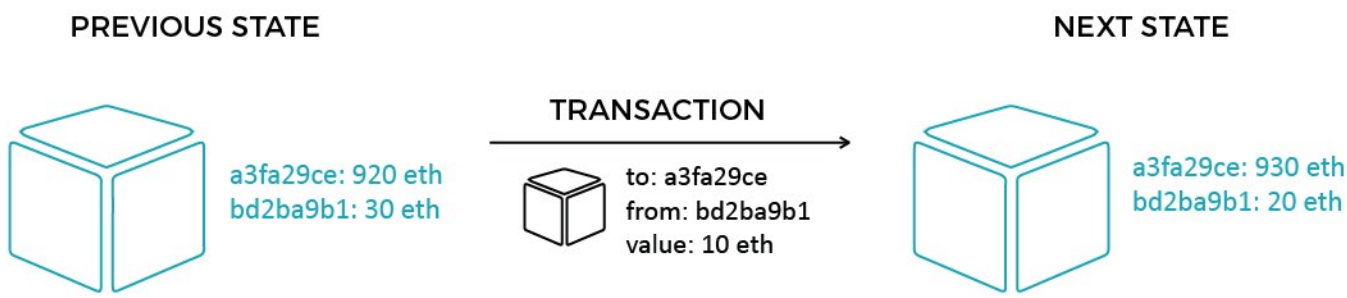
VerifyUnion is a platform utilising the advanced features of Blockchain technology to identify and verify digital identity over the internet. Verify Union will give our clients (organisations seeking to verify their customers or users) superior features and fast verification of users by applying our tailored algorithms across different industries. Powered by the enhanced technology of Blockchain development by linking identity on to the block to produce a tamperproof system which helps to reduce fraudulent activities and spoofing of digital ID documents. By building on the existing Blockchain technology, there is no longer a need to trust server administrators, as the system creates greater authenticity and verifiability through our platform.

VerifyUnion also intends to use the UC Coin to transact in the ecosystem when requesting Trust Validation Services and Social Scoring Information from the platform, as the platform token for the Software-as-a-Service (SaaS) business model. VerifyUnion hopes this ecosystem can reduce the current deficiencies found in the Centralised Platforms.

VERIFYUNION BUILDS ON ETHEREUM BLOCKCHAIN

Ethereum is a decentralized platform that runs Smart Contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.
These apps run on a custom built Blockchain, powerful shared global infrastructure that can move value around and represent the ownership of property. The structure of the Ethereum Blockchain is very much like Bitcoin's, in that it is a shared record of the entire transaction history. Every node on the network stores a copy of this history. The big difference with Ethereum is that it’s nodes store the most recent state of each Smart Contract, in addition to all the Ether transactions. For every Ethereum application, the network needs to keep track of the ‘state', or the current information of these applications, including each user's balance, all the Smart Contract code and where it's all stored.

We are building VerifyUnion on the Ethereum Blockchain which gives us the added advantage of one extra layer of security, and due to the decentralized nature of Ethereum, users can be worry-free as decentralized systems significantly reduce the probability of successful hacking, when compared to centralized systems.



ABSTRACT

NEED FOR A NEW METHODOLOGY

With the proportion of business interactions conducted online continuing to climb, the need for secure digital identities has never been stronger.
Whether it's a company placing an order with supplier, a consumer purchasing from online store, an individual opening a bank a ccount or applying for work or credit, being able to prove identity is a critical step in every online transaction.

With International laws in place for Know Your Client (KYC) and Anti Money Laundering (AML), and specific laws in countries to fight fraud and corruption, the need for Digital Verification is growing stronger by the day.

This need is also growing when it comes to dealing with public sector entities. Both businesses and consumers are becoming increasingly frustrated by the often-convoluted methods they are forced to use to interact with government agencies. Too many people are experiencing a large amount of friction when proving their identity, resulting in them giving away more information than they should, and not being aware of how it is going to be used.
While there are a range of digital ID systems already in use, there remains a need for a unified approach that could be adopted by multiple organizations. Having such an infrastructure in place would streamline interactions while ensuring individual identities remain secure always. And on the other hand, the problem seems obvious. We all need a consistent digital identity (think virtual ID "card") that can identify and authenticate us not only for all our devices, but to all our online services, commerce and banking accounts, and essentially anything where we need to digitally, or even physically, verify who we are.
Solving that problem, it turns out, is very difficult. For one, any kind of digital identity solution needs to be platform and device independent. It’s fine to be able to swipe into your phone with a fingerprint reader, but most people own more devices than just one smartphone, and in many cases, they run different software on different platforms.

The number of victims of identity theft rose by 57% in 2015 in the UK. The data, taken from 261 companies in the UK, suggests fraudsters are increasingly getting people's personal information from social media sites. Facebook, Twitter and LinkedIn have become a "hunting ground" for identity thieves, with more than 148,000 victims in the UK in 2015 compared with 94,500 in 2014.

Introducing Blockchain to this scenario provides an efficient and long-term solution to the problem of Digital Verification. Blockchain, the technology behind the bitcoin digital currency, is a decentralized public ledger of transactions that no one person or company owns or controls. Instead, every user can access the entire Blockchain, and every transfer of funds from one account to another is recorded in a secure and verifiable form by using mathematical techniques borrowed from cryptography. With copies of the Blockchain scattered all over the planet, it is effectively tamper-proof. Blockchain can increase security on three fronts: blocking identity theft, preventing data tampering, and stopping denial of service attacks.

ABSTRACT

SOCIAL TRUST-AS-A-SERVICE (SOCIAL SCORING AND VALIDATION)

We are continuously developing a sophisticated Social “Trust” system which uses a social scoring system to deter-mine users’ level of validation within the platform. Trust Verification is an integral part of the secondary platforms we develop, and represents a significant stand-alone profit centre, in the form of “Trust-as-a-Service” offering a Trust and Social Scoring module. Most of this information will be derived from Social Scoring Algorithms that run parallel to the user’s Digital Identity. The User will receive updates on his/her social score and data from all the social media and public files under his/her management as well as other pubic data, available or unavailable to the public. The user can then share this information when prompted to do so or reject such a request.

This data can include social media scoring and history, credit records, company shareholdings and directorships, firearms licences, drivers licences, police records, and criminal records to name a few.

Users can increase their social score by providing more information about themselves and storing that in their private storage and share that using encryption under individual discretion to the requesting authorities. By using this platform, users get rewarded in VerifyUnion crypto tokens (UC Coins) and keep that for future verifying services. We also expect to buy back tokens from our users for a premium price when the demand for tokens increase.

We also expect to buy back tokens from our users for a premium price when the demand for tokens increase.

RESEARCH AND DEVELOPMENT

In very simplistic terms a digital identity is a digital representation of your real-world identity. Digital identities are an essential part of the transformation of online services, the “key to the door” of digital transactions. VerifyUnion is a digital identity manager that is secure, trusted and will be accepted by the industry wherever a customer chooses to use it. At present, we all have multiple digital identities, typically a unique one with each service provider, designed around traditional company and organization centric service delivery and business models. But this model is fast changing with the emphasis in the digital world now on the age of the customer and user-centric service design. To support this, a new approach for digital identities has emerged. One where the user is in control of their identity. This initiative explored the use of a single digital identity to access multiple services from user, provider and industry perspectives.

The lack of a proper verification system has both financial and social costs. According to the stats as of August 2017, approx. 1.75 billion people in the developing nations lack a proper ID, this includes more than 200 million children aged under 5yrs. Approx. 2.5 billion adults, just over half of the world's adult population, do not use formal financial services to save or borrow. 2.2 billion of the unserved adults live in Africa, Asia, Latin America, and the Middle East.

As an example: within the UK there is no single authoritative source or credential, which can be used for asserting identity securely in an online transaction. 36 million adults (75% of the adult population) in Great Britain are now online every day, and 72% of these adults buy goods or services online. These statistics, combined with the increased sensitivity of online transactions, for example banking and government services, creates a challenge for organizations that need to verify and authenticate the identity of each one of its customers or citizens. As we see more government services move online we need to consider the security required for accessing online healthcare records, employment benefits and taxation affairs, and recognise that these types of transaction require an increased level of security when it comes to the assertion of identity.

VERIFYUNION IS A SOLUTION TO:

Digital Identity Management

With so many more of the world’s population now interacting and transacting online, it means that there are additional requirements to create online “trust” to reduce the risk of online fraud and many other forms of abuse. The creation of digital identities through a framework of standards and governance is a method to create this trust. When organizations can trust people using digital identities it will mean more services and transactions can move online, resulting in huge cost savings.

Current Financial Services Industry

The financial services industry is required to complete Know Your Customer (KYC) checking for the verification of identity to comply with regulations. This is a risk-based approach, which is open to interpretation on a product and institution basis. The industry is currently undergoing a dramatic transformation as it embraces the digital revolution. Increased customer engagement and better user experience, choice, competition, transparency, and new and innovative services are some of the desired outcomes being driven in part by a technology revolution.

RESEARCH AND DEVELOPMENT

Cost of Data Acquisition and Sharing

For a bank to on-board a single customer, it costs them an average of US$15-$25 to load a full KYC profile. If the user wants to apply for an extra service (eg: credit card, car loan) on top of that, they need to provide additional documentation which may or may not be required for the transaction, wasting time (and more cost) for both the provider and the customer. Moreover, the total timeframe needed to complete a KYC profile is also increasing day by day, with more and more stringent regulations adding to the user profile requirements. In general, to be on the safe side, the regulators require collection of as much information as possible to confirm the identity of the user, resulting in unnecessary and sensitive information being transferred multiple times, such as SSN Number, IRD number etc, which might not be needed for the KYC.

Security and Privacy

The biggest concerns are for companies that rely on digital channels for selling their products and services. With every headline about a major data breach, doubts rise about the safety of sharing data. Every day, billions of people around the world use the Internet to share ideas, conduct financial transactions, and keep in touch with family, friends, and colleagues. Users send and store personal medical data, business communications, and even intimate conversations over this global network. For the internet to grow and thrive, users must be able to trust that their personal information will be secure and their privacy protected.
Data transmission across mobile networks is the least secure method, and transactions using a digital wallet will be subject to the risks inherent in any mobile transaction. There is also the risk of having your phone lost or stolen, jeopardizing your personal and financial information. Perhaps one of the biggest risks with a digital wallet is the personal liability in the event of fraud. Most consumers who use debit or credit cards to pay for purchases have a level of protection from their bank or credit card company. Most financial institutions do not hold their cardholders liable for fraudulent purchases on their credit cards. This fraud insurance does not currently exist for consumers using digital wallets.

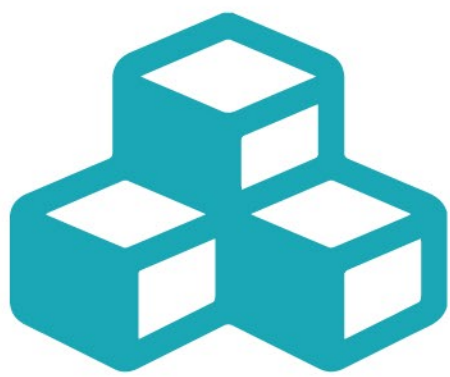
According to data collected by the U.S. Census Bureau. The survey of more than 41,000 households showed that 19% of Internet-using households representing nearly 19 million households had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the survey. By using the Blockchain Technology, it will allow the user to have complete authority over what information they agree to share and it will only be released to the requesting authority under the user discretion on a need-to-know basis. By using advanced technology of Biometric protection and 2FA, there are additional layers of security over the normal Blockchain secure server. In many instances, firms are required to pay high fees to verify the identity of the individual who might have been verified a few seconds earlier for a different provider. By incorporating the identity verification in the Blockchain and using hash functions to verify the authenticity of the block content, the costs can be cut down and the timeframe can be reduced significantly.

ADOPTING BLOCKCHAIN TECHNOLOGY

Integration of Blockchain in VerifyUnion

VerifyUnion is the unique solution integrating Decentralized Identity Verification using Blockchain Technology and initiating the transition from the current Centralized Verification Methodology where all the user information is at risk, and the individual is not in control of their personal information.
By distributing a ledger among all members of the network, Blockchain authentication eliminates the possibility of someone maliciously altering the ledger. Every time a 'transaction' or block of data is added to the chain a majority of the network must verify its validity. This guarantees the integrity of the ledger. One could then use public key encryption, such as the extremely secure RSA encryption, to securely send their credentials. The recipient could then verify this against an entry in the immutable Blockchain resulting in an incredibly secure and reliable way to handle verification of identity.

Security of Blockchain



The Blockchain relies on three major pillars, being (1) consensus, (2) distributed, and (3) trust-less, and the security is derived from a proof of work problem. This problem is designed to take a large amount of computational power to complete and thus, for a single person working it may take years. Whereas for a network of computers it may take only minutes. Thus, the chain can be continually added to and transactions are still processed in a timely manner while securing the data from tampering. The nature of this problem makes it mathematically impossible for someone to change the Blockchain. Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain.

Authentication and Identification using Blockchain

New companies have now begun to harness the potential of the Blockchain and develop a variety of services using the technology. The centre of Blockchain authentication would be a Blockchain ID. This ID is essentially a block of data on the chain that can be both verified by any third party and can display necessary information such as date of birth. The secret to this verification is the Elliptic Curve Digital Signature Algorithm (ECDSA). When adding an ID to the Blockchain, an identification issuing service binds a public key by default and then transfers ownership of the private key to the user. This allows the user, and only the user, to sign a signature that can be verified against the public key stored in the Blockchain. This identification of a user would serve as a decentralized source of authentication. It would essentially be a single-sign-on portal that can be accessed by any app while not being owned by any single entity. A protected app would only have to request a digital signature and an ID from a user requesting access. The app could then verify that the signature is valid and that the user's ID verifies who they say they are.

ADOPTING BLOCKCHAIN TECHNOLOGY

Why we need Blockchain?

This is in no small part due to the terrible lack of security in our identification systems. However, switching entirely to this decentralized system is going to be a long process and in the meantime, users need a way to secure their data and identities. This is where multifactor authentication comes in. Without having to scrap contemporary methods of authentication, service providers could enable multi-factor authentication with the Blockchain. This would serve to add an extra layer of security to applications while slowly introducing people to the benefits of the Blockchain. As easy to use as taking a picture, the entire process could be automated, only requiring the user to create an ID and download an app that handles the necessary authentication handshakes. The decentralized nature of the Blockchain could allow the user to manually sign the request and return it, however, for usability one would most likely rely on an app that leverages this technology. Simply take a picture of a QR code that encodes the authentication request and the app would sign the request and return it to the protected app.

Lack of Efficiency in the Current System

There are a few options currently used for two-factor authentication. For example, one of the most common methods is to send a code over SMS. This works, however SMS messages are notoriously insecure. A potential attacker could sniff messages from any number and read them in addition to spoofing the sender of the message. This poses a great problem because if an attacker knows your name and that your account uses text messages as a backup method of authentication, they could find your listed phone numbers online and then intercept those messages, gaining access to whatever code they send. It is easy and ubiquitous but impossible to secure without changing the SMS protocol itself. The other problem with current two-factor authentication is the proprietary nature of the services. Methods such as Google Authenticator are secure and easy to use. However, Google then has access to all your two-factor codes. This option is much more secure but brings back the issue of a single entity owning the authentication data. A breach of Google could cause all your authentication codes to be leaked. The decentralized approach offered by the Blockchain eliminates this problem because the chain is 100% open to the public and no sensitive data is stored in the clear on the Blockchain.

ADOPTING BLOCKCHAIN TECHNOLOGY

APPLY BLOCKCHAIN METHODOLOGY

Handshaking and Hashing

Blockchain ID's are a viable solution to solve the task of verifying that a user is who they say they are. Furthermore, this functionality could be expanded to do a variety of secure data transfers on behalf of an individual. One service deeply linked with identity verification is the sharing of identity information without the disclosure of unnecessary information. In addition to sharing data, a user could also add data to the chain as proof of a transaction, without giving away the original data of the transaction. Either party could verify a document against this entry and show that it is in fact valid, enabling fast and reliable audits of data. This methodology would be based on the principle of message signing and hashing. Many services already use this technology to securely verify data (such as JSON Web Tokens) while not disclosing the original data.

Proposed Method

A generic authentication flow that has been tested and utilized by companies (eg: Blockstack) relies on a Blockchain centred handshake. This 'handshake' verifies to both the authenticating app and the user that the other party they are communicating with who they think it is. In this example, the protected app is the application requesting authentication, and the user is the entity attempting to gain access to the protected app. The first step of this flow is similar to that of any login. However, the user would not be prompted to enter a password. Instead, a user would see a form on the protected app for a username, it will then either display a QR code for authentication or look in its records for the preferred method of authentication. The QR code example would be easier to set up and would simply encode the authentication request from the protected app. This authentication request is the first step of the handshake. The next step is to verify the request and send a response. This step contains many sub-steps to ensure authentication. First, the user would verify that the request data is legitimate and the protected website is who they are expecting. This could be done by using public key cryptography. This would allow the protected app to sign the request, which is then publicly verified either through the Blockchain or a certificate authority. To support simple transitions, it would be reasonable for this to begin with a certificate authority system used in TLS for HTTS. This could however be transitioned into a full Blockchain authentication by creating an application ID on the Blockchain which could then be verified.

After verifying this request, the user would click a button saying verify login. This would then create a response, sign it, and then send it back to a specified route on the protected app. This request would then be verified using public key cryptography on the protected app and the user will be logged in. The benefit of using the Blockchain is that it is completely decentralized. If you didn't want to use an app to facilitate this flow, the user could simply generate their own signature with their public key and submit it in a form, which the website would then verify. This shows the true benefit of a decentralized system. Because anyone can access the data and the user is in control of their private key, then you as a user are not forced to use a given API to facilitate this request. Putting as much trust in the other system as you are willing to give.

ADOPTING BLOCKCHAIN TECHNOLOGY

Current Problem with Sharing Information

A current problem with identity verification is that you are often required to give more information than the requester really needs. If your transaction is compromised and someone can intercept the data in some way, they will have a lot of information to start forging an identity. To solve this problem, the previous authentication flow could be expanded to create a solution.

First the protocol would define a 'permission' set or request for a particular set of data. This 'permission' level would be defined by a common use case. For example, if the system wants to collect credit information, it could send a 'payment' request. Which the user could then see and determine if they want to disclose their credit card information to this vendor. If they trust it, they could sign the request and send a data packet containing the relevant information. If their bank supports Blockchain authentication, they could simply send a signed payment packet that the website could then forward to the bank and complete the transaction, thus preventing the user from giving the vendor any personal information. Otherwise, the data packet could include the relevant financial information such as credit card number etc. However, to prevent fraud, the website could verify that this person is really the owner of the data and they are not using a stolen card. To do this, cryptographic hashing could be used to verify the data. The packet would first be hashed and signed by the user. This would tell the vendor that it is really a given person sending the data. Next, the site would look on the Blockchain for a signed and hashed version of that data. If the hashes match up along with the signatures, the vendor will know that the data is in fact associated with that person and that the data is untampered, giving them reasonable assurance that the card is owned by the authenticated individual.

Problem to Solve

In order to ensure that an ID is really the person that it purports to be, more secure forms of verification would be required than simply using social media posts etc. Either a trusted authority must distribute these IDs or a third party securely audits sensitive documents of the user that can better verify the ID. Therefore, similar to the case of certificate authorities for the TLS protocol, people would have to trust that these authorities are properly vetting these documents. A hash based system could be used to store records of the document used, so someone can verify that a document is for a given identity, however, this document may be sensitive and thus the owner would not want the plaintext to be available on the Blockchain. This introduces the current issue of placing trust in a third party.

ECOSYSTEM IN DEVELOPMENT

Following completion of deployment of the first phase, VerifyUnion will go beyond the normal digital verification terminology and execute the following successive development plans:

1. Initiate Smart Contract development on Ethereum network to create a system where our users can create contracts on pre-defined conditions, execute at a specific time, and incorporate to all our existing Client platforms.

2. Create a unique token for VerifyUnion called the "UC Coin" as an Initial Coin Offering, which we will use for the second phase of development and for our token incentive program by which we pay our users who verify their Identity, and the Evaluators for their services.

3. Transition to a completely Decentralized App (DApp) which allows more power to the user side, keeping ID sharing to themselves to maintain control of the verification process.

Another second phase development is incorporating VerifyUnion as a SaaS to our initial client "Entisy" which is a peer-to-peer market place in six countries in Australasia, Asia and Africa (so far) and worldwide on Virtual Services. We will also use the tokens as the cryptocurrency for all apps developed or co-developed by us which will allow our users to use the currency on multiple platforms and get benefits of verification using the portal at the same time.

VERIFYUNION PROTOTYPE – PROS EXPLAINED

By developing the ecosystem for VerifyUnion, the main benefits are for:

• Users gain total control over the verification process and the data being shared for Trust and Social Identification. The physical data is in the control of the end user, meaning the user gets control of what Identification is being carried out and the purpose of verification. They can use the reward tokens in UC Coin for future verification process or use that as a payment in our ecosystem.

• Government authorities, financial institutions and corporates can use this system whereby user Identification and Trust can be made possible with user authentication in real time in a cost-effective manner.

• Evaluators can benefit by evaluating the identity of a user and getting rewarded in UC Coin tokens, and they can use the Blockchain system to alter the price for evaluation and badging in real time.

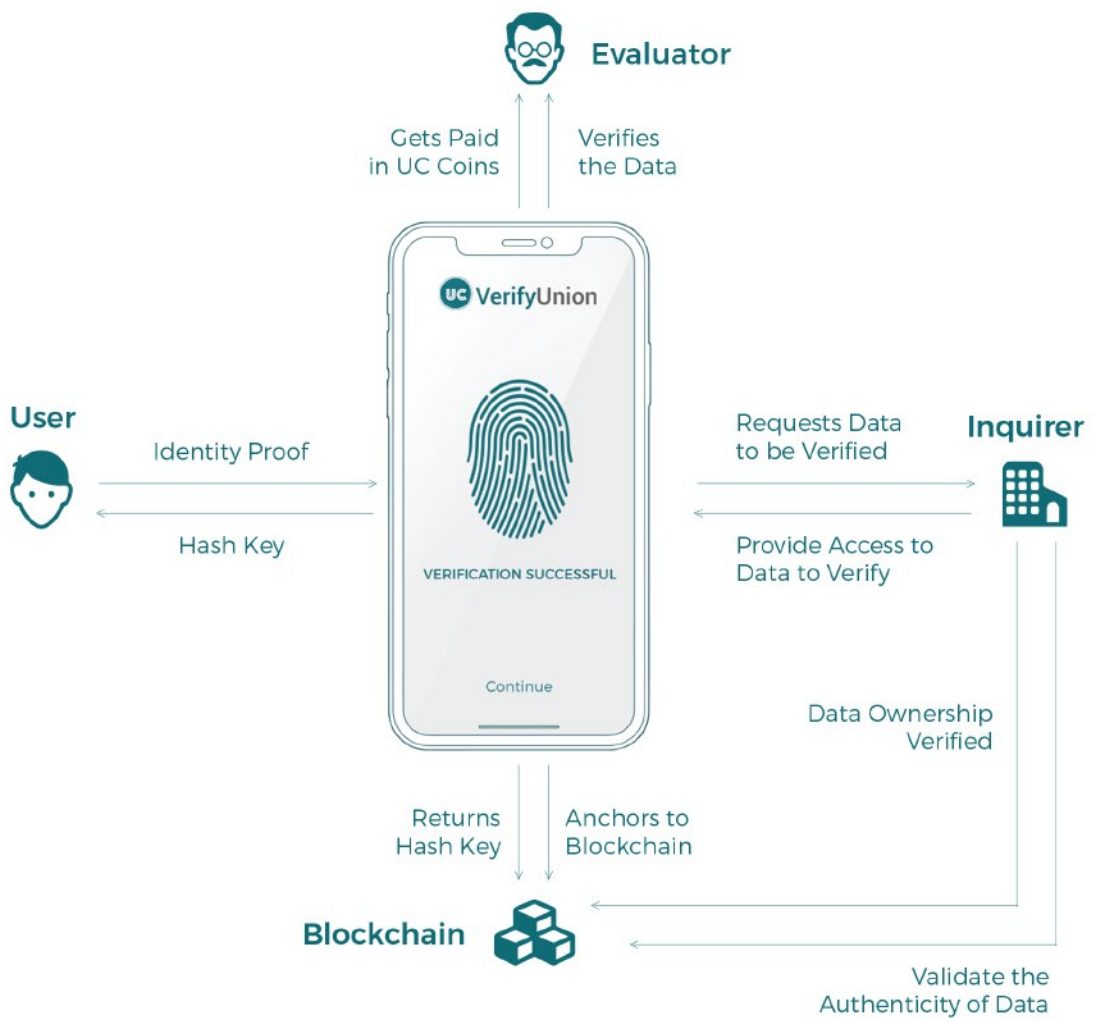
• Service providers who need the verification can get all the required records (after user authentication) in a single platform rather than going to multiple agencies, which reduces their verification costs significantly.

PRODUCT DESCRIPTION

VERIFYUNION PROCEDURE FLOW

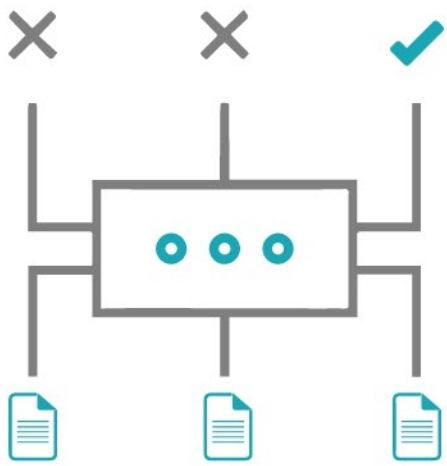
In the first phase, VerifyUnion will be building a hybrid version of a Centralized and Decentralized platform, using Evaluators which are government agencies, central authorities and financial institutions to verify the IDs' (which the user wants to verify) and exchanging incentive tokens (UC Coins) for both Evaluators and users undergoing the process which they can use for future verification activities or sell to release token value.

By using the VerifyUnion mobile app, the user can set Biometric security features and 2FA methods to create the initial layer of security. Then the user reserves the ability to review the information request and decide whether to allow or deny the request, and give only the minimum ID information which is necessary for verification. This method allows the user a real time ID verification using the minimum required documents and a secure method of data transfer.



VerifyUnion works on developing an ecosystem that helps users gain total control. We use the modern methodology of Blockchain protection to provide Verification and Trust Services with the highest level of security possible. By using the VerifyUnion app, users can initiate a verification with the documents stored and verified by "Evaluators" which includes government organizations, officials and financial institutions.

PRODUCT DESCRIPTION



After verifying an identity, a “badge” is given to the user profile which proves that the identity is verified and is added to the Blockchain which we call “anchoring”.
At the next step, authorities who request ID verification such as banks, financial institutions and all agencies who we call “Service Authorities” will reduce their burden of going through independent verification processes. They can rely on the work already done by Evaluators who have added to the Blockchain by requesting authorization from users and using hash functions to get the details from Blockchain. This way a user will know exactly which authority is accessing information and the ways the ID is being used.

The Evaluators can offer their services to authorities who ask for ID verification with user consent, and VerifyUnion rewards both Evaluators and users who verify with our token coin, which they can use for future identification services and all other features within the ecosystem that accept our coins.

The VerifyUnion platform enables real time transactions for Verification and Trust services by using Smart Contracts within the system and enables scalability and robust features for users. The ecosystem will provide control to users, to share required data by user consent. The Evaluators can use Smart Contracts to sell their badging to providers and providers can see the quote range for validation and select the one they prefer to evaluate a user’s identity.

Quotes for validation can be updated by Evaluators in real time which depends on the anchoring time to Blockchain, and will be reflected in the VerifyUnion platform accordingly.

Once the handshake happens between Evaluator and user via a Smart Contract, a transaction is made and data which the user agreed is transferred for verification to the provider seeking verification. The transaction is completed and the Evaluator is paid the price agreed upon in UC Coin and the user is rewarded for their participation with UC Coin, which they can use in our ecosystem and all our partner ecosystems. UC Coin can also be converted to Ethereum and Bitcoin (which will be established in the following phase with VerifyUnion exchange and wallets). The service providers who seek verification will pay VerifyUnion in Fiat Currencies and Cryptocurrencies (if they do not hold UC Coin) which we then use to buy back the UC Coin token coins with which we incentivize Evaluators and Users, from those who want to convert it back to Fiat Currencies or any other cryptocurrency. This will effectively reward the users with more money for verifying their identities. Thus, the demand for the coins becomes greater which means, users can utilize more services using our platform and get more tokens as usage reward, and thereby make money by using our platform.

Users can store their data on personal devices using the VerifyUnion app and optionally can back up to a cloud based or distribution storage platform on individual preference. VerifyUnion will not handle the storage of this form of data, largely due to the significant regulatory implications in multiple jurisdictions of being responsible for Personal Identity information.

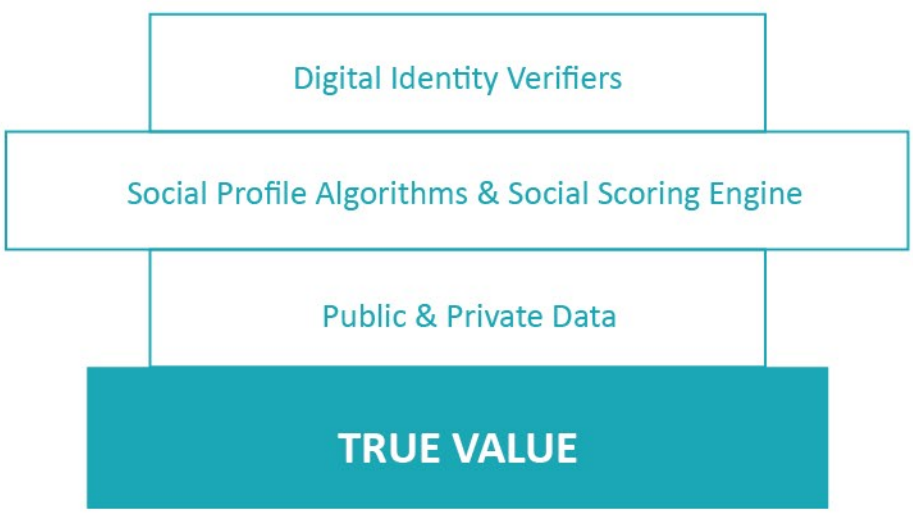
PRODUCT DESCRIPTION

TRUE VALUE PORTFOLIO

The portfolio will include different modules and calculate a “True Value” based on the information that the User wants to provide for the Trust and Verification Services. The portfolio includes a Social Scoring Engine which will link user profile and social data the User shares with the system, and add it to the social score being evaluated. By using more verification services, the User creates a higher value portfolio which they can use for future services in the ecosystem with minimum cost and delay.

Evaluators can analyse the complete portfolio of the User during validation instead of performing repetitive data search, which allows the Users and providers to complete the transaction in minimum time and with enhanced efficiency. This way, the User takes total control over the transaction and can accept or reject requests to share information based on the service user request through the VerifyUnion application.

The Social Score Engine will enable users to use their Public and Private profile accordingly for different verification services. They can complete verification easily by providing references using the VerifyUnion application which allow the Providers to complete and give instant access to the Users. This will remove the delay encountered with conventional verification methods which can take several business days for even minor verifications which shouldn’t require complex procedures and lengthy timeframe.



PRODUCT DESCRIPTION

ANCHORING METHODOLOGY AND MECHANISM

The badging process and anchoring to the Blockchain can be explained in the following elucidation.

• When a user wants to apply for a new service with Service Provider A, the user initiates the request for sending required personal profile information through VerifyUnion app.

• Service Provider A, which acts as the Evaluator, verifies the Identity and Trust for the user using existing methods and creates a social score for the user depending on the data given.

• Provider A hashes the data and the "Social Score" and anchors it to the Blockchain as part of the badging process. Provider A will then transfer the reference number of the Blockchain transaction to the user.

• In the future, when user applies for a service from Provider B, Provider B will request relevant data from the user for the service being provided.

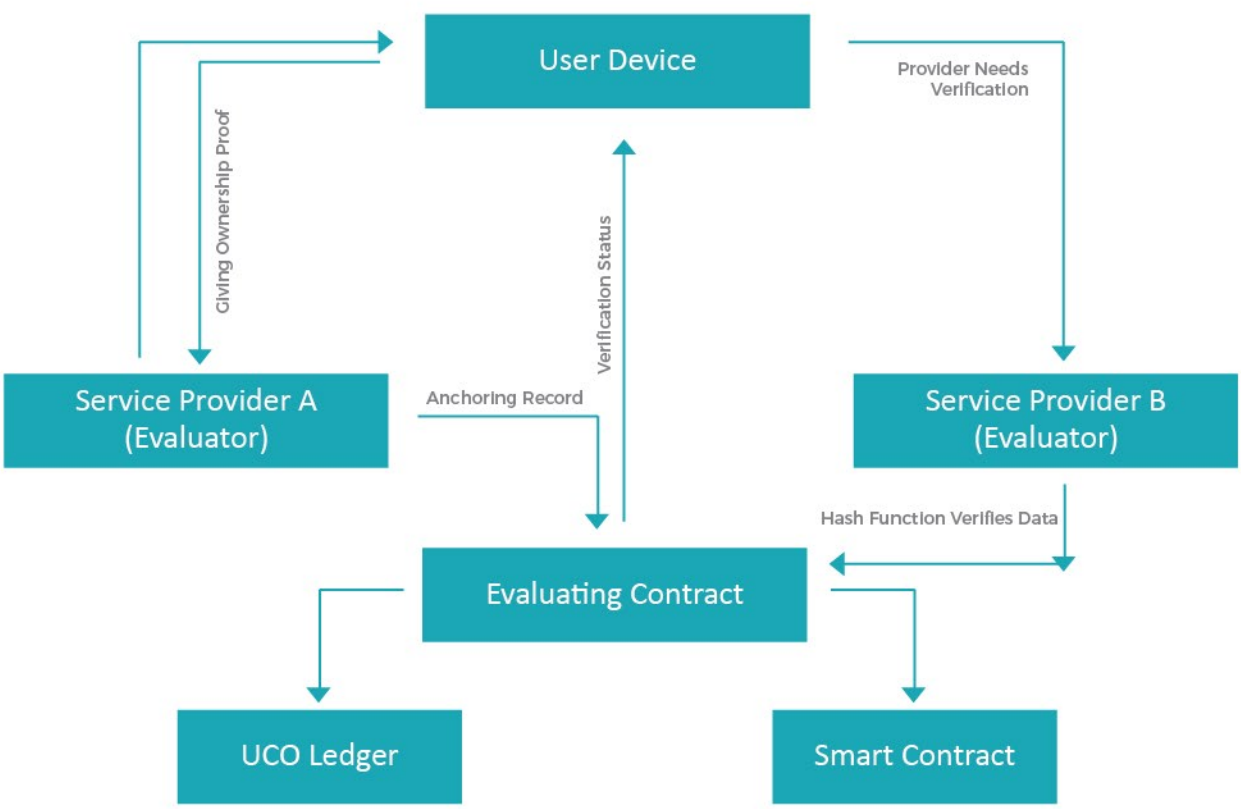
• If the user agrees for the request, Provider B and the user will mutually agree upon an Evaluator who verifies the badging process, let's say it's Provider A. Provider A offers a price in UC Coin for the process which is acceptable to Provider B and agrees with a Smart Contract.

• Provider A will verify user authorization and details of the transaction with the hash key that Provider B wanted to verify on the Blockchain, which was anchored by Provider A previously. Provider B will verify with the hash functions and if it returns the same value, Provider B can verify the user identity and pay the price in UC Coin to Provider A as agreed by the Smart Contract.

• Once the payment in UC Coin is made, the user can release the required data to Provider B, through our App.

• Once the transaction is complete, the user can finish the transaction using the App and then the UC Coin is paid to both user and Evaluator, which is Provider A, for the service provided and both get paid as per the Smart Contract.

ANCHORING METHODOLOGY



SECURITY ENHANCEMENT TO VERIFYUNION

VerifyUnion have added two additional layers on top of Blockchain to ensure the privacy of our users, allowing users to authenticate sharing of personal information.

The two protocols used are:

UNION SMART LATCH

Historically, privacy crises have been caused by perpetrators accessing users' inputs from login fields and by loopholes from service providers. Union Smart Latch layer provides full security by acquiring minimum user information on the login form. When a user is asked to input their email address during Sign Up, Union Smart Latch generates a unique token from our authentication server and delivers it to the user's e-mail. The token is generated once and encrypted by a specific encryption algorithm. Should the token be hacked, the intruder cannot gain access to user information given the static token will fail to match with the dynamic token, then is access is barred.

UNION SMART ENGINE

All client's verification information is encrypted and compressed by the Union Smart Engine, stored on both Blockchain network and our dedicated server. When clients request information from the Blockchain, our dedicated server will find and load that data and run reliable two-way verification. Providing the data is matched, then Union Smart Engine decrypts data and will deliver to the client. Naturally this will enhance the response time and deliver faster results and much better processing times.

SECURITY ENHANCEMENT TO VERIFYUNION

COST OF ATTACK ON BLOCKCHAIN ANCHORING

Let's assume an attacker decides to retroactively modify the anchor on a permissionless cryptocurrency blockchain that utilizes proof of work (e.g., the Bitcoin Blockchain). In order to accomplish this, the attacker would need to overwrite the blockchain starting from the block containing the targeted anchor. According to proof-of-work blockchain consensus rules, the attacker would need to produce an alternative chain of blocks with more cumulative proof of work than that created by honest maintainers. Furthermore, the attacker would need to keep his version of blockchain secret until it becomes preferable to the blockchain generated by the honest part of the network. An ordinary majority attack (e.g., censoring all blocks not generated by the attacker) does not change the blockchain history, hence it would not accomplish the attacker's goals.
Note that the attack would have obvious issues:

• Full nodes would retain the version of the blockchain maintained by the honest miners after the attack. Thus, existing blockchain users (including the users of the anchored blockchain) would be able to verify that the attack took place, significantly diminishing its utility for most use cases (cf. anchoring on printed media, the successful attack on which would necessitate unnoticeably swapping existing printed issues of the medium). The attack itself would require significant amount of preparation, further diminishing the chance to accomplish it covertly.

• Because the attack would be highly noticeable, the attacker would be unlikely to gain profit from selling mined cryptocurrency, as its exchange rate would probably significantly drop after the attack. Hence, it is unlikely that the attack would be supported by rational maintainers on the target blockchain.

Let's assume that the attack begins at the moment t = 0, and the attacked anchor corresponds to t = −ta < 0 (i.e., ta is the anchor age). The honest hashrate and the attacker's hashrate are described by functions g, h : R → [0, +∞) respectively, with the condition ∀t < 0 h(t) = 0. We further assume that h and g are both monotonically non-decreasing: ∀t h˙(t) ≥ 0, g˙(t) ≥ 0.
The initial cumulative difficulty handicap of the attacker's chain is δ=def−ta∫0g(t)dt. The attack ends at the moment τ such that the cumulative difficulty of the attacker's chain reaches that of the honest network, i.e.,

$$\int_0^\tau h(t)\,dt = \delta + \int_0^\tau g(t)\,dt. \tag{1}$$

$$J(h,\tau) = R + Ch(\tau) + O\int_0^\tau h(t)\,dt \to \min \tag{2}$$

SECURITY ENHANCEMENT TO VERIFYUNION

The attack costs consist of three factors:

- R, measured in $, are inelastic capital expenses on the production of hashing equipment
- C, measured in $/(GH/s), are elastic capital expenses of developing, producing and deploying a unit of hashing equipment
- O, measured in $/GH, are operating expenses of maintaining a unit of hashing equipment

Naturally, R, C and O are positive.
Observe that the integral part of (2) can be simplified using (1), resulting in a one-sided optimal control problem for the control h:

$$J = R + O\delta + Ch(\tau) + O\int_0^\tau g(t)\,dt \to \min_{\tau,h} \quad \text{s.t.} \qquad (3)$$
$$\int_0^\tau h(t)\,dt = \delta + \int_0^\tau g(t)\,dt;$$
$$h(0) = 0; \quad \forall t \in (0,\tau) \quad \dot{h}(t) \geq 0.$$

Rather than trying to solve this problem in the generic case (which can be accomplished numerically), we examine a simple partial case.

Assumption 1
h(t) = h ⍰ is constant on the interval (0, τ] (i.e., the attacker starts the attack after an initial equipment procurement and does not increase the amount of the equipment during the attack).
The transition to the constant attacker's hashrate may be justified by the following observation.

Statement 1: The constant attacker's hashrate h(t) = h* is optimal in (3) for any fixed τ .

Proof: Assumption 5 leads to the constraint (1) simplified as

$$h^*\tau = \delta + \int_0^\tau g(t)\,dt,$$

thus yielding

$$J(h^*,\tau) = R + O\delta + C\delta/\tau + (O + C/\tau)\int_0^\tau g(t)\,dt,$$

which is now dependent only on □ and not on *h**.

As *h* is nondecreasing,

$$h(\tau) \models \frac{1}{\tau}\int_0^{\tau} h(\tau)\,dt \geq \frac{1}{\tau}\int_0^{\tau} h(t)\,dt = \frac{\delta}{\tau} + \frac{1}{\tau}\int_0^{\tau} g(t)\,dt. \tag{5}$$

Replacing h( ) in (3) per (5) yields a lower bound estimate $J(h,\tau) \geq J(h^*,\tau)$ with *h** understood as a constant function. $J(h,\tau) = J(h^*,\tau)$ holds iff *h = h**.

Minimizing J in (4) for $\mathcal{T}$, we obtain

$$\frac{\partial J}{\partial \tau} = \left(O + \frac{C}{\tau}\right) g(\tau) - \frac{C}{\tau^2}\left(\delta + \int_0^{\tau} g(t)\,dt\right) = 0. \tag{6}$$

Statement 2: If g(t) is continuous, Equation (6) has the only solution on the interval $\tau \in (0, +\infty)$

Proof:

$$\lim_{\tau \to +0} \frac{\partial J(\tau)}{\partial \tau} = Og(0) + \lim_{\tau \to +0}\left(\frac{Cg(0)}{\tau} - \frac{C\delta}{\tau^2}\right) = -\infty.$$

As *g(t)* is a nondecreasing function,

$$\frac{\partial J(\tau)}{\partial \tau} \geq \left(O + \frac{C}{\tau}\right) g(\tau) - \frac{C}{\tau^2}\left(\delta + \int_0^{\tau} g(\tau)\,dt\right) = Og(\tau) - \frac{C\delta}{\tau^2} > 0 \text{ with } \tau \to +\infty.$$

Hence, $\partial J/\partial \tau$ has different signs on the ends of the explored interval, and since it is a continuous function, there is at least one point $\mathcal{T}$, at which $\partial J(\tau)/\partial \tau = 0$.

Next, observe that (6) has the same solutions on $\tau \in (0, +\infty)$ as the equation.

$$\tau^2 \frac{\partial J}{\partial \tau} \equiv O\tau^2 g(\tau) + C\tau g(\tau) - C\delta - C\int_0^{\tau} g(t)\,dt = 0. \tag{7}$$

Differentiate the left part of (7) for $\mathcal{T}$

$$\frac{\partial}{\partial \tau}\left(\tau^2 \frac{\partial J}{\partial \tau}\right) = \left(O\tau^2 + C\tau\right)\frac{\partial g(\tau)}{\partial \tau} + 2O\tau g(\tau) > 0 \quad \forall \tau \geq 0,$$

because $\partial g/\partial \tau \geq 0,$, and $g(\tau) > 0$. Hence, the left part of (7) monotonically increases meaning that (7) and (6) may have no more than a single solution. This completes the proof.

Consider the simplest instantiation of the honest hashrate function *g(t)*: constant *g(t) = g0* for all *t*; in this case, the initial handicap of the attacker's chain $\delta = g_0 t_a$. Equation (6) is simplified as

$$\left(O + \frac{C}{\tau}\right) g_0 - \frac{C(\delta + g_0\tau)}{\tau^2} = 0,$$

from which the optimal attack duration $\tau^* = \sqrt{C\delta/Og_0},$ and the optimal expenses

$$J^* = \underbrace{R + O\delta + Cg_0}_{J_0} + \underbrace{2\sqrt{O\delta \cdot Cg_0}}_{J_{const}}.$$

A part of expenses J_0 can be viewed as the costs spent on anchor security by the honest miners by the time *t = 0,* and J_{const} is the additional penalty. A much-desired property is that Jconst can be comparable to J_0 , i.e., costs spent on securing the anchor are significantly less than the costs to attack it (Fig. 1).

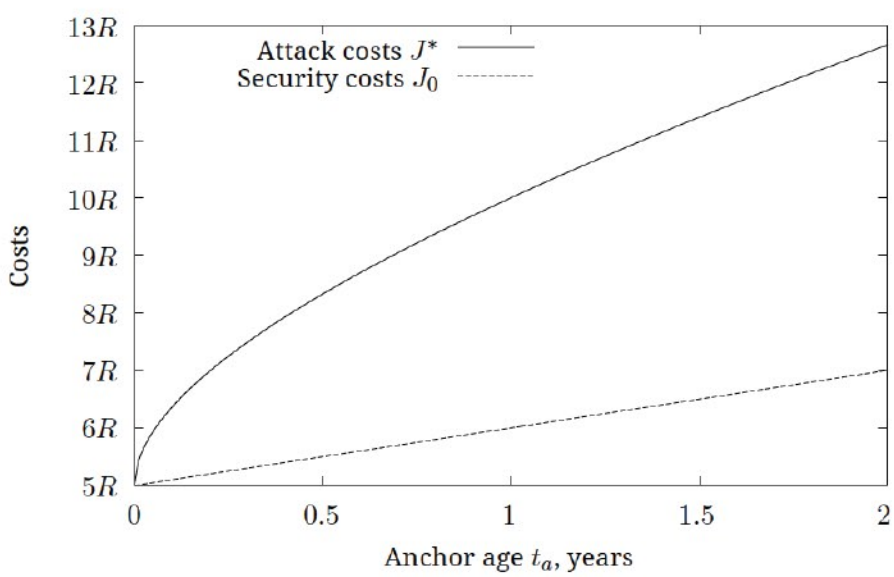


Figure 1: Costs to attack anchoring on a blockchain with the static honest hashrate g_0 depending on the anchor age t_a. It is assumed that the cost factors in (2) $R = Og_0 \cdot 1 \text{ year} = Cg_0/4,$ which is by our estimations close to the current distribution of the factors for the Bitcoin Blockchain.

TOKEN DESCRIPTION

"UC Coin" – The Crypto for VerifyUnion

VerifyUnion are deploying our own token which can be applied in our ecosystem. UC Coin serves as a mode of payment in the VerifyUnion platform and it is used in the reward program to pay our Evaluators and users. This is defined by the Smart Contract that is predefined and agreed upon by both user and Evaluator, which is addressed by the Consensus of the VerifyUnion participants.

In the next phase of development, VerifyUnion plans to expand its services and when the demand for the token increases, resulting in a higher value of the token, users can then sell the tokens back to us for a premium which benefits the user side.

A fixed amount of UC Coin will be created during the initial token issue, and we keep a ledger for recording every transfer of UC Coin between participants using Smart Contracts and Blockchain methodology. Using UC Coin across multiple platforms in the ecosystem, will allow us to safeguard against the deterioration of value of the token due to the utility of the token in a wide ecosystem. The reward program will increase the value of token by rewarding all the participants at the same time and the value of incentives increase in tandem with the growth of the ecosystem.

A new user referral program is also included in the ecosystem where existing users can refer others to earn token and new users can verify their profile and earn more tokens.

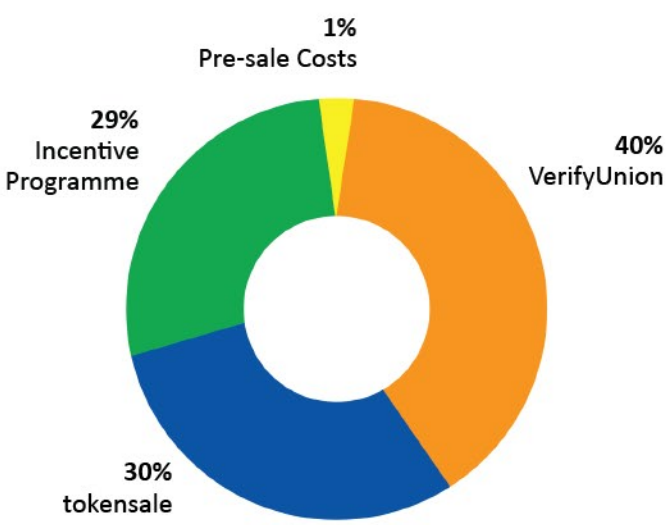
TOKEN SALE TERMS

TOTAL COINS:500M UCN

- 1% used for pre-sale costs
- 30% are sold in tokensale
- 29% are allocated for Incentive Programme
- 40% are retained by VerifyUnion

Storage of Tokensale funds

ETH will be stored in a multi-sig wallet



CAP = $30 MILLION USD

Normal Token cost (Bonus coins will reduce unit price)

1 UCN = $0.1948 USD (approx.)

(Bonus added on top depending upon the phase of purchase)

1 ETH = 1540 UCN (approx.)

CONCLUSION

VerifyUnion aims to eliminate Digital Identity Fraud for our clients and users by deploying a new system which is cost effective and benefits both clients and end users in authenticating Verification and Trust when using digital services. VerifyUnion will remove unwanted storage of Personal User data which is being used in fraudulent activities and remove reliance on any centralized system which has significant exposure to the threat of hacking. Service Providers can reduce the cost in terms of money and time of verifying everyone for every service they provide by using the VerifyUnion platform. End users will be incentivized with tokens to use the portal at the same time being verified for all online and digital services, and can use the token as an investment which can be paid out later or can be spent in our ecosystem.

Users gain total control of the end to end process they are undergoing, and can enhance trust in all the services they are receiving. They will increase their trust verification using our social score and earn more tokens at the same time. By having the total portfolio of users, providers can get a wider picture and grant more services which the user requests since more trusted information about the user is available.

The rate of online fraud will be reduced significantly through VerifyUnion given user hash functions and proof of ownership are also verified through this process, and users can authorize all the information they want to be verified to increase trust and social score. The current problem of ID spoofing and having various social profiles which makes fraud easy will reduce significantly as it makes it very difficult to bypass the system.

COMPANY

LEGAL STRUCTURE

VerifyUnion Pte. Ltd. (201726332G) is registered in Singapore.

NETWORK PARTICIPANTS

Token Holders (Global, open to everyone in compliance with their local laws and regulations)

The VerifyUnion Foundation is in charge of the overall management, all tokens, contributions, and other revenue flows and oversight to keep the VerifyUnion network in good health. Currently its board members include the directors of the VerifyUnion operating company.

VerifyUnion.io Pte. Ltd. is the operating entity that will be contracted by the foundation to build and deploy the core decentralized application.

CONTACT

VerifyUnion Pte. Ltd. (201726332G)

Email: info@VerifyUnion.com

101 Cecil Street, #11-04, Tong Eng Building, Singapore 069533

Web: https://www.VerifyUnion.io

TEAM

MANAGEMENT TEAM

AJ SMITH- CEO

AJ Smith is a Business Strategist, Mentor, Serial-Entrepreneur, VC, Marketing Specialist, Fintech experienced and driven CEO continuously winning high levels of business within a competitive market place. He founded more than 20 successful businesses in his lifetime and has created employment for thousands of people. He is also the co-founder of New Zealand based tech companies Imperial Digital and Entisy, while investing in more than 12 global start-ups (mostly in fintech). He has a passion for Cryptocurrency, Blockchain and Fintech and is frequently invited to be a panellist for seminars. He has "retired" twice in his life and always made it back in business for the passion of the next successful venture.

KERRY FRIEND- CFO

Kerry Friend is an accomplished Senior Executive with a strong CFO background and demonstrated commercial acumen and leadership skills, who has recently returned to New Zealand after over 18 years working in Asia.
His most recent employment role saw him establish from scratch and grow over eight years a significant Asia region-wide business operation for a listed US entertainment software company, based in Singapore. Prior to that he controlled finances for a US$1 billion multi-channel TV joint venture of a major US media group in Japan.

Chartered Accountant (Australia & NZ)
Member, Institute of Directors (NZ)

TEAM

TECHNICAL TEAM

SEUNG HYUN MYUNG
CTO
Blockchain Engineer

KWANGKUE AN
Software Engineer
Blockchain Engineer

THILAN PATHIRAGE
Software Engineer

SHRUTIKA SHEDHA
Graphic/UI Designer

AISHA HANIF
Software Engineer

NARAYANA REDDY
3D Artist

ZEESHAN NAVEED
Digital Specialist

TIM ATAMBAY
Software Engineer

TEAM

ADVISORY TEAM

LEANNE GRAHAM- ex-Xero Rainmaker / SaaS Expert

One of New Zealand's few female IT entrepreneurs and CEOs of a NZX company. Previous Country Manager for Xero, propelling Xero from a newcomer cloud product to becoming the global accounting software standard. Board positions: Velpic – Chair, Cognitives – Chair and these advisory board roles: Nibo (Brazil) – Cloud Accounting, Anfix (Spain) - Cloud Accounting, Yudoozy (NZ) Freelance Platform, Big - (Australia) Video Platform.

NICK FITNESS- Financial Analyst

Nick is an Investment Advisor, Stockbroker and Investor. With over 10 years of experience with top tier investment banks (Forsyth Barr, Macquarie & Morgan Stanley), both in the UK and New Zealand. He is an Authorised Financial Adviser (2012), and accredited NZX Associate Advisor (2013). Nick has also been a member of New Zealand Leaders, mentoring leading businesses and start-ups seeking knowledge, networks and capital to grow.

GREG SHARP- IT Security Engineer

Greg Sharp has spent 23 years in the IT Industry both in the UK and in New Zealand, is a CISSP qualified IT security engineer and currently is the Managing Director of Base 2 located in Auckland, New Zealand.

ROGIN THADATHIL- ICT Business Analyst

Rogin is an ICT Business Analyst focusing on Blockchain based fintech. He holds a Master's degree in Corporate Finance and Strategic Banking from Massey University (2016). After Graduating with high honours as a Software Systems Engineer, his vision to merge the possibilities of Technology into Finance paved him the way to create new Financial elements and advance as a Financial Engineer.

PARTNERS

Alpha Testing Partner

Blockchain Development Partner

Security Partner

SOCIAL MEDIA

Open and transparent mutual communication is critical to the success of the VerifyUnion Crowdsale, as well as the ongoing advancement of the venture.
Your questions and suggestions are welcomed at the following locations:

REFERENCES

• Ethereum White Paper - http://www.the-blockchain.com/docs/Ethereum_white_paper-a_nex-t_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

• Ethereum Project – Ethereum.org/

• Mining? What Is Bitcoin. "What Is Proof of Work." Everything You Need to Know about Bitcoin Mining - 18 June 2015 - 09 Dec 2016.

• Blockstack. "Blockchain Auth" GitHub - 04 Dec 2016.

• Application of the Blockchain For Authentication and Verification of Identity Ben Cresitello-Dittmar. November 30, 2016

• The value of digital identity to the financial service sector - Bryn Robinson-Morgan, December 2016

• Investigating challenges in digital identity - report written by Gary Simpson & Emma Lindley south Yorkshire credit union & innovate identity

• The digital identity dilemma - recode.net/2016/8/10/12413592/digital-identity-virtual-id-card-fido-web-api

• Establishing digital identity causing problems as users giving away too much - Ian Grayson: Oct 4, 2016

• How Safe Are Blockchains? It Depends. Allison Berke - March 07, 2017

• Are Concerns About Security and Privacy Threatening the Future of Online Commerce? - Mihaela Paun : Jun 02, 2016

• Digital Identity Issue Analysis Report v1.6 - 8th June 2016

• Identity fraud up by 57% as thieves 'hunt' on social media http://www.bbc.com/news/uk-36701297