Back to the Future

Revolutionising Digital ID with new technology and centuries old governance

Stephen Wilson, Richard Mallam

June, 2024

Back to the future

Revolutionising Digital ID with new technology and centuries old governance

We believe that the establishment of Verifiable Credential technology is a back-to-the-future moment.

At last, the many nuanced ways in which we prove things about ourselves online can mirror the familiar processes that have organised and governed real world credentials for hundreds of years. In this new world, an authorised government agency, bank or educational body can issue secure digital credentials directly to citizens, customers and students. It is a world in which you can *prove* your license, membership card or student ID, and everyone will know that you and only you hold that credential. It is a world in which you can't be impersonated.

Our mission at Verified Orchestration is to enable this back-to-the-future digital world. We want to lower the learning curve, reduce the cost and increase the value of Verifiable Credential technology, while retaining the established governance structures and contexts within which all important credentials operate. We want to work within your organisations' established processes and systems, augmenting rather than revolutionising, improving rather than sacrificing. We want to bring trust back to your digital world.

Any change can be daunting, with a large majority of IT change programs encumbered by people, process and technology issues. We have built Verified Orchestration to reduce this risk for you – providing intuitive user experiences, working within your processes and providing robust, globally available technology. This change can happen incrementally and organically, but it has the potential to revolutionise how we all engage with the digital world around us.

© Verified Orchestration Pty Ltd
June 2024

Verifiable Credentials are new again

Verifiable Credentials have been around for a long time. As a reader of this White Paper, you have more than likely used Verifiable Credentials without knowing it. They are commonplace, embedded in mobile phones, payment cards, e-passports, smart phones and smart watches.

So, what is a Verifiable Credential?

The mobile phone SIM is an early example and provides a perfect explainer. “SIM” stands for Subscriber Identification Module and is both a special purpose integrated circuit and an administrative record. The SIM holds an official copy of your account information and your unique international subscriber number, all of which is digitally signed by your phone company. The SIM also holds a unique cryptographic key which is used by the handset to digitally sign (in simple terms, “mark”) the start and stop of every call you make. This signature is verifiable by network operators globally and allows them to know which subscriber is making which call from what location, anywhere in the world.

The global cell phone network could not function without Verifiable Credentials. The same goes for global credit card payments. The EMV chip card system replaced magnetic stripe cards long ago, which were vulnerable to skimming and counterfeiting. Instead of a magnetic stripe storing and passively transferring cardholder data to a terminal, the chip card carries a Verifiable Credential holding the cardholder data, a cardholder key, and the signature (endorsement) of the issuing bank. Every payment made with the chip card is signed (marked) by the cardholder key, rendering it tamper resistant and globally reconcilable.

Verifiable Credentials are a technology that puts instrumental pieces of information about individuals into the hands of those individuals and empowers them to present that information directly, purposefully and securely. Verifiable Credentials are decentralised in that the information they carry is valid on its face and can be presented directly, peer to peer, without intermediation. Verifiable Credentials enable empowerment, security, privacy and convenience of decentralised presentation with the benefit of centralised governance and veracity standards.

© Verified Orchestration Pty Ltd
June 2024

Verifiable Credentials and the identity problem

Verifiable Credentials have been used for decades but they have been reenergised lately to help solve digital identity. SIMs and EMV cards are highly specialised, dedicated to singular applications, with proprietary standards overseen by industry associations, and bound to physical chips. Today, Verifiable Credentials are being standardised by several global working groups, with a view to countless extended use cases and end user applications.

Why the shift to Verifiable Credentials?

The way we handle most identity information online has historically followed a distinctly centralised pattern. Instead of placing identity information into the hands of you the holder, it tends to be added to a database on a server on your behalf where it sits waiting to be exercised. To make anything happen with this information, you the holder are required to activate it on the server somehow (usually by quoting a plaintext username and password) triggering a cascade of actions “in your name”. Internet banking, online shopping, remote workflows, e-health, e-government travel booking, ticketing and so on all follow the same pattern.

This centralised disjointed proxy management of our affairs is soothingly referred to as “digital identity”. If you think about it, centralised identity management is instinctively odd. Imagine if we handled driver’s licenses in the same way as current online identity: the motor vehicle registry would ask you to give your license back to them, and in its place issue you a username and password to access it and release it whenever you happen to need it.

It would be incredibly inconvenient and laborious. More significantly, your licence would be placed at constant risk of criminal abuse because your username and password can easily be stolen, and all the sensitive personal data associated with your licence exposed.

© Verified Orchestration Pty Ltd
June 2024

In an AI-enabled world, this threat grows exponentially worse. Generative language and visualisation models now create compelling Deep Fakes of your personal traits, your voice, even your appearance, sufficient to trick biometrics algorithms and human gatekeepers. Traditional approaches to Digital Identity thus don't make sense; we need a change.

Why is digital identity the way it is?

The online world has followed this unreal pattern ever since the "Identity Metasystem" was published in 2006. The Identity Metasystem described a now-classical arrangement in which a Subject and a Relying Party deal with each other using information about the Subject from a third-party Identity Provider. The three-party model is entirely reasonable, however the Identity Metasystem also specified that most interactions would draw down identity information in real time. But technology changes…

The new wave of interest in Verifiable Credentials crystalised in July 2018 when the World Wide Web consortium (W3C) released the Verifiable Credentials Data Model 1.0 with the byline Expressing verifiable information on the Web.

Verifiable Credentials are revolutionary digital technology, placing cryptographic keys under the sole control of the credential holder, making credentials highly resistant to theft, counterfeiting or takeover. The new wave of standards now allows secure customised Verifiable Credentials to be carried in mobile digital wallets and used in a range of business applications to reliably prove particular endorsed facts and figures.

© Verified Orchestration Pty Ltd
June 2024

Core concepts: recap

What is a credential?

The word “credential” has several meanings.

In this paper, we try to avoid technicalities. We use “credential” in the everyday sense of the word, remaining aware that it varies. A credential is generally a qualification or entitlement, which is given to you by an authority of some sort. Common credentials include driver licences, educational qualifications, professional memberships, Medicare or other social security cards, health system identifiers, tax file numbers, employee ID cards, student ID cards, citizenship certificates and passports.

A credential can be evidenced by a physical thing such as a paper certificate or plastic card, which you can conveniently show to another person to prove you hold a certain qualification or entitlement, represented by the thing. On the other hand, a credential can be more abstract; it can be the fact that you are qualified or entitled to something by virtue of a process you have gone through.

Credentialing

Credentialing is the word used for the detailed processes that lead to someone holding a specific credential. Often complicated; often rules-bound (legislation, professional charters, international conventions). Important credentialing can be restricted by law to designated authorities.

There is more to digitising a real-world credential than capturing a convenient image of it. Examples of the properties and processes that need to be respected include:

- Important physical credentials such as licences typically have anti-counterfeiting features such as watermarks and microprinting

© Verified Orchestration Pty Ltd
June 2024

- Photographs are standard on driver licences and passports as a means to mitigate the risk of an imposter trying to present a stolen credential
- There is often a tightly managed supply chain behind the production of especially sensitive credentials; special paper for example is used for printing passports; bank card production plants will screen their employees and deploy strong building security measures
- Credentialing organisations such as universities and hospitals will usually be accredited under government regulations, and subject to regular quality audits, which enables their credentials to be trusted nationally and internationally.

Cryptographically Verifiable Credentials

Since Stanford researchers Whitfield Diffie and Martin Hellman released their 1976 paper *New Directions in Cryptography* introducing public key encryption, we have been able to reliably secure communications between two parties on a public network.

A critical feature of public key encryption is that any data can be "signed" with the private key and verified by anyone with the public key, providing assurance that the data originated from the holder of the private key without that private key being exposed. Public key signatures are what enable authenticity and agency for digital workflows, authorisations, and credentials.

As mentioned, SIMs and EMV cards have embodied Verifiable Credentials for many years in tightly constrained applications (telephony billing and credit/debit payments). The past few years have seen the technology decoupled from special purpose chips and standardised in open communities, enabling broader application, even democratisation of the way data is controlled.

The best-known contemporary Verifiable Credential standards are being developed by the World Wide Web Consortium (W3C) and the International Organisation for Standardisation (ISO) mobile driver licence (mDL) Working Group 10. W3C verifiable credentials will be truly open and highly customisable; mDL Verifiable Credentials are likely to be constrained to driver licensing and government ID use cases.

© Verified Orchestration Pty Ltd
June 2024

Convergence of all these technology advancements means that one party (an issuer) can evidence the creation of particular data and securely provide this unique data to another individual (a holder). In other words, *signed* data can be regarded as *original*. The proliferation of mobile computing also means that every individual can bind all sorts of unique data and workflows to their own private keys, leveraging these digital assets on a personal device that is always connected to an open global network. For the first time in history, we can finally express the way we have been dealing with credentials in the physical world in a digital manner.

Provenance and verifiable presentation

Let's briefly look more closely at the power of digitally signed data. What is it exactly that verifiable credentials allow us to verify?

Firstly, the best-known property of verifiable credentials is provenance of the issuer. A verifiable credential is a data structure in a standard format (e.g. W3C or ISO mDL) which is digitally signed by or on behalf of the issuer. This static signature proves cryptographically that the Verifiable Credential must have originated from that particular issuer. The issuer signature can be chained through additional credentials that confer issuer metadata such as the audit status of the issuer, or the source of the issuer's authority.

Secondly, in most cases a verifiable credential includes a public key of the credential holder, matched to a private key they hold in a wallet. That private key can be used (automatically, inside the wallet software) to sign any presentation of the credential. This dynamic signature protects the integrity of each presentation of the credential, and the integrity of any transaction that is created using the credential.

A verifiable credential wallet is generally locked by a biometric or PIN; the private keys within the wallet cannot be used unless the wallet is unlocked by its owner. Therefore, the existence of a signed piece of data that is verified by the holder's public key is strong evidence that the data originated from the wallet's owner. This is verifiable presentation (aka proof of possession) and is almost as important as credential provenance, for it allows digital workflows to be confidently attributed to specific actors, both humans and devices.

© Verified Orchestration Pty Ltd
June 2024

Example 1: Verifiable Credential student cards

A student Alice holds a verifiable credential issued by her university and carried on her smartphone within an app. The Verifiable Credential includes Alice's student number, her library privileges, and course of study. Alice uses her credential to order library materials via online forms which are prefilled with the relevant verified details. She also undertakes online exams and submits them via her app which applies an indelible signature using her Verifiable Credential. Some of the facilities on Alice's campus use electronic access control; she can open the door to her lab by opening her app and presenting her mobile phone to a reader.

Example 2: EMV payment cards

"EMV" standards for Europay Mastercard Visa, the original founders of the payment smartcard standard that supplanted magnetic stripe cards and more or less eliminated card present fraud. Card holder details in an EMV card are formatted in a proprietary credential structure and signed by the issuing bank. At the merchant point of sale, the cardholder inserts their card and unlocks it thus signalling consent; the chip embedded in the card digitally signs a dynamic packet of data (including the purchase and card holder details) which is sent to the merchant terminal, verified with respect to both the cardholder chip and the issuing bank, and then forwarded into the payment network for processing. The combination of static signature of the issuing bank, dynamic signature of the chip over the transaction, and the PIN lock provide solid evidence that the legitimate cardholder was in control of the purchase at the time and place it was made.

© Verified Orchestration Pty Ltd
June 2024

Digital functionality and security

Decentralised Presentation

A cryptographically verifiable credential is *verifiable on its face*; that is, the Verifier doesn't need to "call home" to check the validity because the static signature of the issuer can be verified offline (if the endpoint has a reliable copy of the issuer public key).

Technically, everyone can now carry their own authenticator in their pocket, assuming their mobile device is compatible.

Credentials are presented peer-to-peer or peer-to-application. The direct presentation mode is faster, more private and lower cost. The economic impact of this shift is profound. By moving credential verification to the edge, back-office processing is reduced and the attack surface for fraud and identity theft is much reduced. Cryptographically assured processes produce enhanced audit trails and greater certainty for all stakeholders.

Trust in an untrustworthy world

The dizzying advance of generative AI is shaking our sense of what's true and what's not, now that so much of our professional and personal time is spent online. Convincing deep fakes of targeted individuals are being used to misappropriate creative works and to spoof biometric security systems. Grave fears are held for the integrity of democratic elections with social media being flooded with synthetic likenesses preaching messages for and against all sides

How can regular people regain reasonable "baseline" levels of trust in what they read and see? Some level of scepticism is healthy of course but civilisation as we know it might grind to a halt if citizens have to mistrust everything. How will we

© Verified Orchestration Pty Ltd
June 2024

consume mass media, read emails, make payments, answer the phone, or work remotely and securely if we can't trust the digital medium?

Verifiable credentials are part of the answer.

Watermarking of synthetic images and originals will utilise Verifiable Credentials issued to algorithms on the one hand and human creators on the other. Device-bound private keys – sometimes referred to as having *hardware roots of trust* – cannot be defeated by software and provide the ultimate means to verify digital content. AIs can create real time moving image replicas of you, but no LLM can reproduce your private key or counterfeit your device-bound digital wallet.

As the former head of the U.S. National Strategy for Trusted Identities in Cyberspace, Jeremy Grant recently said, "one thing AI does not know how to defeat is public key cryptography" (https://www.makingdatabetter.com/2195663/13928793-ep5-navigating-digital-id-the-role-of-government).

- In banking, Verifiable Credentials will combat the new waves of fraud perpetrated through synthetic identities, and improve know-your-customer (KYC) processes by rendering government issued IDs impervious to theft and replay
- In education, verifiable student IDs are key to avoid imposters in remote learning, and to ensure tamper-resistant qualifications and micro-credentials are in the right hands
- Professional bodies and licensing agencies will Use Verifiable Credentials to carry trade certificates so central to workplace safety especially in high-flux industries such as resources, energy, construction and hospitality
- In enterprise, businesses will issue contractor IDs and training certificates using Verifiable Credentials to ensure workers are trained, compliant and known to the organisation, improving outcomes in distributed and integrated workforces

© Verified Orchestration Pty Ltd
June 2024

Table 1: Functionality and security of credentials by form factor

Credential function	Form factor		
	Plastic card	**Traditional Digital Model: database lookup by credential identifier**	**Verifiable Credential**
Uniqueness; anti-counterfeiting	Guilloche printing, holograms, microprinting.	No assurance once credential data has been read from database.	Digital signature of issuer assures provenance.
Proof of possession	Holder's photograph on the card confirms it has not been stolen.	None; anyone who knows the credential ID can act as the holder.	Digital wallet unlocked by biometric or PIN enables each presentation to be uniquely signed using the holder private key.
Transferability	Uncontrollable; limited by photo only when card is presented to another human.	Uncontrollable; credentials sharing may be deliberate or malicious.	Non-transferable (only via re-issuance).
Biometric assurance	In-person assessment of photo on the card against the person holding the card.	Only when enforced by biometric authentication.	Digital biometric verification controls every presentation from the wallet.
Security of procurement	Production complexity; blank card stock control; operator personnel security; production standards certification.	Database security; operator personnel security; database access encryption (SSL/TLS or similar); multifactor authentication.	As per plastic card.
Credential data carried	Very little, constrained by human readable typeface, magnetic stripe capacity, 2D barcodes etc. ~100 bytes.	Unlimited.	Moderate; no intrinsic limit to capacity of a VC data structure but there is no point overloading the mobile device. ~100KB.
Verification	In person, human-to-human. Online via IDV API or image sharing.	Digital, via API to issuer.	Digitally native; independent of issuer. Mobile device to device (QR code or NFC "tap") or mobile device to server ("click").
Verifiers	Anyone.	Integrated verifiers.	Anyone with a compatible application.
Verification Complexity	Low.	High.	Low.

© Verified Orchestration Pty Ltd
June 2024

The importance of context

Credentials are meaningful only in context.

A credential generally conveys some sort of entitlement or an authorisation to act, conferred by the credential issuer. The issuer is recognised as authoritative by a community of interest, the members of which rely on the credentialing process to ensure that only fit and proper people are holding appropriate credentials. The rigour and strictness of the process vary depending on context; it is natural that the credentialling of students, sporting officials and air traffic controllers will be very different. It is possible that an air traffic controller works weekends as a soccer referee and is enrolled in an Indonesian language course. That person might therefore hold three different credentials, but will have no difficulty knowing which role they are performing at any time. If they carried Verifiable Credentials, they would probably be associated with distinct applications which would be invoked more or less automatically as the person activates the appropriate app for their current activity.

A credential — whether it is the abstract or physical instance — is taken to mean that the holder has satisfied a credentialing process — nothing more and nothing less. The credential doesn't usually mean anything outside the community of interest, in other contexts.

A credentialing process is usually treated as a "black box". The credential holders experience the process firsthand, but other members of the broader community of interest might not need to know the details and still trust that there are rules and controls to ensure the integrity and meaning of the credential.

In the digital world, context is usually manifest in community specific transaction software, made available only to the appropriately qualified users, perhaps activated by an appropriate credential and which creates a user experience in which the user knows what credential to present.

© Verified Orchestration Pty Ltd
June 2024

Example 3: Solicitor credentials

In Australia, solicitors are a type of legal professional governed by professional societies. To be credentialled as a solicitor, one must attain an appropriate law degree, meet various professional requirements, agree to the society's rules, and maintain a continuing education load. Membership of the law society is renewed periodically and with it, the solicitor's credentials.

Certain important functions in our society are reserved for solicitors, such as the preparation of wills and real estate conveyancing. The advent of electronic conveyancing has transformed the speed and efficiency of many property sales by allowing settlement to happen remotely and asynchronously (paper conveyancing used to require vendors' and buyers' solicitors to meet face to face to sign deed documents).

Ordinary citizens buying and selling real estate appreciate they are protected by the law and the professional processes that govern the solicitors, without knowing anything at all about those processes.

What is a natural issuer?

With so many different business contexts, credentialling processes and governance arrangements, in most cases, each credential only has one "natural issuer", responsible for how the credential relates to its community of interest.

When adopting Verifiable Credentials, these natural issuers continue to occupy their established trusted role in the ecosystem. But they can avoid the complexity of integrating cryptographic technologies into their credentialing processes by simply outsourcing the Verifiable Credential production just as they have probably outsourced plastic card production for physical credentials to date.

The new verifiable credential should have exactly the same meaning as the old plastic card: both are tangible evidence that the holder has been credentialed. Of course, there is so much more that we can do when holding a secure digital credential compared with inert plastic, but the salient point here is that the

© Verified Orchestration Pty Ltd
June 2024

procurement of Verifiable Credentials by natural issuers follows the established principles of outsourced physical credential production, where the enterprise retains control of credentialing and conditions for use, while a specialist provider is engaged in the technical matters of production and distribution.

Table 2: Examples of natural issuers

Domain	Issuer	Participants	Credential
Employment	Tax Office	Workers	Tax File Number
	Employer	Employees Contractors	Staff ID
Public Health	Medicare	Patients	Medicare Card
	Medicare	Healthcare providers	Provider Number Prescriber number
Private Health	Medical colleges	Specialists	Specialisation
	Private hospitals	Contracted doctors	Admissions privileges Billing contracts
International Travel	Dept of Foreign Affairs	Travellers	Passport
	Governments	Visitors Immigrants	Visa
Professional bodies	Professional bodies	Workers	Member ID Certifications
Tertiary Education	Universities	Students	Student ID Degrees Certifications
Secondary Education	High Schools	Students	Student ID Matriculation certificate
Sports	Sporting bodies	Players	Membership Card
	Clubs	Members	Membership Card
Trade	Registered Training Organisation	Tradespeople	Trade licence
Retirement Fund	Pension funds	Workers	Membership ID
Credit cards	Issuing bank	Cardholder	Credit card number
Global cell phone system	Telco	Subscriber	SIM
Adult goods & services	Roads Authority or state government	Customers	Proof of Age

© Verified Orchestration Pty Ltd
June 2024

Realising the re/evolution?

The Self Sovereign Identity (SSI) movement has sought to leverage Verifiable Credentials to reclaim control of data and digital power. The more ambitious SSI projects reject "administered identity" and seek to empower individuals with bring-your-own decentralised identifiers (DIDs) that are minted on a blockchain. The newest Verifiable Credential protocols are also informed by blockchain architectures, with the objective of decoupling from establishment identification and resource management.

Occasionally, self-sufficient digital communities will break away from the establishment and happily manage their own affairs, bartering for goods and services using cryptocurrency, privileging individuality, and providing for all-new self-ordained digital guises.

At the extreme, this sort of brave new world appeals to a narrow fundamentally libertarian faction, where individuals desire autonomy and embrace the responsibility for technology that is entailed. They happily roll-their-own cryptography, maintain private key wallets using open-source tools, and do their own research to check the back-story of all the parties they deal with including credential issuers.

Such break-away communities are free to recognise people and peoples' abilities in whatever way they like. But as the SSI movement evolved and sought to bring change to mainstream life, it quickly found that self-asserted claims and self-issued credentials are of limited use. Most important credentials derive from third parties that are recognised by larger sets of stakeholders as authoritative over certain qualifications or entitlements.

As we've seen, real world credentialling involves rules and quality controls (audits and certifications) that substantiate how credentials are assigned. The backstory of an issuer (reputation, regulations, charters, audit and so on) underpins the meaning and dependability of its credentials.

For many natural issuers, the more extreme self-sufficient approach is cumbersome, brings little benefit, and carries real regulatory risk.

© Verified Orchestration Pty Ltd
June 2024

It is undeniable that there is strong resistance to change, around the world, and certainly here in Australia. There are valid concerns about relying on untested decentralised infrastructure for many of their most sensitive interactions.

We see this as a false choice.

We approach the problem differently. We see the power of Verifiable Credentials as augmenting and strengthening processes and governance that have stood the test of time, rather than replacing them. We exponentially improve identity outcomes, without ruining your business. Importantly, we leverage global scale infrastructure used by almost all organisations and natively integrate to the productivity suite.

Verifiable Credentials can be managed within existing hierarchical credentialling processes, and capture the backstory of each issuer. Different issuers get their authority in different ways. Some are chartered or legislated; others are community organisations that operate under a social contract; some issuers are entirely commercial in nature. Issuers are often audited; some are additionally accredited under strict conditions. Generally speaking, the stricter the rules under which an issuer operates, the greater the certainty of its credentials.

Nothing is ever perfect; sometimes things go wrong. In a tightly governed credentialing ecosystem, parties (both individual and business) enjoy a spectrum of protections, including warranties, liability limits, redress mechanisms, and compensation schemes. These protections do not come for free; they come within a regulatory and/or social context.

Creating contextual trusted ecosystems

Historically, humans have established trust through direct relationships within a circle of well-known counterparts. As our world has expanded, the methods of establishing trust also changed. Printed identity documents were first recorded in the 1400s, but only became ubiquitous during and after the industrial revolution.

In today's modern world, it is now common for citizens to have relationships with tens or even hundreds of organisations at any one time. Through this lens, we see contextual trust ecosystems everywhere – in government and citizens, education

© Verified Orchestration Pty Ltd
June 2024

providers and students, sporting bodies and players, businesses and customers and employees.

Technology has fundamentally reshaped the trust at the core of these contextual ecosystems. No longer are customers dealing with bank tellers and branch managers; rather, transactions are facilitated by machines and online banking platforms. While technological progress has brought huge benefits, it has also carried cost, most notably through cybercrime, scamming, impersonation and account takeovers that are prevalent in our online world.

The next technological paradigm shift, AI, will bring global benefits, but it will also exponentially worsen quantitative and qualitative cyber risks. AI-enabled deepfake technology, among other AI-enabled attack vectors, will undermine our trust in institutions, organisations, government and individuals.

Governments, professional organisations, educational institutions, training providers, sporting bodies, banks, health providers and employers all have a responsibility to create, support and maintain their contextual trusted ecosystems. In an AI-enabled world, Verifiable Credential technology will become a cornerstone technology in achieving this outcome.

Unlocking the power of technology with you

Verifiable Credentials technology is available today to help organisations empower their members to exercise their relationships, entitlements and qualifications online, securely and seamlessly. Whether you are a bank with customers, health provider with employees, enterprise with an integrated workforce, training organisation with students, or a government with citizens, you can issue Verifiable Credentials that prove who your people are and what they are authorised to do in the digital world.

But you will need a partner to join your trusted credentialling process to the backend supply chain of cryptographic credentials and distribution to wallets.

Verified Orchestration is that partner.

© Verified Orchestration Pty Ltd
June 2024

We provide you all the benefits of Verifiable Credential technology, manage the complexity, work within your established processes, and provide simple integration interfaces, coupled with a delightful end-user experience.

We leverage globally available, deeply trusted infrastructure. We have a flexible and adaptable platform for customising verifiable credentials to your community and its applications. We enable the system shift incrementally, locally and organically.

Our mission at Verified Orchestration is to enable a back-to-the-future digital world. It is a world in which tried and tested processes and governance, coupled with game-changing technology, create, support and maintain your trusted ecosystem.

In our modern world, the time to act is now.

© Verified Orchestration Pty Ltd
June 2024