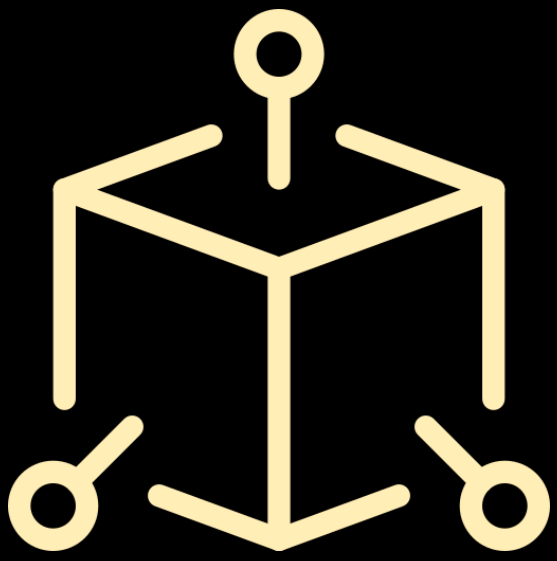


Verification-as-a-Utility Business Model

Blockchain based digital verification

WHITE PAPER

EDITORS

Arianna Trozze
Maya Bhatti

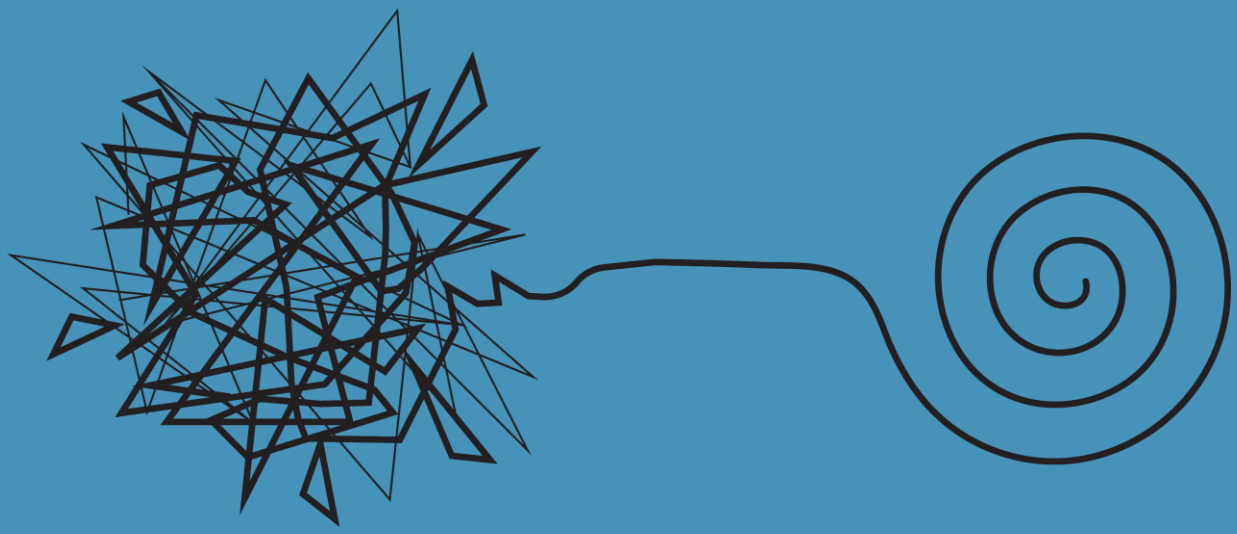
DATE

July 2020

VERSION

2.0

infoeaze



Abstract

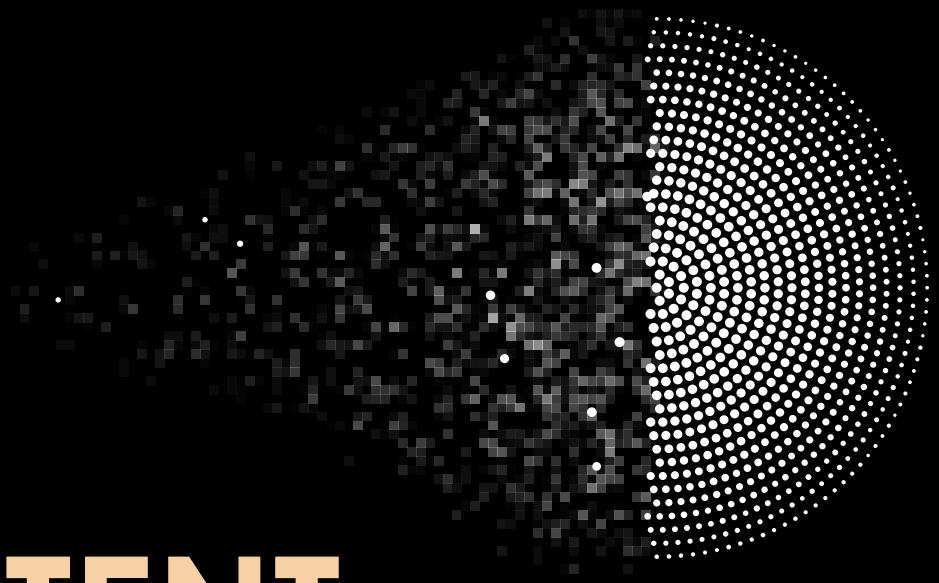
The background check system is broken. The big incumbent verification providers that drive the ecosystem enjoy huge revenue gains but fail to take a human-centred design approach and fall short on user experience. While they use digital capabilities such as machine learning and data lakes to generate insights—with a focus on reducing verification turnaround time, accuracy and quality of service—none of the providers have gone far enough to change the core initiation and execution of the verification process across the value chain. Users face poor experience and at times incur privacy violations and data errors with no visibility or even awareness of these underlying issues.

By 2026, the global verification business is expected to reach $7.64 billion [1]. This is a high-growth market that requires fundamental change. Users are slowly recognising the value of their data and favouring business that are not only fit for digital world, but also conduct business in an ethical and equitable manner. Hiring organisations face increasing risks due to the length of the verification cycle. Furthermore, in 9 out of 10 cases, there is no way to verify a candidate's past experience with start-ups. Former employers must spend human and temporal resources answering hiring organisations' queries to verify work experience claims, meaning money is being spent on employees who no longer work for the business.

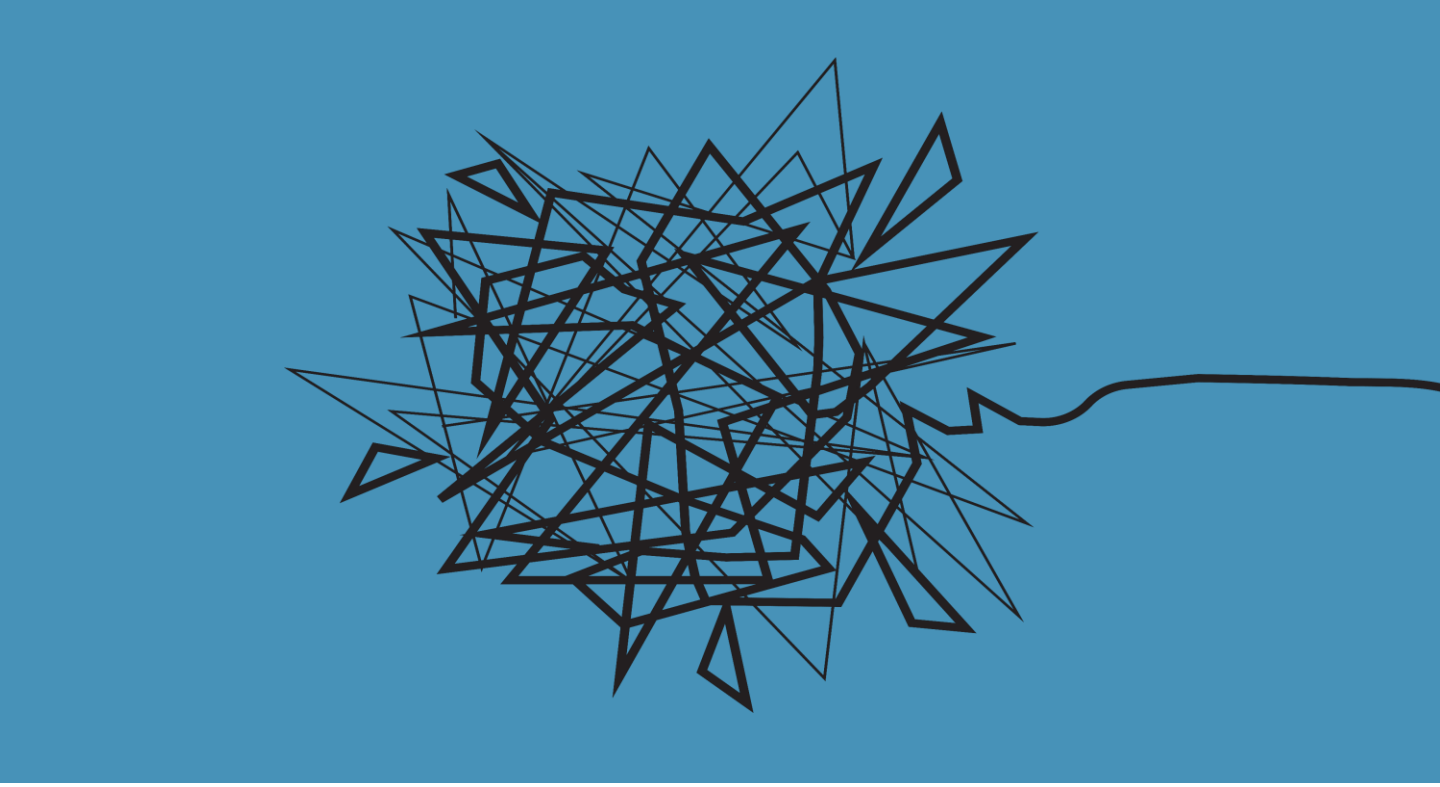
The solution to these problems is a decentralised, self-sovereign and transparent Verification-as-a-Utility digital service—a service where reward-based tokens are issued via blockchain to past employers and users who share their data for verification.

Consent is a Verification-as-a-Utility service platform that incorporates all of this and more. The first component is the **Consent Portal**, a free, open-source, consent-focused platform that issues self-verifiable certificates, removing the need for hiring organisations to contact past employers. Apart from removing the cost incurred by past employers to prove any prior employee's experience, the platform rewards past employers for their participation in the consent-respecting ecosystem. The second core component, the **Consent Wallet**, is available to credential holders. It uses the **Consent Token** both as a mode of payment and for reward allocation, rewarding credential holders who use the Consent Wallet to store, share, manage and transfer verified credentials.

Self-sovereign identity is at the core of the Consent Token and associated technologies, thereby solving the important problem of monetizing personal data while protecting users' privacy by giving them control of their personal data.



CONTENT



1. Introduction

Background verification is meant to be the final step taken by hiring organisations to ensure a sound hiring decision, while controlling, managing and mitigating risk. For many organisations, a background check carried out by a background verification provider provides this **assurance**.

In practice, the verification process may take weeks and, at times, the full results of verification checks are available only after an employee has commenced employment. Most employers continue to risk hiring fraudulent candidates despite employing the verification process to mitigate this risk.

The background verification market is rife with middlemen and complexity. Companies have introduced a host of correlated problems for past employers and hiring organisations and users. Users have lost their privacy, face data errors and endure repeated, painful and slow cycles of filling out forms about their previous employment experience. Background verification companies repeatedly request for same information, do not share candidate data with other background verification agencies and carry out expensive KYC checks each time they receive a new verification request. Users have further lost trust in both private and governmental institutions, as identity theft and fraud continue to skyrocket due to increased cybercrime activity.

This white paper will review the current state of verification and highlight current challenges all stakeholders face in the background verification ecosystem. It will outline a new solution that creates a human-centered, transparent and efficient digital verification for past employers, users/holders of credentials, and hiring employers (including background verification providers), accurately valuing and rewarding the stakeholders within the ecosystem—i.e. built on consent-respecting behaviour and practices.

1.1An Inefficient and Broken Market

To explain the inherent inefficiency in the market, we consider the **sample scenario** depicted below.

In this scenario, the two fictional background verification companies, VeriCheck and EasyCheck, both have contacted Mr Rohit's university and his previous employer at different times to complete his background check. In this process, both the background verification companies incurred a total cost of $100 and, most importantly, spent 30 days to repeatedly contact the source to fulfil the verification. If Mr Rohit switches job 15 times in his lifetime, same process will be repeated by the same or other background verification companies.

This scenario highlights the following inefficiencies:

1. Background Verification companies (BGVs) repeatedly incur **long Turnaround Times** (TAT), thus creating risk for the hiring company that seeks Rohit's background check.
2. BGVs **continue to incur costs** from Mr Rohit's background checks that they already carried out for a different employer.
3. The companies contacted by background verification companies to verify Rohit's employment credentials will receive multiple calls **requesting for same information**. This means Mr Rohits's previous employer will incur the cost of having a dedicated resource to answer queries around Mr Rohit's employment credentials, even though Rohit is no longer an employee.
4. BGVs do not have access to Mr Rohit's **previously verified records**, nor do they usually have a mechanism to store and share previously verified credentials. This is true even if there is an opportunity for one background verification company to share details with another.
5. The verification process frustrates the hiring companies and the job seeker, Mr Rohit, as he must undergo the **same cycle repeatedly**. This also creates room for errors in the data shared for verification.

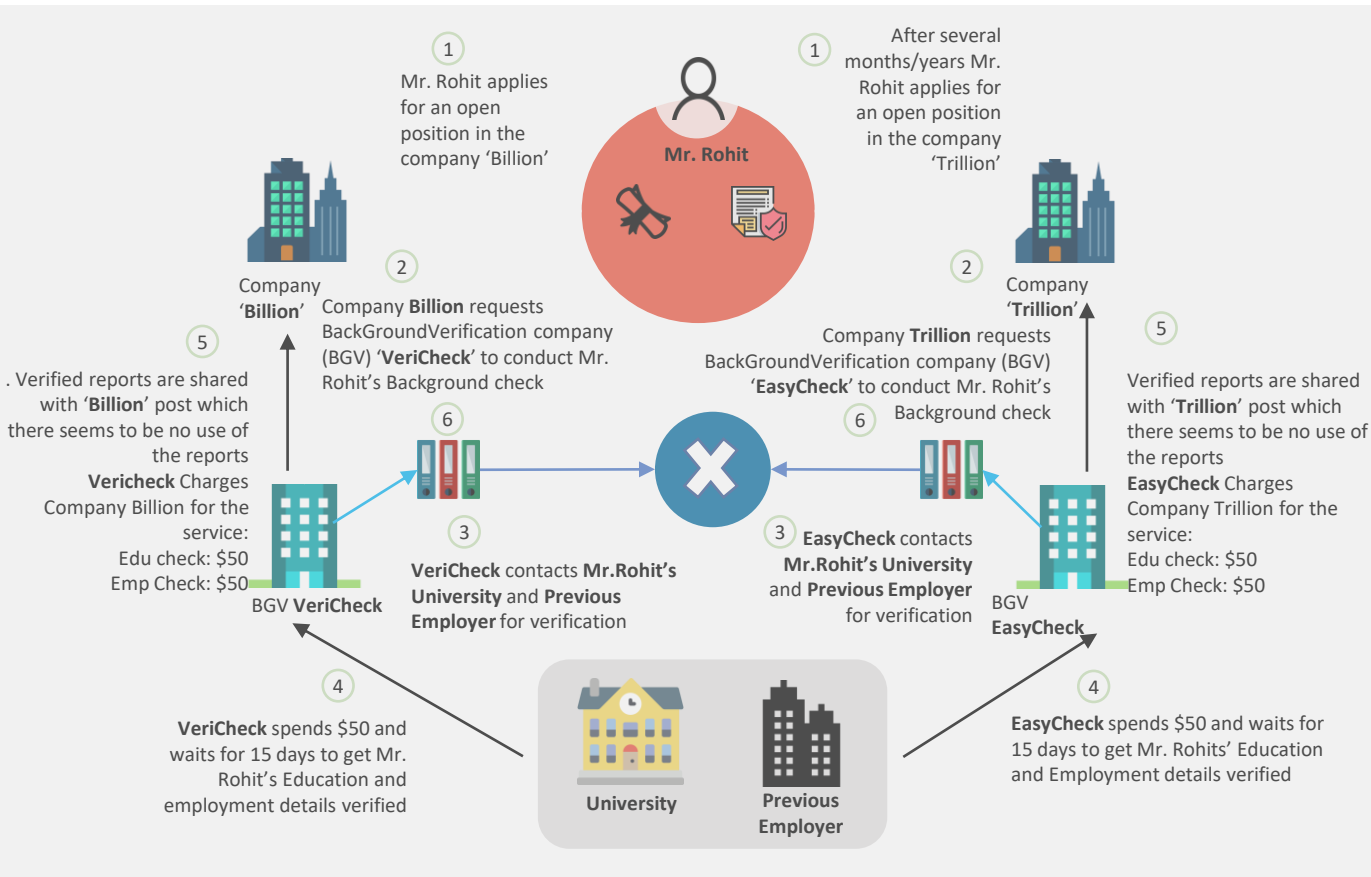


Figure 1: Sample Scenario to explain current verification system

ISSUES

The below three tables depict some of the most common scenarios (with fictional names and contacts) that lead to a data breach, non-compliance and/or incorrect record keeping within the background verification cycle. These issues are usually invisible to the user who shares his/her personal information and are seldom transparently reported to any regulator. This delays TAT which, in turn, delays the hiring process. There are also direct reputational and cost implications for the verification provider. Finally, the user experience is unpleasant and, at its worst, causes users further distress during their job search.

DATA BREACHES		BIGGEST CHALLENGES		
Cases	**Scenarios**	**Delay in TAT**	**Business Impact**	**Bad Stakeholder Experience**
Correct ex-employer, incorrect region	Verification request was supposed to be sent to past employer, ShippingCo in Hong Kong, but the request was incorrectly sent to their Singapore office (hk@ShippingCo.com vs. sg@ShippingCo.com).	✔	✔	✔
Incorrect ex-employer	Verification request was supposed to be sent to past employer Metrostore (hr@metrostore.com) but was incorrectly sent to Easystore (hr@easystore.com) as the email address is similar.	✔	✔	✔
Correct ex-employer, incorrect email	Verification request was supposed to be sent to authorised and secure email address (vivin@bigstore.com) but was incorrectly sent to HR's generic email (hr@bigstore.com).	✔	✔	✔
Incorrect applicant chosen	Verification request was supposed to be sent to Beststore.co for Rohit but the request was sent for Ravi.	✔	✔	✔
Incorrect upload of personal information on client portal	Verification was done for Mr Rohit but BGV team uploaded all the verification details including the personal information of Mr Rahul on Mr Rohit's upload section of client portal.	✔	✔	✔

COMPLIANCE ISSUES		BIGGEST CHALLENGES		
Cases	**Scenarios**	**Delay in TAT**	**Business Impact**	**Bad Stakeholder Experience**
Current employment issues	Candidate does not want his potential employer, Bigstore, to be disclosed to his ex- or current employer, Metrostore, but the BGV team reveals it. The BGV team had sent a verification request to Metrostore which had his potential employer's name on It.	✔	✔	✔
Incorrect verification template	BGV sent the education verification template instead of employment template, leading to re-verification and repeated contact of the ex-employer.	✔	✔	✔
Incorrect closure of verification check	Verification check was supposed to be closed as "verified clear" but was incorrectly closed as "verified major discrepancy".	✔	✔	✔
Delay in processing checks	Verification checks were not initiated on time, delaying follow-ups and missing closures (*specific checks were supposed to be initiated on Thursdays but were not, thus delaying verification by another week*).	✔	✔	✔
Failure to refer to the client's mandatory documents before initiating request to ex-employer	Rohit has a verification template requiring his salary to be verified and disclosed to his ex-employer but BGV failed to disclose his salary. His salary was not verified by his ex-employer which led to re-opening the check. The ex-employer had to be contacted again for the salary to be verified.	✔	✔	✔

INCORRECT RECORD KEEPING		BIGGEST CHALLENGES		
Cases	**Scenarios**	**Delay in TAT**	**Business Impact**	**Bad Stakeholder Experience**
Contact list not up to date	Bigstore has informed the BGV about their new email address (hr@bigstore.com) meant for verification but the verification team failed to circulate the info and did not update the contact list. The team sends the request to Bigstore to the old, inactive email address (oldifhr@bigstore.com).	✔	✔	✔
Unnecessary candidate chasing	BGV was supposed to exhaust all search engines to track the contact details of the candidate's ex-employer (*for new initiation*) but the verification team placed the check on hold, leading to them contacting the candidate for his/her ex-employer's contact details which were easily available from a Google search.	✔	✔	✔
Contact list not referred	Bigstore stated that it will not accept any verification request from a specific BGV anymore, but the updated contact list was not referred, and a request was still sent to Bigstore requesting verification.	✔	✔	✔
Multiple contacts	The verification team failed to ask the ex-employer all the required questions at once, leading to them contacting the ex-employer more than once.	✔	✔	✔
Incomplete documentation	All the email audit trails pertaining to a verification request were not uploaded on the client database by the BGV team, yet the check was closed. Client requests for the check to be re-opened.	✔	✔	✔

In addition to problems caused by the BGVs, candidates and ex-employers often make mistakes which lead to data breaches, non-compliance and/or incorrect record keeping. Furthermore, these issues are usually beyond the scope for process improvement by the background verification providers. We conclude this section with two tables depicting some of the most common scenarios (with fictional names and contacts) involving candidate and ex-employer errors.

CANDIDATE			BIGGEST CHALLENGES		
Category	**Cases**	**Scenario**	**Delay in TAT**	**Business Impact**	**Bad Stakeholder Experience**
Fake certificate	Incorrect documents	Candidate uploads incorrect education or employment certificate.	✔	✔	✔
Compliance issues	Delayed candidate response	Issuing organisation may require additional information or phone authorisation to comply with verification request; however, candidate fails to respond on time or fails to provide required documents.	✔	✔	✔
Compliance issues	Failure to declare all mandatory information	Candidate fails to declare mandatory information on the BGV form which is crucial for the verification process.	✔	✔	✔
Compliance issues	Incomplete document	Delay in providing letter of authorisation to conduct verification.	✔	✔	✔

EX-EMPLOYER			BIGGEST CHALLENGES		
Category	**Cases**	**Scenario**	**Delay in TAT**	**Business Impact**	**Bad Stakeholder Experience**
Compliance issues	Regulations of ex-employer & hiring employer clashes	Hiring employer is requesting for 9 questions to be verified but ex-employer verifies only 5 as per its internal policy.	✔	✔	✔
Compliance issues	Regulations of ex-employer & hiring employer clashes	Hiring employer and ex-employer have different standard verification templates.	✔	✔	✔
Compliance issues	Regulations of ex-employer & hiring employer clashes	Potential employer's request for re-verification denied by ex-employer.	✔	✔	✔
Compliance issues	Regulations of ex-employer & hiring employer clashes	Ex-employer requests that candidate calls the verifier directly to conduct verification and will not reply to requests from the BGV.	✔	✔	✔
Insufficient record keeping	Lack of records	Ex-employer does not maintain records beyond a certain period.	✔	✔	✔
Lack of response	Unable to contact	Universities and organisations are closed for public holidays.	✔	✔	✔
Outdated record keeping	Ex-employer did not notify about secondary person of contact	Ex-employer fails to inform BGV of contact temporarily processing verification requests.	✔	✔	✔
Lost records	Data-related mishaps	Records lost due to fire, natural disaster or cyber hack.	✔	✔	✔
Incorrect verification received	Incorrect response from ex-employer	Ex-employer was supposed to send verified request for Mr Rohit but instead sent Mr Raj's credentials, delaying the process.	✔	✔	✔
Data breach	Ex-employer failed to provide updated point of contact	Ex-employer failed to notify BGV that the previous point of contact is no longer associated with the organisation and a new contact will process verification requests.	✔	✔	✔
Data breach	Ex-employer sent request to incorrect BGV	Ex-employer sent the verified credentials to the incorrect BGV (sending the verified response to xxx@bgv1.com instead of to to yyy@bgv2.com).	✔	✔	✔
TAT clashes	Mismatch in ex-employer's and potential employer's TAT	Potential employer's TAT to close verification is 15 days but the ex-employer's standard TAT is greater than 15 days.	✔	✔	✔

CIRCLE OF PAIN

IN BACKGROUND VERIFICATION

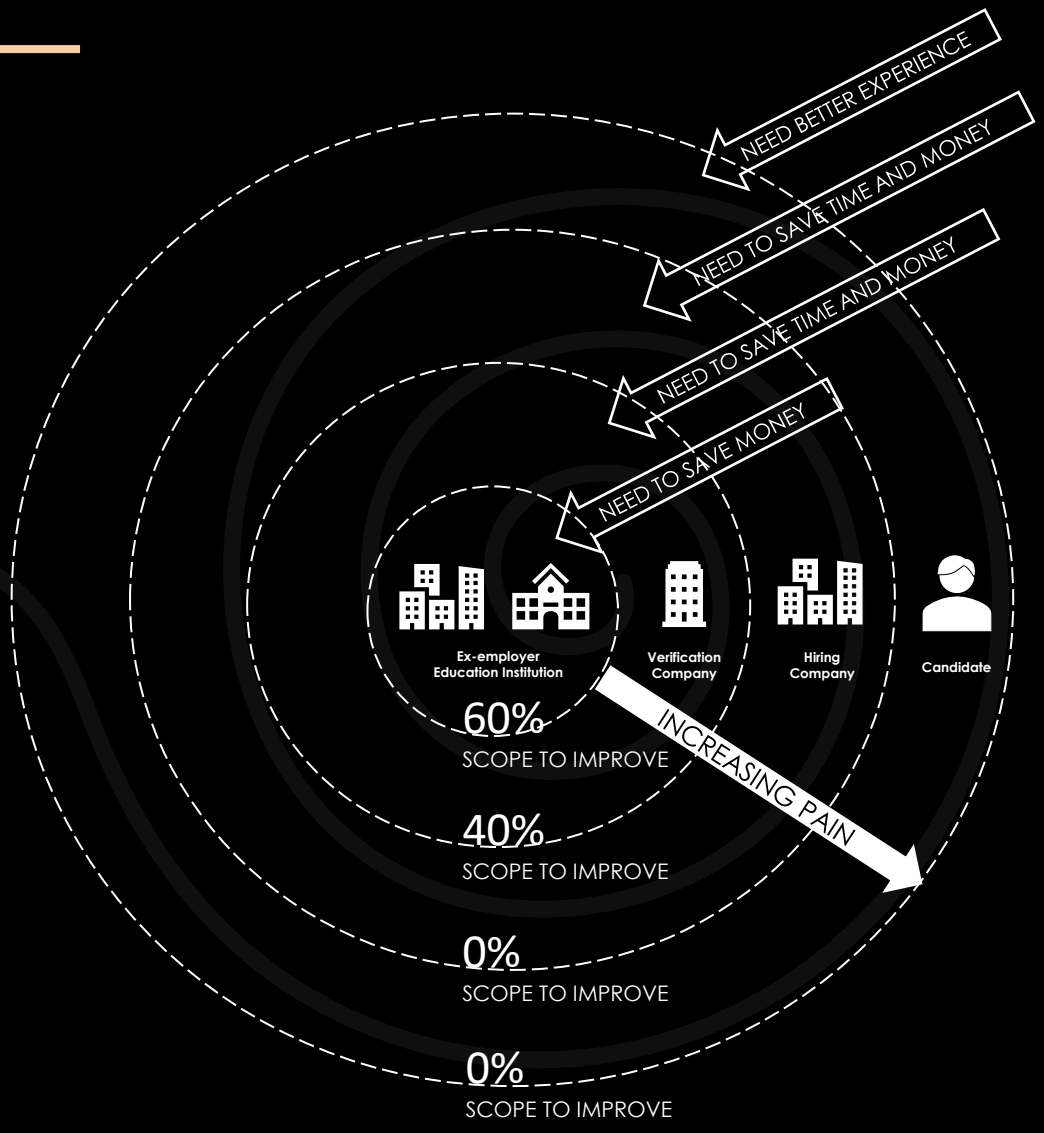
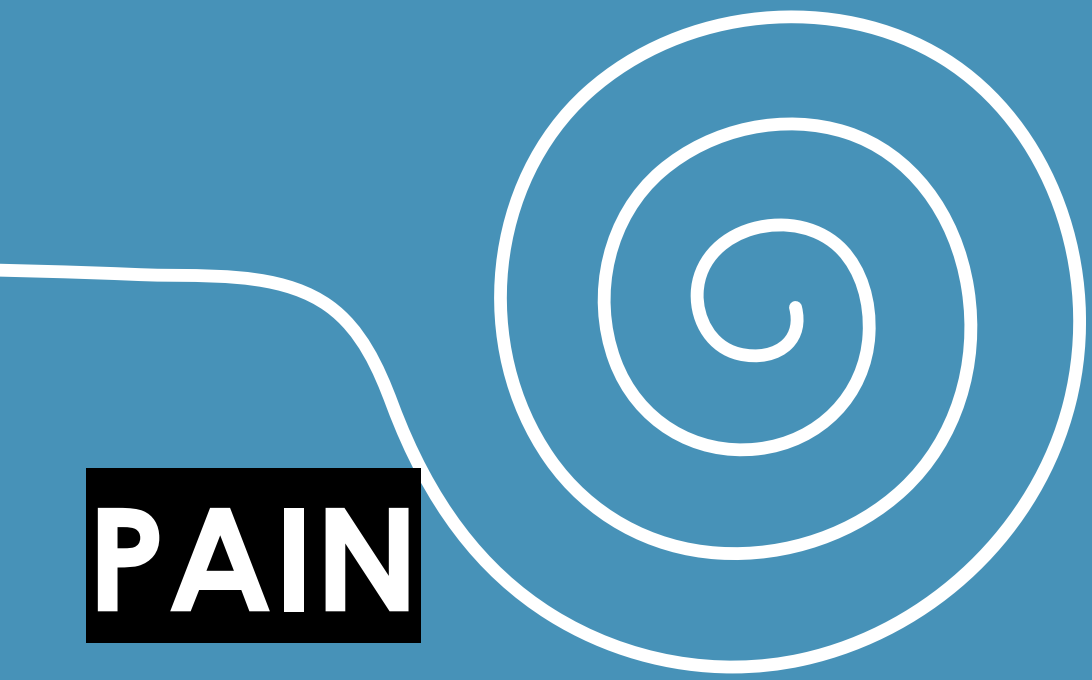


Figure 2: Circle of Pain within the Verification Ecosystem



The cases depicted above are anonymised versions of actual occurrences in the verification industry today. These incidents can be directly attributed to internal training, policies, standards, change management, software systems, data quality and operations team structures. The more manual the verification process, the higher the probability of such a scenario occurring. Solving the above-listed pain points around data breaches, non-compliance, incorrect record keeping, etc. yields a maximum of 40% efficiency for background verification providers. The key opportunity for improvement lies with past employers, including how past employers chose to accept, process and verify claims on past employment; the scope for improvement is close to 60% (Based on Infoeaze internal Analysis).

The diagram on page eight, "**CIRCLE OF PAIN**" depicts the key pain points by various stakeholders within the ecosystem and the scope to improve which is in their control. The diagram also highlights the key incentive expected by stakeholders for change (*i.e. save money, time, etc*).

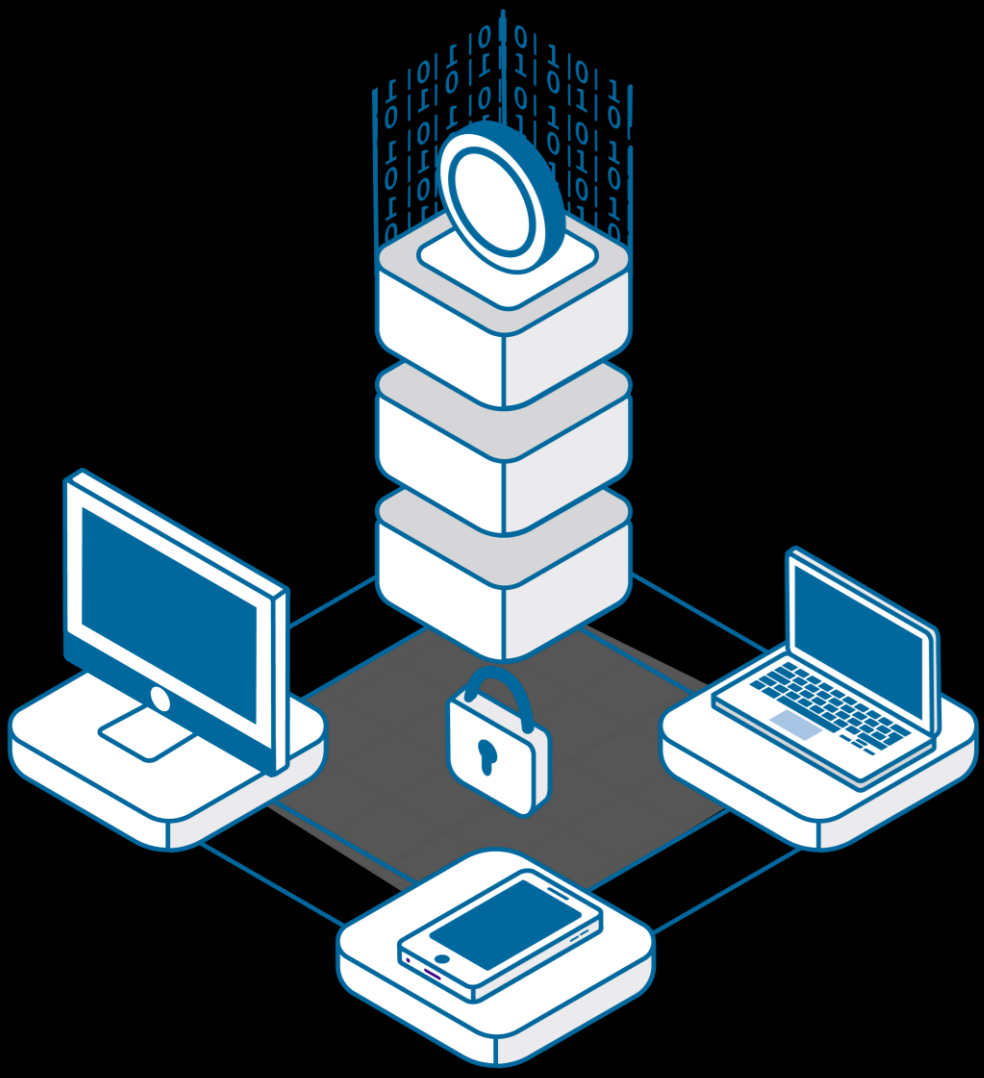
Armed with inside knowledge of such issues in the background verification process, at Infoeaze we believe the right application of blockchain and machine learning-based technical capabilities, in conjunction with a Self-Sovereign Identity (SSI) philosophy and human-centred design, is the best and most sustainable approach. We propose a Verification-as-a-Utility business model where we automate verification, payment, token transfer to create a fair, transparent, and frictionless experience for all stakeholders.

Since the majority of the problem is out of scope for any one stakeholder to make a significant change, we offer a complete redesign of the process in the form of Verification-as-a-Utility business model, using the **Consent Platform**, that aims to:

- **Fix the broken verification process** by reimagining the process in a human-centred manner;
- **Reduce the time-to-hire** with pre-agreed Consent during the onboarding process; and
- **Save employers money** by helping them issue self-verifiable certificates to reduce future total transaction cost around compliance, training, time and resources.

OUR SOLUTION

VERIFICATION-AS-A-UTILITY



2. Our Solution: Verification-as-a-Utility

The newly proposed business model below aims to achieve a high net promoter score (NPS) through its human-centred design approach by:

1. **Removing** the need to fill in lengthy, repetitive background verification forms;
2. **Avoiding** incorrect storage or recording of credentials;
3. **Automating** compliance for data handling;
4. **Reducing** the scope for a data breach; and
5. **Increasing** transparency around data access requests.

Instant access to verified credentials within the Utility model requires three key activities to be performed proactively:

1. Past employers would be encouraged to issue employer-verified credentials that are self-verifiable by users, removing the need to incur any future transaction costs associated with verification. In return, they would receive revenue share via the Consent Token.
2. Candidates would be encouraged to accept and store the verifiable credentials via a Consent Wallet.
3. Candidates would consent to share minimal data to pass a background verification check, i.e. using a pre-consent procedure to share employment and education background. In return, they would receive revenue share via the Consent Token and benefit from quicker verification.

Finally, to remove the cost associated with resources and compliance, access to the Consent Portal would be free for organisations to issue verified credentials.

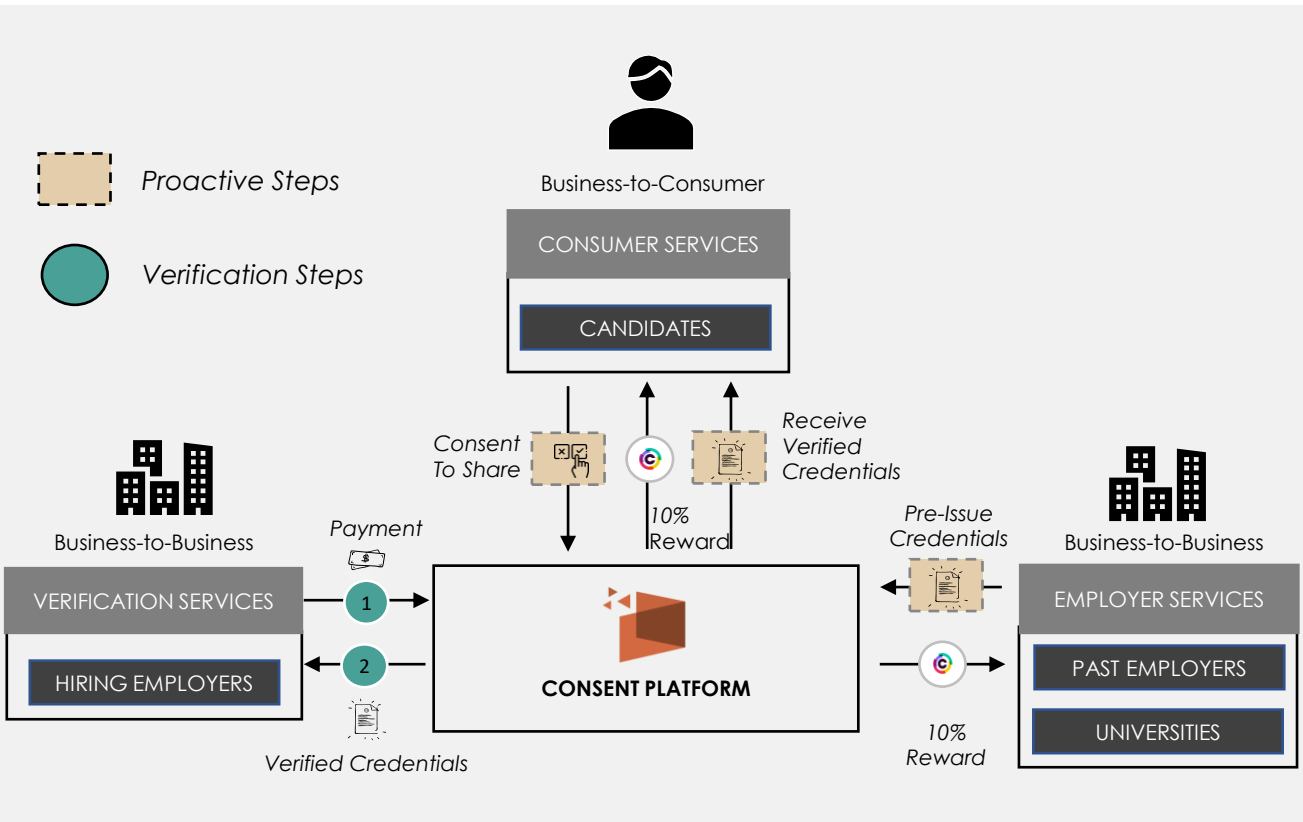


Figure 3: Proposed Solution to fix a broken verification ecosystem

OUR PRODUCT

CONSENT PORTAL | CONSENT WALLET

CONSENT PLATFORM

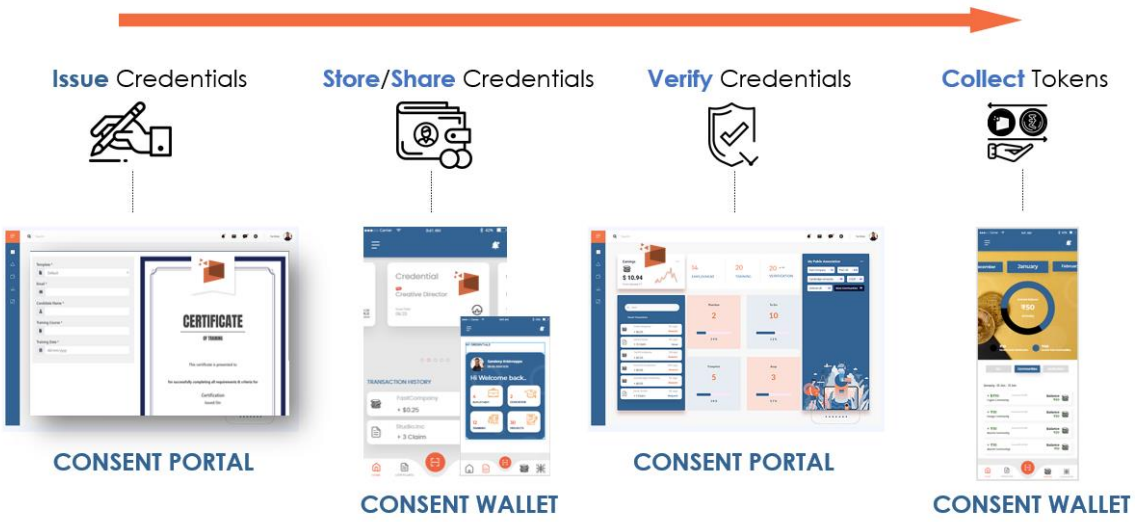


Figure 4: Two key components of Consent Platform

1. ***Consent Portal:*** Used by organisations to issue user-verifiable W3C-compliant Verified Credentials used by hiring organisations carrying out verification using an online portal to validate credentials shared by users.
2. ***Consent Wallet:*** For users to store, share and transfer Verified Credentials. Also used to store Consent Tokens *which are rewards issued in the form of tokens for consenting to information sharing*.

3.1 The Consent Marketplace

The World Economic Forum's Global Blockchain Council recently published the *Presidio Principles: Foundational Values for a Decentralized Future,* a list of principles to safeguard the promise of blockchain technology aimed at providing creators of blockchain applications with a baseline for designing systems that preserve the rights of their participants. As of 12 June 2020, the draft attracted 72 Signatories globally [21]. In accordance with Principles 6 and 8 under **Agency and Interoperability**, the Principles explicitly reference the role of consent for data stored in third-party systems and the ability to revoke consent to future data collection systems. In accordance with Principle 15 under **Accountability and Governance**, the ability to **opt-out** of applications that do not treat data in accordance with internationally recognised governance and data protection standards (i.e. GDPR if in Europe) is necessary.

At the heart of such values is the need to protect users. At Infoeaze, we believe this starts with turning the traditional business model upside down and placing Self-Sovereign Identity at the core. While opting-out is important for data protection, an opt-in model will prove very effective as well. This is especially true where a reward system is in place that is fair, transparent, ethical and built on user consent.

Our vision for the Consent Marketplace includes both existing and novel services:

1. **Novel services**, i.e. verifying project claims against individual employment and verifying claims on individual skills backed by actual work (*unlike the self-proclaimed and user-endorsed skills on LinkedIn*). These would be feasible in a Consent Marketplace of the future.
2. **Existing services currently deemed intrusive and unfair**, i.e. promotions and advertising (*this does not exist in BGVs*) in the digital world (*the likes of Facebook or Google audience targeting that uses personal data i.e. attitudes, habits etc*). These services could be redesigned in a non-intrusive (using opt-in) and fair (revenue share/rewards) manner in the Consent Marketplace of the future.

Figure 5: Token allocation for new services in the Consent Marketplace as rewards

The token allocation roadmap above illustrates some of the services we envision bringing to the Consent Marketplace around both Verification-as-a-Utility and communities and advertisements. The **reward distribution** in this marketplace would **start at 20%** and increase for every new service introduced (*i.e. Communities or CV Check*) into the Consent Marketplace.

A live **transparency dashboard** would be available to showcase the growth of the Consent market in real-time. This incentive model would increase in size with new services at the discretion of Infoeaze. Depending on the sustainability of the underlying platform at a given stage in the new service launch, the revenue generated would be allocated (*in proportion to the value generated using the underlying user data*) to the users and organisations participating in the market. The platform goes beyond the minimum standard of fairness and sets a new industry standard around rewards to build brand trust and loyalty.

3.2 Token Technology

We propose the Consent Token as a means of value exchange in the Verification-as-a-Utility business model for secure, consent-based storing, sharing, transfer and verification of a user's credentials using the Consent Portal and Consent Wallet mobile app.

The Consent Token is issued as a:

- **Reward for organisations** issuing self-verifiable credentials for employment, education, projects, training, or any industry-specific claims;
- **Reward for a user** or credentials holder for storing, sharing, or transferring verified credentials when the credentials are verified using Consent Wallet; and
- **For payment by the hiring employer** or background verification agencies for credentials verification to cover operations, maintenance, and future development of the Consent Platform.

The Consent Token, a token based on the Ethereum ERC20 standard, is an important element of the Consent Marketplace. Ethereum is an open-source, blockchain-based, distributed computing platform, oriented towards smart contracts. Our Consent Tokens would be created using Ethereum distributed virtual machine that allows end users to construct smart contracts for transactions. Smart contracts define the rules and penalties around an agreement in the same way that a traditional contract does, but also automatically enforce those obligations on the Ethereum blockchain. These contracts are cryptographically secure and can verify or enforce performance of the contract. Token contracts are a standard feature of the Ethereum ecosystem.

Ethereum has been used for mobile payment systems, distributed exchanges, tokens pegged to commodities and fiat currencies, market clearing mechanisms, micropayment systems for distributed computing resources, commodities and securities exchanges, crowdfunding, and legal document verification. Large firms have invested in experimenting and testing Ethereum. **Infoeaze has carried out global engagements** and advised some of the big 4 FMCG, big 4 utilities providers and defence contractors on Ethereum-based projects in areas such as nuclear, space, energy decarbonisation, sustainable aviation fuels and guarantee of origin.

According to Initial Coin Offering (ICO)/Security Token Offering (STO) spring 2020 edition published by PwC, in the first ten months of 2019, over 380 token offering have raised a total of USD $4.1 billion [3]. STOs continue to be a pivotal blockchain-based crowdfunding instrument. More and more established institutions globally conduct directly-issued corporate STOs. Examples include Bank of China ($2.8bn), Austrian Government ($1.4bn), BBVA (€150m), Daimler (€100m), Société Générale (€100m) and the World Bank ($108m) [3].

TOKENS

Micropayments using Consent Tokens will be accomplished by integrating with **crypto exchange partners** and using their open-source crypto wallets. The high-level concept of rewards payment involves the hiring organisations (*or background verification agency*) sending a payment in Consent Tokens along with request for users to share verified credentials via an access request. When the user receives the request to share relevant claims and the user consents, the verification is instant. At this stage, the flow of payments unlocks and the smart contract transfers 80% of the Consent Tokens to Infoeaze while 20% is passed on as rewards to the original issuer (*past employer*) and holder (*user who shared his credentials*).

In the early stages of the service launch, Infoeaze will **share 20% of total revenue**. As new services are added, the Consent Platform will increase the reward by 10% (*for a newly launched service or product only*). This incentive model would increase in size at the discretion of Infoeaze. Depending on the sustainability of the underlying platform at a given stage in new service launch, the revenue generated would be allocated (*in proportion to the value generated using the underlying user data*) to the users and organisations participating in such a market. This is to ensure users of the Consent Wallet own a stake in the Consent Marketplace as a prosumer (*users who produce and consume services in our Consent Marketplace*) at later stage of the product evolution. The word prosumer is a term coined in 1980 by American futurist Alvin Toffler [4] which is increasing in popularity in the energy sector where power consumers are also power generators in the renewable energy market (i.e. solar energy).

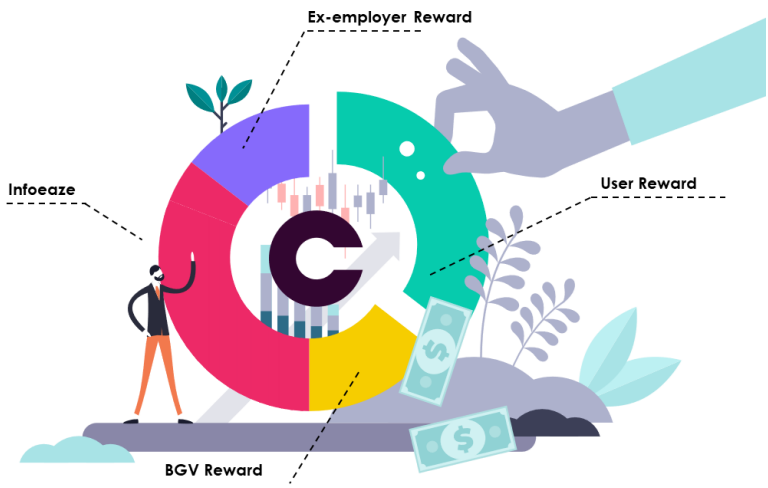


Figure 6: Verification-as-a-Utility Business Model with Tokens as Rewards

3.3 Tokens Used as Verification Payment

When organisations seek to verify a given claim regarding employment or education, hiring companies use third-party verification services. Carrying out the verification without a middleman is currently too expensive. The price for such services is based on the number of verification checks and the type of verification checks organisations require. Introducing tokens as a means of payment opens a world of possibilities around **micropayment**, **tracking** the flow of a fraction of any given token and **promoting loyalty** and **fairness** in a convenient manner.

As part of the Verification-as-a-Utility business model, on launch, the Consent Platform will make it easy for employers to issue self-verifiable claims for specific projects for external contractors or existing internal employees. The cost to validate these micro claims would be a fraction of a complete verification. This is a service which is just **not feasible in the current ecosystem** due to the overhead cost to operationalise it across the verification value chain. While this is unlikely to be a preferred service for incumbents (HireRight, FirstAdvantage, etc.), it is a competitive advantage to provide a strong user interface and price-competitive service on our Consent Platform.

In the newly envisioned business model, hiring employers who would like to verify a candidate would be able to purchase Consent Tokens via fiat currency to use as a mode of payment. These tokens would further be distributed as incentives back to issuers (*past employers that issued certificates*) and users (*credential holders*). Once the Consent Platform matures, and more new services are added, the percentage of **rewards would increase** and make tracking the provenance of these requests highly transparent to all the stakeholders.

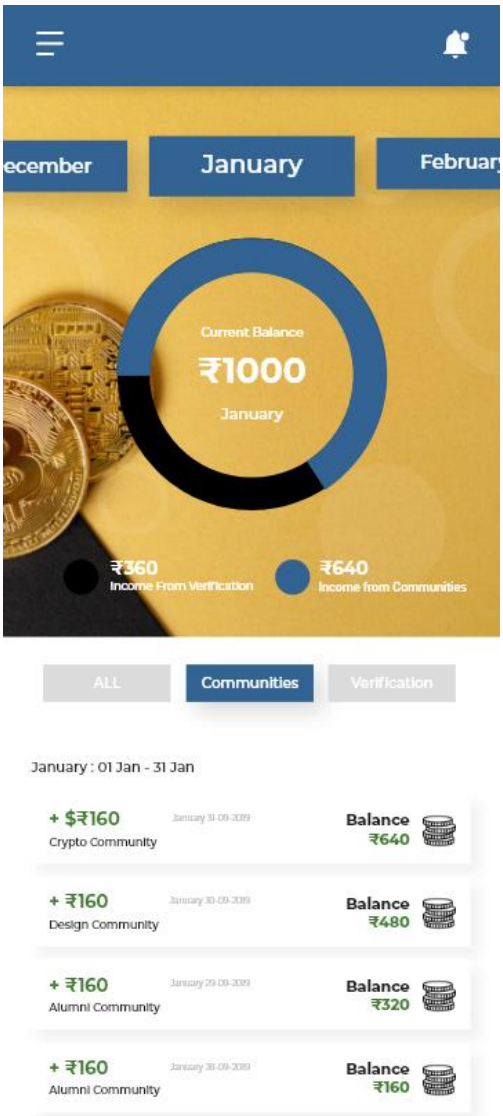
CREDENTIALS

3.4 Tokens for Credential Holders

As users are given access to the Consent Wallet to store, share, or transfer verified credentials, we strive to give the best user experience possible. **Our vision at Infoeaze is to be the world's number one Verified Credentials Wallet to store, share and manage verified credentials.** Hence, innovating and introducing new services for the benefit of our users is our top priority. We strive to create and share real value from the user's data from day one. The reward tokens will be our key value proposition for our customers, allowing them to monetize their data with the touch of a button on the mobile app.

Currently, none of the verification companies issue tokens to share their revenue. The verification companies that do share tokens tie the users to the platform that issued them and hold no value outside in the real world (*i.e. you are unable to convert the tokens to local fiat currency like rupees or dollars*).

When it comes to token analytics, we help users understand how their Consent to share personal data is rewarding them at every stage of the credential verification lifecycle. Infoeaze has an easy to use **analytics system** that will show users where and how they are earning their tokens. Once users understand how they can control the data, it is a lot easier to make sure they understand the direct correlation of rewards to all the small actions they take on the Consent Platform.

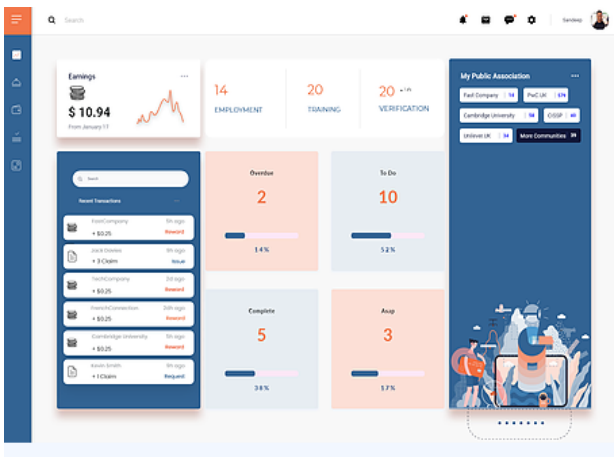


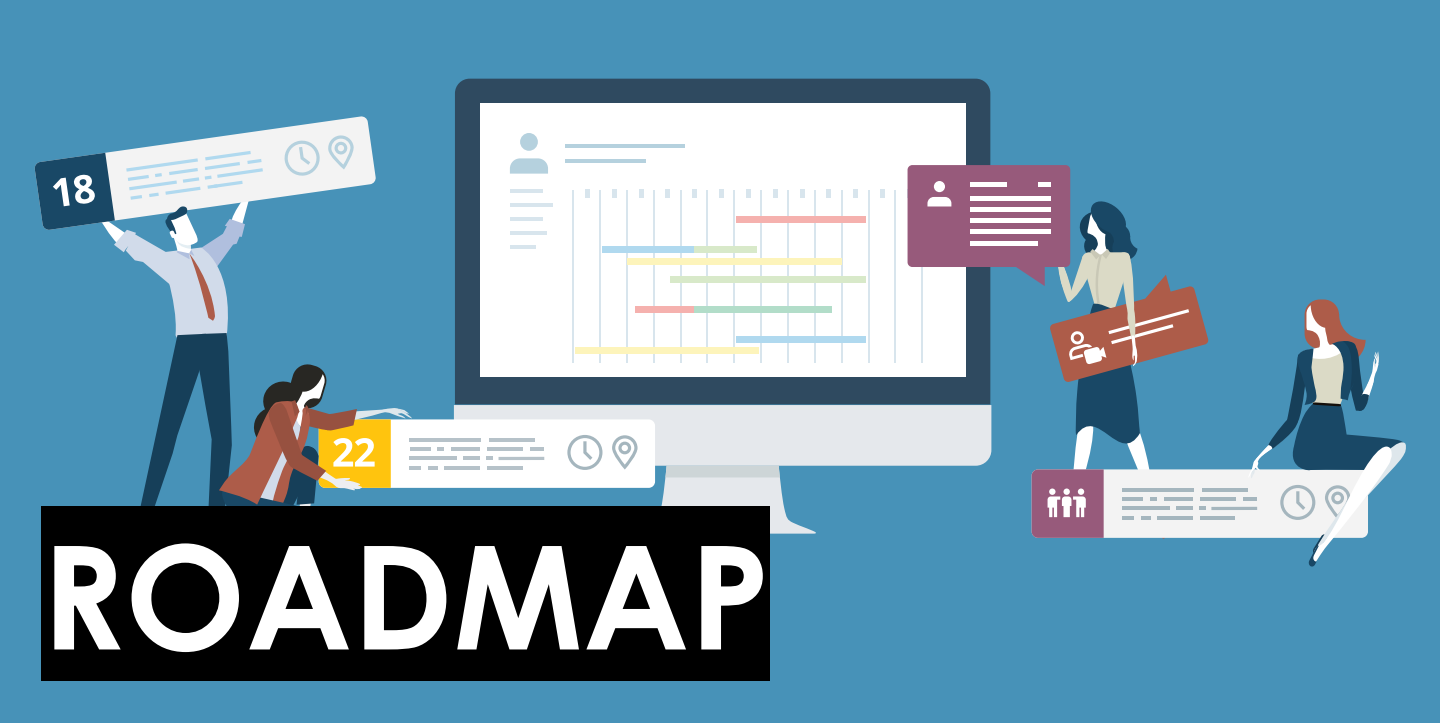
3.5 Tokens for Credential Issuer

The key opportunity for credential issuers in the Verification-as-a-Utility business model allows for the **reduction or reallocation of required human resources costs** (*approximately Rs. 42 lakhs per 5000 employees*) to prove past employees' experience when requested by verification companies. As more institutions possess W3C – Verified Credential issuing capability, as part of identity or human resources software or even help desk systems (*i.e. Microsoft Active Directory for B2C, Workday, Service Now etc*) [5][6], we envision a world where most of the vendors would make it easy for employers to issue such credentials. To fast track this adoption curve of self-verifiable credentials using Verified Credentials data model 1.0, we will be offering early access to Consent Portal to start-ups across India for free (*for the first two years*) and then to the wider enterprise service sector.

To promote more organisations onboarding and issuing credentials to current and past employees, the Consent Platform will share 10% of its revenue in the form of tokens for every verified candidate. This would not only help in **cutting down existing costs**, but also enable organisations to **earn reward tokens**. These tokens would self-pay for the effort in generating these credentials with an effort to payback ratio of 1:5 .

When it comes to token analytics, like the analytics issued for user via the mobile wallet, Infoeaze has an easy to use analytics system integrated within the Consent Portal. The embedded dashboard will highlight where and how institution-issued credentials are earning Consent Tokens. The analytics will showcase time saved in conducting manual checks and continue to reward employers for quick turnaround on new credential issue requests, i.e. requests raised by its former employees. This would help employers understand the **direct correlation of rewards and small actions** they take on the platform to close past requests to issue credentials on time.





3.6 Feature Roadmap

- ***Consent Portal***: Launch for Start-ups initially and later available for all organisations (*i.e. enterprise customers*).
- ***Consent Wallet***: Launch for users initially and later available for enterprise customers across various industries (*energy, transportation, etc*).
- ***Payment Gateway***: Launch to accept payments in any currency, including crypto currency such as Bitcoin, Ethereum, etc.
- ***Crypto Exchange and Consent Tokens***: Integration of embedded crypto wallet from our partners (*to be established*) that can enable storage and trading of Consent Tokens.
- ***CV Check***: Launch of premium service for recruitment and verification companies for verified talent search.
- ***Enterprise L&D Certificates:*** Focusing on Learning & Development for in-house teams to issue self-verifiable certificates based on a subscription model.
- ***Renewable Energy Guarantee-of-Origin Certificates:*** Focusing on Green Hydrogen, Sustainable Aviation Fuel and Green Ammonia for Energy Transition Markets.
- ***Communities & Endorsements***: Launch of basic alumni community around employers and educational institutions initially. This will be further extended to create new communities around popular career-based community interest groups.
- ***Audience Targeting for Consented Ads***: Launch of consent-based opportunity tracker for users and opportunity publisher for organisations. (i.e Investors targeting start-ups)
- ***Decentralized Stake:*** Launch of 100% community-owned decentralized financial affordability verification platform for organisations in the payment and lending businesses.

BUSINESS LANDSCAPE

COMPETITION

LANDSCAPE | OBSERVATION | KEY PLAYERS | COMPARISON MATRIX

4. Business landscape

The stakeholders in the current background verification ecosystem include **huge revenue-earning** global verification companies such as Equifax ($700m) [7], Sterling ($558.9m) [8], HireRight ($482.5m) [9], Accurate ($325m) [10] and some new entrants in the Indian market like Authbridge ($10m) [11], IDFY ($2.5m) [12] and Springrole ($1.5m) [13]. Some of the companies are exploring the use of machine learning and Artificial Intelligence for reporting and automation while others are looking at Blockchain as a potential technology to reduce costs and increase efficiency.

The current market suggests there is no organisation which currently focuses on giving users control of their personal data (*using Self-Sovereign Identity*) and enabling easy monetisation of their personal data (*fair token rewards for revenue sharing*).

Finally, since most of the disruptive start-ups in background verification started before any maturity in data portability standards, there has been **little consideration around interoperability** between different organisations (*past employers or hiring organisations*) or the vendor (*verification providers*) data model. The W3C – Verified Credentials data model 1.0, published on 19 November 2019 [14], is one such standard which facilitates data portability across various implementing organisations or vendors. Though some organisations are now exploring integrating the W3C open standard into their data exchange model, this is not embedded in the current background verification incumbents' business models.

Thus, the unique proposition the Verification-as-a-Utility and the Consent Platform brings to the market include:

- Tokenised incentive for **revenue sharing**;
- **Self-Sovereign Identity**, giving users control of their personal data;
- Using **W3C Open standards** to make credentials portable; and
- Frictionless experience with **human-centred design** and product development.

4.1 Key Observation : Why Avoid Data Hoarding

Equifax is one of the three largest companies in consumer credit reporting alongside Experian and TransUnion. They collect information of over 800 million individual consumers and 88 million businesses worldwide. Equifax Workforce Solution (EWS) is being presented to the market as a trusted and resilient business modelled around their product**, The Work Number** [15].

The Work Number bridges the Employer services and verification services by managing three data portfolios:

- Employment;
- Income; and
- Identity (ID, Date of Birth, Residency, etc).

Employment and Income data are at the centre of this data hub supporting a multitude of services (40 services in total as of 2020) in mortgage, government, corporate, financial and more. This model validates the breadth of services that can be offered within the verification sector and its scalability.

However, there is something very important to note from a security standpoint. The EWS framework is built on centralised data which means that it is susceptible to hacks and cyber-attacks by organised agencies leading to far reaching effects in the verification industry. This is not new and, in 2017, **Equifax compromised 143 million people's social security numbers** and other data [16]. This is a clear reminder of why Self-Sovereign Identity *and* decentralised records are the way forward for secure storage.

4.2 Competition

MARKET SCAN		COMPARISON		
No	**Name**	**Reward Tokens**	**W3C – VC Standard**	**Self-sovereign Identity**
1	Infoeaze (Consent)	☑	☑	☑
2	Blockcerts [17]	X	In Progress	In Progress
3	Sofocle Technologies [18]	X	X	☑
4	Auxesis [19]	X	X	☑
5	SpringRole [20]	☑	X	X
6	Zebi	X	X	X
7	Hire Right	X	X	X
8	Sterling Talent Solutions	X	X	X
9	Accurate	X	X	X
10	First Advantage	X	X	X
11	Equifax	X	X	X
12	AuthBridge	X	X	X
13	Fourth Force	X	X	X
14	Millow	X	X	X
15	SecUR credentials	X	X	X
16	Prompt Personnel	X	X	X
17	Helloverify	X	X	X
18	IDfy	X	X	X
19	BCDiploma	X	X	X
20	Smart Certificate (CVTRust)	X	X	X

4.3 Comparison Matrix

COMPARISON	
CURRENT ECOSYSTEM	**VERIFICATION-AS-A-UTILITY BUSINESS MODEL**
Data storage - organisation-controlled	Data storage – user-controlled
Re-active	Pro-active
Not transparent – hard to achieve transparency	Transparent across the value chain
No revenue share	Revenue share
Poor user experience	Excellent experience
Data Breach is common	Consent-based disclosure
Requires manual record keeping	Automation at the core
Verification is repeated	One-time verification, repeated usability
Cost incurred by past employers	Revenue earned by past employers

OUR ROOTS

MISSION | VISION | VALUE | MANIFESTO | TEAM

5.1 OUR MISSION, VISION, VALUES

MISSION

Build trust in digital identity and solve important problems.

VISION

To be the world's number one verified credentials wallet to store, share and manage verified credentials.

VALUES

Inclusion, Compassion, Knowledge, Creativity and Nimbleness.

5.2 Our Manifesto

1. Right to Issue

Any institution should be able to issue verified credentials for free to help the holders.

2. Own Your Data

Users should be able to own and store data conveniently with no vendor lock-in.

3. Choose Your Opportunity

Users should be able to view what they consent to and not what the advertisers choose.

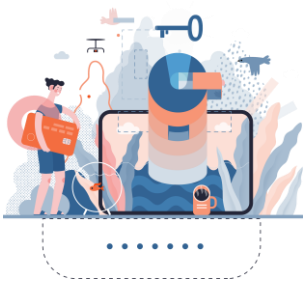
4. Control Data Privacy

Users should be able to share data on a need-to-know basis without disclosing all of the data.

5. Instant Verification

Users should be able to prove their details instantly and not have to wait for days.

6. Fair Incentive



Users should be able to monetize their personal data in a convenient manner.

5.3 Our Core Team

Madan Prasad | Co-founder | Chief Executive Officer | Full-time

Madan leads the team as Chief Executive Officer with extensive process knowledge in the background verification business. He has worked at FirstAdvantage, HireRight, Aegis and America Online. He is also a six sigma black belt qualified professional for process improvement.

Santosh Golechha | Co-founder | Chief Technology Officer | Part-time

Santosh leads the team as Chief Technology Officer with 20 years experience in Software Development and Architecture. He has worked across California, Boston, Atlanta and Houston. He is currently based in Vizag and manages three associates within our development powerhouse.

Sandeep Krishnappa | Co-founder | Chief Product Officer | Part-time

Sandeep leads the team as Chief Product Officer with 14 years of cross industry background in Knowledge Transfer and Digital Transformation. His past experience includes working at Northern Railways, Unilever R&D, British Gas, PricewaterhouseCoopers, KBC Advanced Technologies and, most recently, at Kellogg Brown & Root.

Lakshmi Kumari | Background Verification Lead | Full-time

Lakshmi has over 11 years experience working in background verification process and knowledge process outsourcing. She currently leads our internal BGV process team. and customer experience journey. Her experience also includes casualty and liability insurance at Ajg Gallagher and, people and process management at First Advantage and First American Title.

Abhishek Venkatesha | Business Development Lead | Full-time

Abhishek was one of our first partners to join Infoeaze and leads all our business development activities and external engagement. He worked at KPMG and Dunzo before joining Infoeaze to take on the challenging leadership role of developing our business globally. He has BA Honours in Business Management from Sheffield Hallam University.

Atif Ahmad | Investment Lead | Part-time

Atif has over 12 years of experience as a project/program management and business consultant with extensive experience spanning multiple industries. Atif is a Chartered Engineer, ITIL 4 certified, a PRINCE2 Practitioner and has an MBA from Alliance Manchester Business School. His past work experience includes Cisco, Siemens, DNV-GL and Invensys (A Schenider Company).

5.4 Our Advisors

Alina Zhou | Finance

Alina has over 10 years' experience working across the United Kingdom, China and Singapore. She is currently Head of Finance (ASEAN) at Alibaba group. She is CIMA/CGMA qualified and has extensive experiences across various finance functions, specialising in financial planning and analysis and continuous improvement to process and risk management.

Arianna Trozze | Crypto

Arianna has over 11 years' experience working as a consultant, product manager, analyst and researcher. She is currently a PhD Candidate at the EPSRC Centre for Doctoral Training in Cybersecurity (University College London). Her most recent work was for the law firm Kobre & Kim. She has an MSc from the University of Oxford and a BA from Franklin University Switzerland.

Asfiaa Husaini | Talent

Asfia has 12 years experience working in the information technology and services industry. She started her career at Goldman Sachs and then worked for Tesco, NetApp and spent the last 9 years at Dell EMC. She is skilled in Talent Management, Recruiting, and Technical Recruiting. She has a Master's in Human Resources Management.

Maya Bhatti | Marketing

Maya has over 20 years' experience and has worked for large multi-national organisations as well as SMEs. More recently, Maya worked at PricewaterhouseCoopers for 14 years, where she was the Global Marketing Campaign Leader for Artificial Intelligence and Cyber Security. Prior to this she was Global Financial Services and Asset Wealth Management Marketing Leader.

Bhanu Chandran | Learning & Development

Bhanu has over 28 years' experience in human resources with a successful history of working in the Financial Services and IT industry. She is currently Vice President of HR & Contacts at Amazech. In the past, she headed talent development at Goldman Sachs in India and served as Vice President – L&D for Asia Pacific at Northern Trust.

5.4 Our Advisors

Abdulla Mahmood | Brand

Abdulla has over 18 years of experience in Marketing and Business Development. He is currently a Director at Al Ahli Holding Group, Dubai. He focuses on strategic brand alliances with regional and international government bodies, global talents, celebrities and Hollywood Studios such as Netflix, Marvel, Disney, Fox and Sony. He was honoured as Asia's Most Influential CMO, Asia's Marketing Professional and Asia's Corporate Communication Professional.

Kevin Clarke | Services

Kevin has over 35 years experience in Energy Consulting. He is currently CEO of CREAS and focuses on strategic and technical advisory to venture capital, private equity funds and banks investing in sustainable technology for the energy-to-chemicals. He has held senior leadership positions at Kellogg Brown & Root, Permasense (A Emerson Company), KBC Advanced Technology (A Yokogawa Company) and others.

Jyothish Nair | Design

Jyothish has over 20+ years experience in the creative sector. He is currently Vice President and Associate Partner at McKinsey & Company, London. His past experience includes reshaping the future of design systems across digital experiences, physical products and service touch points as a Group Creative Director at Barclays, Creative Director at Native Design and associate creative director for Publicis Sapient.

Longzhu Shen | Artificial Intelligence

Shen is a scientific consultant on machine learning, mathematical modelling, quantum chemistry and GIS computations. He has post doc research experience at University of Cambridge and Yale University. He also holds a PhD in Chemistry from Carnegie Mellon University, M.S. in Computational Biology from Beijing University of Technology and B.S. in Biochemistry from Northwest University.

Varun Sethi | Legal

Varun Sethi is a lawyer who has been a start-up evangelist and consultant for past 7 years, consulting for more than 120 start-ups in India and abroad, including more than 95 funded by Indian and U.S. VCs. His efforts have been covered by the Economic Times, Bloomberg TV, Money Control, Forbes India, Crypto Currency and other media outlets.

TOP 10 RISKS

VERIFICATION-AS-A-UTILITY BUSINESS MODEL

6. Top Ten Business Risks and Mitigation Strategy

NO	TOP 10 RISK	PROBABILITY	MITIGATION STRATEGY
1	Cryptocurrency governance policies vary regionally	60%	☑ - DOCUMENTED GAP ANALYSIS
2	Regulatory authorities may want to review SSI credentials process for background verification	20%	☑ - DOCUMENTED LOBBYING STRATEGY
3	Dependency on partner wallet; transaction fees may change, the service provider could suffer major operational issues such as falling victim to a cyber-attack	80%	☑ - DOCUMENTED WALLET PROVIDERS
4	Getting enough start-ups to sign-up	20%	☑ - DOCUMENTED INCENTIVE STRATEGY
5	Ex-employers may decline to provide verification via the Consent Platform	50%	☑ - DOCUMENTED INCENTIVE STRATEGY
6	Consent credential holders fail to see the value and refuse to use the Consent Wallet	50%	☑ - DOCUMENTED PR STRATEGY
7	Unauthorised access to Consent Portal.	30%	☑ - DOCUMENTED KYC STRATEGY
8	Unauthorised universities opening accounts on Consent Portal.	99%	☑ - DOCUMENTED KYC STRATEGY
9	Lack of W3C Adoption across the industry	10%	☑ - DOCUMENTED PR STRATEGY
10	Users migrating to a different wallet	50%	☑ - DOCUMENTED LOYALTY STRATEGY

HORIZONS BEYOND

ENVIRONMENT | SOCIAL | GOVENANCE

7. Scaling Verifications-as-a-Utility across Industries

A Consent Platform created for background verification can play a key role towards sustainability impact analysis for organisations and governments when focused on Environmental, Social and Governance (ESG) issues. It also **helps investors understand fund exposure** to ESG-related risks. This may be used by long-horizon investors with a goal of limiting potential financial costs connected with issues like water scarcity or carbon regulations.

We envision, on completion of product development, the underlying **Consent infrastructure will be licensed or shared** with partner organisations that could benefit from using the Verification-as-a-Utility business model to cut transaction costs around sustainability impact analysis. We have already seen a huge interest in self-verifiable credentials (*and already partnered*) in the renewable energy markets with respect to guarantee-of-origin verification and decarbonisation strategy to meet carbon emissions targets by global organisations.

Below is a list of possible opportunities around sustainable impact analysis in the envisioned Consent Marketplace:

Environmental Issues

- **Climate Change**: This would include issuing verified credentials around carbon emissions and tracking carbon footprints of consumer products.
- **Natural Resources:** Reducing water spillage by benchmarking claims shared by utility providers, encouraging biodiversity, land usage and raw material usage via satellite imagery verification.
- **Pollution and Waste**: Verification of industrial footprint around toxic emission of waste, electronic waste and recycling packaging materials.
- **Environmental Opportunity**: Managing claims around Green Buildings that use, for example, decentralized rainwater harvesting. Verifying guarantee-of-origin claims for renewable energy that covers not only solar, wind and hydropower, but also emerging green hydrogen and green ammonia exports.

Social Issues

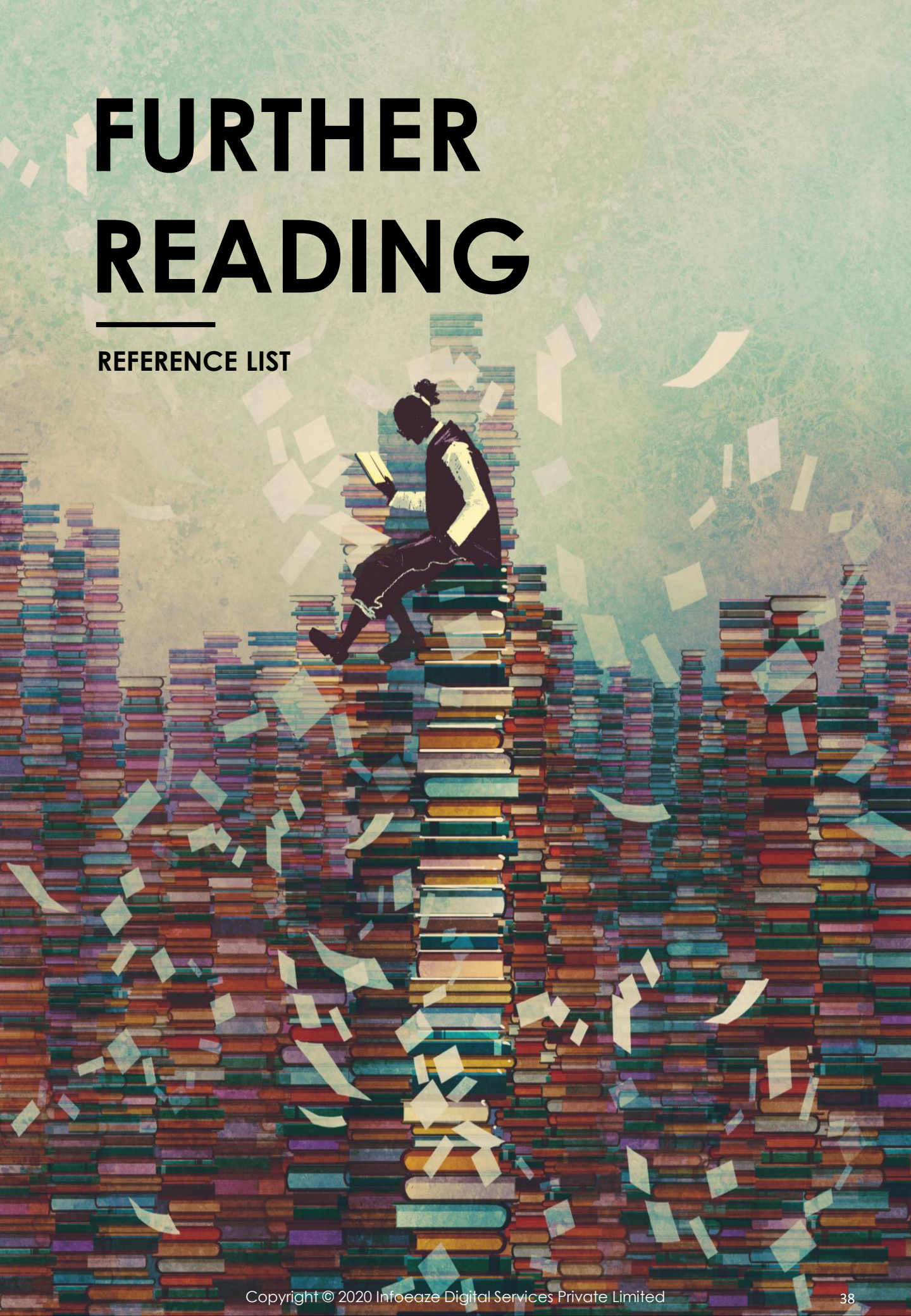
- **Human Capital:** Verifying claims on upskilling and talent development of local communities, health and safety records, industrial engineering work permits on critical assets, i.e. project- or contract-based credentials.
- **Stakeholder Opposition**: Verification of controversial sourcing within supply chain for industrial manufacturing.
- **Product Liability**: This includes chemical safety (GMO tracking), privacy and data security standards (Self-Sovereign Identity) and product safety and quality (sustainable aviation fuel).
- **Social Opportunities**: Verifying secure communication (content delivery networks or open-source satellite networks) and nutrition and health (in facility management services).

Governance Issues

- **Corporate Governance**: verifying corporate securities (due to qualities around liquidity and transparency), voting in corporate elections (election of director for pension plans), ownership of stake (decentralised autonomous organisation) and know your customer or know your partners.
- **Corporate Behaviour**: Real-time auditing (carbon emissions), related party transactions in disclosure rules (suspicious asset transfers) and earning management (accounting manipulation).

FURTHER READING

REFERENCE LIST



8. References & Further Reading

Abstract

[1] https://www.globenewswire.com/news-release/2020/06/01/2041528/0/en/Employment-Screening-Services-Market-to-Reach-7-64-Billion-by-2026-at-8-3-CAGR.html

The Consent Marketplace

[2] https://www.weforum.org/communities/presidio-principles

Token Technology

[3] https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

[4] The Third Wave BY Toffler- book PUBLISHED in 1980

Tokens for Credential Issuers

[5] https://www.microsoft.com/en-us/security/business/identity/own-your-identity

[6] https://credentials.workday.com/docs/overview/#:~:text=Workday%20Credentials%20provides%20tools%20and,is%20requesting%20from%20the%20user.

Business landscape

[7] https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/quarterly-results/2020/equifax-workforce-solutions-june-2020-update.pdf

[8] https://www.owler.com/company/sterlingcheck

[9] https://www.owler.com/company/hireright

[10] https://www.owler.com/company/accuratebackground

[11] https://www.owler.com/company/authbridge

[12] https://www.owler.com/company/idfy

[13] https://www.owler.com/company/springrole

[14] https://www.w3.org/TR/vc-data-model/

Key Observation

[15] https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/quarterly-results/2020/equifax-workforce-solutions-june-2020-update.pdf

[16] https://www.wired.com/story/equifax-hack-china/

Competition

[17] https://www.blockcerts.org/guide/

[18] https://www.sofocle.com/industry/blockchain-in-education/

[19] https://auxesisgroup.com/certify/

[20] https://blog.springrole.com/

8. References & Further Reading - Continued….

Additional Reading

a. *https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-token-assets-securities-tomorrow.pdf*

b. *https://www.pwc.com/it/it/publications/assets/docs/blockchain-and-digital-identity.pdf*

c. *https://datum.org/assets/Datum-WhitePaper.pdf*

d. *https://www.forbes.com/sites/joewalleneurope/2018/07/23/blockchain-run-platform-offers-european-consumers-opportunity-to-profit-from-own-personal-data/#20a21c18290a*

e. *https://arxiv.org/ftp/arxiv/papers/1712/1712.01767.pdf*

f. *https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45*

g. *https://github.com/jandrieu/rebooting-the-web-of-trust-fall2016/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf*

h. *https://www.w3.org/2019/09/18-didtalk-minutes.html*

i. *https://www.designkit.org/human-centered-design*

j. *https://www2.deloitte.com/us/en/pages/financial-services/articles/making-blockchain-real-customer-loyalty-rewards-programs.html*

k. *https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-tokenization-of-assets-disrupting-financial-industry.pdf*

l. *https://cointelegraph.com/explained/how-to-use-smart-contracts-for-revenue-sharing-explained*

m. *https://www.equifaxsecurity2017.com/consumer-notice/*

n. *https://www.msci.com/documents/10199/03d6faef-2394-44e9-a119-4ca130909226*

o. *https://www.msci.com/documents/10199/239004/MSCI-2019-ESG-Trends-to-Watch.pdf*

p. *https://www.msci.com/documents/1296102/15388113/MSCI+ESG+Fund+Ratings+Exec+Summary+Methodology.pdf*

q. *https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/09/impact-of-esg-disclosures.pdf*

Glossary

- **Blockchain** - a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree)
- **Environmental, Social and Governance (ESG)** - refers to the three central factors in measuring the sustainability and societal impact of an investment in a company or business.
- **ERC20 Token Standard** - is the Ethereum token standard which is used for Ethereum smart contracts. Developed in 2015, ERC-20 defines a common list of rules that an Ethereum token has to implement. Giving developers the ability to program how new tokens will function within the Ethereum ecosystem. This token protocol became popular with crowdfunding companies via Initial Coin Offering (ICO).
- **Ethereum** - is the second largest cryptocurrency platform by market capitalization, behind Bitcoin. It is a decentralized open source blockchain featuring smart contract functionality. Ether is the cryptocurrency generated by Ethereum miners as a reward for computations performed to secure the Blockchain. Ethereum serves as the platform for over 260,000 different cryptocurrencies, including 47 of the top 100 cryptocurrencies by market capitalization.
- **General Data Protection Regulation (GDPR)** - The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.
- **Guarantee-of-Origin (GO)** - is a tracking instrument defined in article 15 of the European Directive 2009/28/EC. A GO labels electricity from renewable sources to provide information to electricity customers on the source of their energy. Guarantees of origin are the only precisely defined instruments evidencing the origin of electricity generated from renewable energy sources.
- **Human-centred Design (HCD)** - *is an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques. This approach enhances effectiveness and efficiency, improves human well-being, user satisfaction, accessibility and sustainability; and counteracts possible adverse effects of use on human health, safety and performance*. ISO 9241-210:2019(E)
- **Initial Coin Offering (ICO)** - is a type of funding using cryptocurrencies. It is often a form of crowdfunding, however a private ICO which does not seek public investment is also possible. In an ICO, a quantity of cryptocurrency is sold in the form of "tokens" ("coins") to speculators or investors, in exchange for legal tender or other (generally established and more stable) cryptocurrencies such as Bitcoin or Ethereum. The tokens are promoted as future functional units of currency if or when the ICO's funding goal is met and the project successfully launches.
- **Net Promoter Score (NPS)** - is a management tool that can be used to gauge the loyalty of a firm's customer relationships. It serves as an alternative to traditional customer satisfaction research and is claimed to be correlated with revenue growth.
- **Security Token Offering (STO)** - is a type of public offering in which tokenized digital securities, known as security tokens, are sold in cryptocurrency exchanges. Tokens can be used to trade real financial assets such as equities and fixed income, and use a blockchain virtual ledger system to store and validate token transactions. Due to tokens being classified as securities, STOs are more susceptible to regulation and thus represent a more secure investment alternative than ICOs, which have been subject to numerous fraudulent schemes.

Glossary

- **Self-sovereign Identity (SSI)** - With self-sovereign identity (SSI) the individual identity holders fully create and control their credentials, without being forced to request permission of an intermediary or centralised authority and gives control over how their personal data is shared and used. The user has a means of generating and controlling unique identifiers as well as some facility to store identity data.
- **Verifiable Credentials (VC)** - are the electronic equivalent of the physical credentials that we all possess today, such as: plastic cards, passports, driving licences, qualifications and awards, etc. The data model for verifiable credentials is a World Wide Web Consortium Recommendation, "Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web" published 19 November 2019
- **World Wide Web Consortium (W3C)** - is the main international standards organization for the World Wide Web. Founded in 1994 and currently led by Tim Berners-Lee, the consortium is made up of member organizations that maintain full-time staff working together in the development of standards for the World Wide Web. As of 21 October 2019, W3C had 443 members.

Disclaimer :

The primary focus of this white paper is for the readers to analyse the product, understand the root cause of current problems existing in the background verification process and the effective digital solutions suggested to mitigate those critical factors in order for the potential customers and stakeholders to make an informed decisions without compromising on the Personal Identifiable Information that gets exchanged from one hand to another.

This white paper is only for information purpose and does not in any way intend to create any elements of a contractual relationship.

Estimates and few statements mentioned in this document are forward looking situations based on future contingencies which may lead to the variations in the estimates shown in this document.

The data shown in this white paper should not be taken as advice to buy, sell or hold any security. This document may not be distributed to anyone other than the intended audience.

Reproduction or distribution of all or any of this material is strictly prohibited.

Contributors :

Madan Prasad, Lakshmi Kumari , Atif Ahmad, Abhishek Venkatesha, Santosh Golechha, Asfiaa Husaini and Sandeep Krishnappa

13:07:2020:01:41

Infoeaze Contact

Madan Prasad | CEO

Email: madan@infoeaze.in

Tel: 00 91 98860 38978

Abhishek Venkatesha | Business Development Lead

Email: abhishek@infoeaze.in

Tel: 00 91 96323 75277

Company: www.infoeaze.in

Project: www.consenttoken.com