Fix fraud – with trusted transactions, through verified self-sovereign digital identities

In the digital age, nothing can grow without trust

Yesterday’s tools are no match for tomorrow

The first commercial transactions were face-to-face. It was a good way to ensure trust: the counterparty had to be physically present. And if they ran off, at least you could chase them. But with the advent of ecommerce, technology created a divide between customer and provider.

Over the years, products evolved to bridge this gap. Mainframe computers became laptops, and then mobile devices. The more intimate the interface became, the ‘closer’ businesses and consumers could get.

While this shift from physical to digital has brought many benefits, it’s also had less welcome effects. Today’s corporations hold more of our personal data than we ever anticipated, or feel comfortable with.

And as we’ve moved more and more online, digital platforms and processes have failed to keep up. We can’t trust them to collect, store or share our personal information safely. In fact, consumers’ information is frequently abused and misused, without our knowledge or consent. The trust in the system that supports our very digital lives has been massively eroded.

Businesses are impacted, too. They’ve been forced to add extra safeguards to outdated password-based login systems. We’ve seen the rise of 2FA, SMS, card readers, unique mobile IDs, and more – all of which are creating more friction for consumers and businesses alike. At the same time, data breaches and identity fraud are not just commonplace – they’re actually increasing.

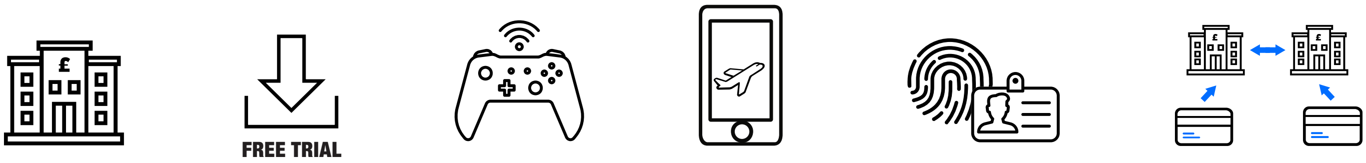
In 2021, the average cost of a data breach reached an all-time high of $4.24 million. Even though businesses are already spending millions more to combat financial crime, and meet their regulatory and compliance responsibilities.

THE SYSTEM IS BROKEN. IT’S FAILING CONSUMERS, AND FAILING BUSINESSES. WE NEED FUNDAMENTAL CHANGE.

$4.24 MILLION

AVERAGE COST OF A DATA BREACH

SOURCE: IBM



Why existing identity technologies fail

More than any other time, the period of COVID-19 has highlighted the need for greater trust in the digital age.

The pandemic has shown the need for far greater contactless and remote access to goods and services. But existing systems have proved difficult to adapt. In a recent survey of nearly 3,000 Regulatory & Compliance Managers, 65% of respondents admitted that the crisis had forced them to take shortcuts with their KYC requirements. Before the pandemic, fewer than half of surveyed companies had been subject to due diligence checks. In its wake, that number is shrinking even further.

In a survey by the Economist Intelligence Unit (EIU), 61% of 1,610 global executives said they'd changed their transaction processes as a direct result of the pandemic. And in this rush to adapt, companies have taken some dangerous shortcuts.

COVID-19 has highlighted the need for a solution to privacy, security and improved due diligence. A perfect example of this is the COVID Credentials Initiative ("CCI"). This is an open global community, collaborating to enable the interoperable use of open-standard-based, privacy-preserving credentials and other related technologies for public health purposes.

As businesses move increasingly towards data-driven systems, consumers have never had more reason to be wary of how their information is being accessed, stored and used. The same shift also means that businesses need to better manage fraud, and all their data security, privacy and regulatory obligations. Consumers are demanding a new level of trust from businesses – and rightly so. As we move forward, companies that want to win and retain customers will have to address this gap.

People want to control their own data. They want the confidence that no one can access that data without permission. And they want stronger authentication than a password that's all too easily forgotten – or compromised.

Of course, they also want to become ever more mobile and connected. And in response, digital services are moving towards solutions that not only establish trust, but also maintain it. Developers and service providers, take note: the importance – and value – of genuine trust has never been higher.

A digital identity is now well established as one of the most significant technology trends for enabling and maintaining trust – and so combating fraud. So, if digital identities are the 'silver bullet' of trust, why have none of the existing identity technologies managed to penetrate the mass market? It's because they fail in one of three ways:

1

THEY DON'T WORK FOR THE BUSINESS

Existing solutions don't verify identities at both ends of a transaction. And the payment history is only tied to payment methods – not the identity itself.

2

THEY DON'T WORK FOR THE CONSUMER

Federated, device-dependent, single-use identity solutions don't give consumers control of their identity. Or they don't deliver across the lifecycle of creating an account, payment, and accessing services.

3

THEY DON'T WORK FOR THE COMPLIANCE TEAM

Until now, self-sovereign identity solutions have been incompatible with compliance and reporting requirements.

In short, existing systems can't provide adequate security for either businesses or consumers. And many are not fully compliant – especially across multiple markets.

The only way is trust

Data security is in crisis. Fraud and financial crime is on the rise. And the pandemic has shown us the importance of remote, contactless access to services whilst ensuring the right level of due diligence and meeting regulatory and compliance obligations.

This has intensified the drive for digital identity frameworks. This in turn has generated new technologies and regulations to support the transformation, and new standards that foster compatibility and interoperability.

Critically, we all want a sense of control over our data. And we want to authenticate ourselves by who we are, not what we can remember.

At this moment, businesses, customers and regulators need trusted transactions. The only way to deliver this is by establishing a persistent, verifiable digital identity. One that not only establishes trust but maintains it through every interaction, for the entire life of the relationship between consumer and service. Even across multiple products. Trust has become an essential component for both innovation and development.

The good news is, this type of identification system is now possible, thanks to a combination of emerging technologies and forward-thinking protocols.

We have the answer

Companies have to enable trust in data and technology from the outset. And they can – with an approach we call Trusted Transactions.

Trusted Transactions are supported by a wide range of emerging technologies and techniques, leading to the creation of a true Self-Sovereign ID, or SSI. These include Decentralised Identifiers (DIDs), Verifiable Credentials (VCs), and Key Event Receipt Infrastructure (KERI). All these solutions use cryptography, zero-knowledge proofs, and blockchain elements to create systems of identification that are virtually impossible to fabricate.

DIDs enable users to prove their credentials independent of any centralised registry. With VCs, they can verify this information without giving away their personal data. Infrastructure approaches like KERI will allow identity verification with or without accessing a blockchain. So it'll even work offline.

By combining these techniques with biometrics and unique identifiers, it's possible to create trusted transactions. Transactions that are secure, and linked to unfalsifiable user features, like fingerprints or face scans.

AI can also monitor for patterns of behaviour that point to illegal activity like money laundering or terrorist financing. And because the data can be independently confirmed by all, the need for blind trust is replaced with trustless veracity.

This approach creates huge positive impacts. Consumers and businesses both feel the benefit of trusted transactions in account creation, moving digital assets, making payments, and when using services. It makes for frictionless, secure customer experiences. Fraud and false positives are massively reduced. And there are major improvements in privacy, security, compliance, efficiency, and time to market.

All of this will revolutionise many consumer interactions with commerce and the economy – specifically in financial services, digital assets, recruitment and onboarding, micropayments, travel, and gaming. In the next section, we describe each of these use cases in detail.

Trusted Transactions in action

STOPPING FRAUD IN FINANCIAL SERVICES

Trust has always been essential in finance. But even with background checks, two-factor authentication, and other identifying fraud detection and security measures, there have always been unavoidable risks.

With the proliferation of connected devices, and the rise of Open Banking and fintech products, reliable privacy and security has become even more important. The convenience of banking, transferring money and paying bills through a mobile app cannot be overstated. But the system can only work if it includes airtight protocols consumers can trust.

It's not just about the back end of these platforms. It's more about the many ways consumers can be harmed through hacks, SIM-swapping, impersonation scams – or even their own errors.

So called "phishing" scams are a common pitfall. Scammers send an email or text message designed to look like it comes from a trusted service, packaged as a promotion, reward or security alert. The message prompts the user to follow a link to what looks like the regular login screen. In fact, the link is nefarious and the user's data is sent to the attacker.

SIM swapping is a more sophisticated technique, in which the attacker uses social engineering to trick a mobile carrier into transferring the user's service to a different device.

This might sound unlikely, but it can be highly effective. Many carriers will do this based only on the sort of information that can be gleaned from a bit of social media investigation – such as name, post code, the user's phone number, and maybe a security question.

Even if the user is highly vigilant and uses strong 2FA authentication, the data being stored on a centralised server remains vulnerable to attack. Such servers should be highly secure, but users have no control over that whatsoever. So trust becomes an issue again.

Unfortunately, the current open banking regulations mean consumers have very few protections against these types of risks.

Businesses need protection, too. When they interact with a customer, they need to be sure it's the person they think it is. That's essential for maintaining their regulatory compliance, data, and brand. But it's not always easy. Organisations can be affected by the same threats outlined above for consumers.

But there is an answer. Verified digital identities at each end of a transaction can mitigate all these dangers – and more.

Critically, this approach means businesses no longer have to protect the data themselves. Each party is cryptographically proven, so each end party just needs to confirm the identity of their counterparty. Payments won't process without this confirmation.

And because it's biometrically enforced, it's impossible to fabricate. That makes phishing impossible, because only the official platform can confirm its identity to the user. The consumer can't even pay the wrong person if they try: the transaction simply won't go through unless it's with the agreed verified parties.

FREE TRIAL

NO MORE ABUSE OF FREE TRIALS

In recent years, subscriptions have become the predominant model for many online services – especially SaaS platforms, streaming content, and gaming. Free trials are a great way for these businesses to give consumers a taste of their offers, without the commitment of a year-long contract.

Unfortunately, such trials are repeatedly abused – both by consumers looking to beat the system, and by businesses themselves, who are often unclear or misleading about the terms of a trial, and when charges will be processed.

Users often 'cheat' a free trial by signing up repeatedly under different email addresses, mobiles or credentials. They also share the trials with other people. When this happens en masse, it costs the companies involved millions of dollars.

Meanwhile, it's reported that 59% of customers signing up for free trials have at some point found themselves charged against their will. Vagueness about trial obligations and time-frames can effectively mislead users into thinking a deal is better than it is. Some cases involve outright manipulation.

Verified SSIs make it possible to restrict individual users to one free trial each, as they can't provide multiple credentials. The same system can also prevent surprise charges, as the user's biometrically enforced identity is required to authorise the transaction. If they decline, the free trial can simply expire.

Users often 'cheat' a free trial by signing up repeatedly under different email addresses, mobiles or credentials.

ONLINE GAMING WHERE EVERYONE WINS

Online gaming continues to expand globally. As it does, new payment methods are emerging to cater to this new market, and deliver a more seamless customer experience. At the same time, the value of global online gambling and betting is expected to reach 82 billion euros by the end of 2024.

Online gaming and gambling customers need far greater protection than they currently enjoy. That requires a revolution in the industry's economic models.

In the broader video gaming world, blockchain promises new levels of engagement, ownership and even economic investment. Non-Fungible Tokens (NFTs) offer one solution. If NFTs are implemented into virtual worlds, players can effectively 'own' the items they purchase, craft, or earn in-game. Linking these NFTs to the user's ID means they can stay with the user across different game worlds – and even be sold on secondary markets. Players get greater control, and what had previously been simple purchases act more like investments.

Here's a practical example from Microsoft. The Xbox ecosystem depends on collaboration between its thousands of developers, publishers, authors, designers, production houses and distributors. In 2020, Microsoft recognised that it needed to address certain points of friction.

A multitude of manual processes and siloed systems meant developers and publishers couldn't link complex royalty calculations to the underlying data. So they spent time and resources on reconciling, validating and tracing back the transactions, then recalculating and verifying the royalties. It was exceptionally difficult for distributors to reconcile data from different sources.

In the next few years, the world of online gaming will be transformed by the combination of a whole new model for microtransactions, ownership of in-game content, and security for both users and the ecosystem. The platforms that thrive will be the ones that deliver personalised, bespoke experiences users can trust.

This is especially important now, because many companies already face the challenge of acquiring new players and retaining existing ones. If they can leverage the franchises players love with a whole new model for engagement and tangibility, they stand to attract more new players than ever. Everything hinges on what blockchain technology can provide.

The platforms that thrive will be the ones that deliver personalised, bespoke experiences users can trust.

FRICTIONLESS TRAVEL: THE NEW NORM

In the hospitality and travel industry, SSI technologies and trusted transactions can significantly improve the travel experience while also ensuring privacy and security.

Every year, companies in this sector are forced to spend more money trying to protect databases of customer information they don't really need. Even if a customer has only ever made one reservation, they end up on the company database – which is subject to GDPR and other legal scrutiny around the world.

The development of SSI, and its associated blockchain-based decentralised technology, means the customer retains control, because they have to grant access to their data to complete the reservation. At the same time, businesses can minimise data storage and its associated risks.

Financial services are critical to the travel industry. Using a verified digital identity for trusted transactions protects businesses from fraud and increases their operational efficiency.

This is especially important for international travel. Take the IATA Travel Pass. Based firmly on decentralised digital identity, this system is currently used by travellers to store and manage their verified certifications for COVID-19 tests or vaccines. But it's easy to imagine how much more it could do, from health and flight credentials to Uber rides, restaurant experiences and hotel access. The sky is literally the limit.

> **But it's easy to imagine how much more it could do, from health and flight credentials to Uber rides, restaurant experiences and hotel access. The sky is literally the limit.**

SIMPLER, CHEAPER, FASTER RECRUITMENT

Credentialing is one of the biggest issues for an organisation recruiting new staff. There can be more than 20 separate credentials for some individuals, involving considerable time and cost. Plus, reassigning staff to new placements can mean having to request the same volume of documents over and over again.

A digital credentialing platform can massively improve the process for both employers and employees, simplifying the onboarding journey and reducing the time it takes to recruit. Individuals have access to their verified credentials via their own digital wallet, making it much easier to store, share and maintain that data going forward. With multiple parties involved in these transactions over the course of someone's career the W3C Verifiable Credentials standard ensures portability and interoperability.

Employees own and control their own documentation, in their own secure digital vault. They share verified documents (like photo IDs, qualifications, work permits, references etc.) on a read-only, time-restricted basis between specified parties, for verification, regulatory or auditing purposes.

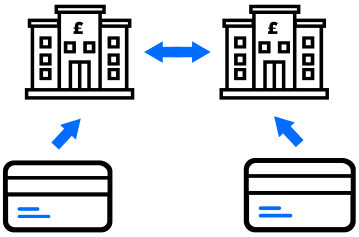
All relevant data is individually encrypted with the employee's private key and stored in the cloud. Permissioned IPFS data storage allows data to be deleted for GDPR and CCPA purposes. This means the data can be recovered if a device is lost or stolen. It also means documents can be made accessible for set time periods, as required by regulation and compliance for auditing purposes.

How employees receive and share credentials:

1. Connect to the services via a digital wallet and scan documents for verification
2. Documents are verified and saved in the employees secure digital vault
3. Employees can selectively share access to the verified credentials as required

This technology offers huge benefits to businesses across a variety of industries such as, healthcare, education, and government:

- Greatly reduced onboarding times – from weeks to days
- Significantly less recruiter time following up credentials
- Massive reduction in data storage – no risks of a breach
- Credentials can be used repeatedly, and re-verified as required, saving time and money
- Tangible commercial benefits
- Tamper proof credentials
- Businesses don't have to hold employee data – saving all the responsibility and cost of storage
- Easier access to verify information, making it simpler to share



FATF TRAVEL RULE: SOLVED

Verifiable credentials are ideal for ensuring compliance with the new Financial Action Task Force (FATF) Travel Rule for domestic and cross-border wire transfers.

The Travel Rule is an update to FATF Recommendation 16, extending it to cryptocurrencies. It now covers all Virtual Asset System Providers (VASPs), financial institutions and obliged entities. It requires that the originator and beneficiary of any digital fund transfer must exchange identifying information. They must also guarantee the accuracy of that information.

With a verifiable credentials platform, each party can create a verified identity that's cryptographically proven, using W3C verifiable credentials to prove all or part of its identity.

Originators – information required for virtual asset transfers

- Originator name (from driver's license or passport)
- Account number (where used to process the transaction)
- Physical address (from driver's license)
- National identity number, customer identification number, or other unique identity number (from identity card)
- Date of birth and place of birth (from passport)

Beneficiaries – information required for virtual asset transfers

- Beneficiary name (from driver's license, passport or identity card, as a business's KYB)
- Account number or virtual wallet number (where necessary)

Each identity is established through the creation of a unique PeerDID (Peer Decentralised Identifier), with accuracy guaranteed through the cryptographic proof of the verifiable credential.

This means that either party can provide cryptographic W3C verifiable receipts for their transactions. And it means that unless the rules are fulfilled, the transaction cannot happen.

> It requires that the originator and beneficiary of any digital fund transfer must exchange identifying information. They must also guarantee the accuracy of that information.

The time for trust has come

The process of 'verified authentication and authorisation combined with verifiable credentials' is critical to making information trustworthy and simplifying transactions. That's because trust is fundamental to a transaction.

As more transactions take place online, it's never been more important to know who your customer is, and be able to verify their identity at each and every transaction. Especially when dealing with sensitive personal information – whether corporate data, billing information, or private medical records.

But the increased risk of fraud, identity theft, and cyber threats has driven rapid digital transformation. For businesses and consumers making digital transactions, trust is paramount – especially in the post-pandemic world.

Technologies like biometrics and AI are increasingly important in creating trust, managing verification and authentication, and preventing fraud.

As organisations and customers become increasingly digital, there's only one way to establish and maintain trust. That's to verify the customer and business is legitimate before they even connect to a service or customer, and then tie every transaction to a verified self-sovereign identity – thus closing the loop.

At Nuggets, we've developed solutions that deliver trusted transactions. This means everything from compliance concerns, tying IDs to payments, and even transferring identification to a new device while preserving trust.

Companies don't need a kit of parts. They need a fully formed model for their use cases. By deploying our white label identity service in the way that suits you and your customers, you can meet regulatory requirements while also massively improving customer experience.

As businesses continue to adapt to the demands of rapid digital transformation, there will be more change, and uncertainty. Omnichannel solutions will be more important than ever, with customers and businesses relying heavily on electronic transactions. Trust and identity has never been as important as it is now.

Most importantly, companies will be able to grow and create value at all levels by building trust with customers, and embedding that trust into all forms of data.

Welcome to the era of trust.

About Us

TRUSTED PAYMENTS

Nuggets is a trust solution. The platform enables trusted transactions through verified self-sovereign identity.

SELF-SOVEREIGN DIGITAL IDENTITIES

Whether you're a bank, insurer, subscription service, telco or logistics company, Nuggets self-sovereign identity allows you to deliver on your regulatory expectations while building a competitive advantage. For your consumers, it offers greater convenience, confidence and choice.

PERSONAL CLOUD VAULT

With Nuggets, consumers get back control of their data, and you become a champion of trust.

AUDITABLE NUGGETS OF DATA

We make trusted identity work for both consumers and for businesses – for every login, every purchase, every service request, and every delivery.

Contact us now to discover how Nuggets' trust solution can help your organisation.

+44 20 3286 0522
partners@nuggets.life
www.nuggets.life

nuggets