| Whitepaper |

AU10TIX

IDENTITY INTELLIGENCE

Next IDV

Tomorrow's Security Starts with Today's Privacy: Changing the Way We Approach Identity Verification with Decentralized Verified Credentials

WWW.AU10TIX.COM

Next IDV

It's clear that today's data privacy strategies are falling short.

As data volumes compound, organizations are faced with an insurmountable challenge: keeping data secure both to protect consumers' privacy and meeting ever-evolving compliance requirements. Yet these strategies often fall short of preventing data breaches, and consumers continue to lose trust in organizations.

In fact, **86% of American consumers** say they're increasingly concerned about data privacy, and companies don't blame them; 33% of business leaders admit that worry is valid and consumers should be wary of how organizations treat their data. With such low confidence in how companies manage data, it's no surprise that identity verification is a particularly sore subject for consumers and organizations alike.

Identity verification (IDV) plays an important role in modern society. Authenticating users, customers, employees, and citizens is critical to maintaining integrity and security by ensuring people are who they claim to be. However, the time-tested ways of ID verification—including saving personal information in a corporate directory, database, or secrets vault—may expose people's personally identifiable information (PII) to a higher risk of exposure and fraud.

That's why AU10TIX, a trusted leader in the identity verification space, is introducing the next generation of IDV that helps put individuals' private information back in their hands.

AU10TIX has partnered with Microsoft's Active Directory to fundamentally change how businesses—and the people who power them—approach identity verification with decentralized verified credentials (VC). While this transformational shift has been on the horizon, Web3 and blockchain capabilities have finally made this goal a reality available on a global scale.

By leveraging decentralized Web3 technology, users can gain newfound control over their identities and companies can verify user identities without the responsibility of keeping that data secure in their own directories.

Now is the time to prioritize better, decentralized data privacy. But decentralized VC is only possible if we collectively abandon a company-based privacy approach and adopt a community-based approach instead. Here's everything you need to know to prepare for the changes ahead.

What Is Decentralized VC?

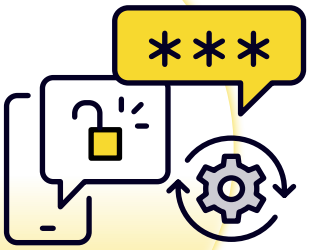
Decentralized verified credentials—or **decentralized VC**—is a component of digital identity management that allows users to confirm their identity without providing copies of personal documents.

Decentralized identity management allows users to store and encrypt documentation like passports, driver's licenses, insurance cards, and credit cards in secure blocks. These decentralized identifiers are verified and combined in a unified digital wallet on a blockchain, containing the user's single sovereign identity.

With this technology, users can independently maintain their digital identities and prove that they are who they claim to be—without exposing their private information. That opens the door for users to quickly verify their identity with **zero-knowledge proof** to onboard at a new job, receive government benefits, or even pay for their morning coffee.

Why Is Decentralized VC Important?

Protecting sensitive data is becoming progressively more difficult for organizations. Even with the latest cybersecurity measures in place, data breaches are a dime a dozen, and maintaining sensitive data remains a huge risk. Yet many companies are required by law to retain and secure data for years. For example, healthcare companies are frequent targets for data breaches because they're required to keep personal health data for six years under HIPAA regulations.



Unsurprisingly, these data breaches make customers, employees, and citizens wary about sharing their personal data. But for many, providing this data feels like a necessary evil to gain access to the resources and opportunities they need. It's no wonder that the **average consumer's data is stored by 350 companies** at any given time.

But consumers don't want organizations to maintain copies of their PII. Organizations don't want the onus of protecting more data either.

That's why decentralized VC is necessary: to reinvigorate the trust between consumers and organizations.

Often, organizations don't need to save passport photocopies, credit card numbers, or insurance information once it has been verified; they simply need this information to prove a consumer is who they claim to be. Validating identity with decentralized VC is a powerful way to streamline processes, store less data, and reduce costs for financial processes and outsourced verification.

Plus, a decentralized virtual wallet makes it easy for consumers to authenticate their identity while maintaining control over what information they provide organizations. When a user retains ownership of their self-sovereign identity—both online and offline—they have more control over

their privacy and personal data, making them less susceptible to fraud or identity theft.

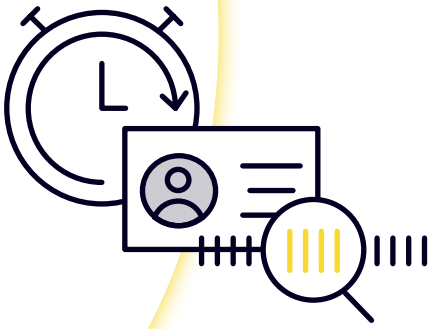
How Does Decentralized VC Work?

1. Verifying credentials starts when a user authenticates their identity in person. For example, a person could verify their identity with their local government using a photo ID. That photo ID is a decentralized identifier (DID) that serves as the first block on your digital identity blockchain. The verified ID information is then added to your digital wallet, proving you are the person pictured on that photo ID.

2. From there, users can add different DID to their wallet by creating new blocks. For example, once their name on their ID is verified, they can request a copy of their diploma issued to the same name ID from their university. This diploma creates the second block on the digital wallet blockchain. If a future employer wanted to verify their education, the user could instantly validate that they graduated from a particular university by sharing that information from their digital wallet.

3. Decentralized verified contextual credentials—and the blocks that make up a user's digital identity—are securely stored in a repository on Web3's decentralized global blockchain infrastructure. The repository caches information with cryptography, allowing users to upload whatever DID they want or need into their digital wallet. Users can access a single application to manage their identity and instantly provide the proof needed for organizations to verify their identity.

4. Soon, users may be able to verify their identity without in-person authentication too. Leveraging biometric authentication features can make it even easier for people to verify their credentials or prove their identity in an instant. For example, if a verified fingerprint was part of a user's digital wallet, they could potentially use a fingerprint reader to automatically pay for lunch or check in for a foreign flight without ever sharing a credit card or passport.



What Are the Main Features of Decentralized VC?

Aside from the clear privacy benefits decentralized VC provides users, the features and benefits of contextual credentials go far beyond empowering users to maintain their identities.

Global decentralized VC is incredibly cost effective, reducing many of the costs organizations and governments currently face from processing paperwork, verifying identification, and securing and storing huge volumes of data. This innovation can also speed up verification processes like onboarding employees for a new job, approving citizens for government support, or verifying patient health insurance.

Since blockchain technology maintains detailed logs of transactions and ownership, organizations can easily demonstrate compliance with local privacy laws. This provides transparency and simplifies auditing to prevent mistakes or resolve them more quickly.

Since there is no central authority managing the decentralized VC repository, digital wallets remain fully tamperproof. Yet with buildable, customizable networks, users and enterprises can create a more trusting relationship and quickly share information without giving organizations unfettered access to personal data.

How Can Different Organizations Use Decentralized VC?

Naturally, individuals have to maintain different relationships with multiple organizations. An employee may not want to share the same information with their employer as they do with their government, their doctor, or their local gym.

Decentralized VC allows users to freely share the information they want to share and safely conceal the rest, so they can maintain boundaries around their personal information. For organizations, they benefit when they receive only the information they need to verify a user's identity, so they don't have to request, copy, process, store, and manage multiple users' sensitive data.

Business and government leaders have a huge opportunity to foster trust by adopting decentralized VC early. By demonstrating that they take personal privacy seriously, leaders can restore a strong relationship with users while streamlining operating processes.

Here's how each organization type can benefit from decentralized VC.

B2B

Due diligence is a crucial step in developing lasting and trusting relationships between businesses. While not all businesses are legally required to follow **Know Your Business Standards**, every business benefits from verifying their vendors.

Decentralized verified credentials allow companies to share relevant, encrypted business data securely with other businesses during onboarding. In response to an RFP, a business can use decentralized VC to automatically share information like company ownership documents, tax information, and insurance policies.

For companies that need to report on their vendors to meet compliance regulations, a transparent blockchain transaction log makes it easy to streamline auditing and demonstrate payments. Decentralized VC can also allow businesses to pay for services without directly sharing business credit card or bank account information.

B2C

Many consumers are wary of sharing their personal information with businesses, but decentralized VC makes it easy for customers to pay for things quickly, easily, and securely both online and in person.

Customers can pay for items using cryptocurrency or a connected credit card stored in their digital wallet, speeding up service times and reducing payment processing issues. If customers are buying age-restricted or location-restricted items, companies can also request instant verification of the customer's age or location before completing the transaction.

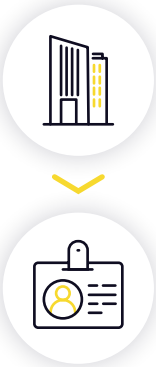
Decentralized VC can also help companies develop a stronger relationship with customers. Many local businesses leverage reward clubs or loyalty programs to generate repeat business. With customers able to automatically provide their membership information within their digital wallet or with biometric authentication, companies can gain the data they need to track returning customer preferences without connecting that data to a user's private information, like a phone number or email address.

B2B2C

Large marketplaces and middleman businesses perform double the identity verification to create a trusting relationship between sellers and buyers. But with decentralized VC, B2B2C businesses can streamline verification processes and reduce fraudulent sales or purchases on their platform.

These businesses use decentralized VC to provide confidentiality for both customers and sellers. For example, by verifying customer information, businesses can rapidly ship out products to the right buyers without giving sellers direct access to buyer addresses or credit card information. Meanwhile, platforms can also verify sellers to confirm they are legitimate, legal vendors and provide the proper tax paperwork without requesting documentation.

By streamlining the verification process, the middleman business can collect payment from customers faster and confidently remit payment to sellers sooner, so sellers could receive their payout even before their product reaches the customer's door.



B2E

Employers are notorious for paperwork-heavy hiring processes, but with decentralized VC, weeks spent onboarding are a thing of the past.

Right from the beginning of the application process, applicants can verify their qualification for a position, making hiring significantly easier. Then, once a candidate is selected, new hires can prove their identity, education, and past work experience at the click of a button, eliminating the need for third-party background checks and identity verification.

Companies can also use decentralized VC to improve their security posture by allowing employees to access approved resources with biometrics or automated authentication. This eliminates the need for traditional IAM

technology or tools like single sign-on or multifactor authentication, which can save companies money on IT and HR resources.

B2G

Both citizens and businesses need to regularly interact with their local government, but decentralized VC makes it easy to cut through red tape.

For example, waiting at the DMV to renew a driver's license could be a thing of the past. Citizens can verify their identity and securely reapply for their license from home. Decentralized VC can also help citizens gain faster access to government services like unemployment, Social Security benefits, or child support.

Meanwhile, companies working as government contractors can use decentralized VC to verify an individual worker's security clearance, access records and government systems, and streamline payments.

It's Up to Us to Create a Safer World

While the technology for contextual credentials is at our fingertips, we still have a way to go to make decentralized VC a reality.

As security professionals, it's easy to get excited about all the possibilities decentralized VC offers and overlook the understandable reservations consumers may have about securing their identities with blockchain technology. But by minting a new standard for how we verify identities and demonstrating our commitment to protecting consumer data, we can usher in the future of self-sovereign identity management.

However, that future starts with abandoning the company-first style of managing individual user profiles, and instead, considering more universal ways to shift into community-based identity verification.

Ultimately, decentralized VC is only possible through a global community effort. It's up to us—the ID community at large—to band together and commit to creating a safer, more secure world.

Will you join us? Learn more about how AU10TIX is leading the way with verifiable credentials.
Book a customized demo today.