

Testimony of Cody Carbone President and CEO, The Digital Chamber House Committee on Veterans' Affairs Subcommittee on Oversight & Investigations

June 11, 2025

Chairwoman Kiggans, Ranking Member Ramirez, and distinguished members of the Subcommittee, thank you for the opportunity to testify before you this morning. My name is Cody Carbone, and I proudly serve as the President and CEO of The Digital Chamber.

The Digital Chamber is a non-profit trade organization committed to promoting blockchain adoption. We envision a fair and inclusive digital and financial ecosystem where everyone has the opportunity to participate. I am here today on behalf of our membership, representing over 200 companies across the globe.

We sincerely appreciate the Subcommittee's interest in harnessing emerging technologies to enhance the services provided to those who have served our nation. Congresswoman Nancy Mace has introduced H.R. 3455, the "Veterans Affairs Distributed Ledger Innovation Act of 2025," directing the U.S. Department of Veterans Affairs (VA) to study how blockchain technology can revolutionize the delivery of veterans' benefits and services. Her efforts highlight bipartisan recognition that outdated 20th-century systems are failing our veterans and that modern tools like blockchain must be explored.

Why Modernization Can't Wait

Blockchain has the potential to transform the VA. The VA possesses a commendable history of innovation, ranging from the pioneering implementation of electronic medical records to recent advancements in cloud computing and artificial intelligence. However, many of the legacy systems that once placed the VA at the cutting edge are now straining under 21st-century demands, leading to slowing claims, fragmenting health records, and leaving veterans to navigate a maze of paper and outdated portals.

The VA provides critical benefits and care to a community of nearly 17 million U.S. military veterans, along with their families and survivors. Ensuring that these veterans receive efficient, transparent, and reliable services must be a national priority. We stand at a moment when the digital revolution can be utilized in the service of those who served us.

What is Blockchain?

Blockchain is a digital ledger that's shared across multiple computers, or nodes. When a record is written, it is cryptographically sealed into a time-stamped *block* that also contains the fingerprint (hash) of the block before it. If anyone tries to alter a past entry, every subsequent fingerprint breaks—making tampering immediately obvious and preventable. This built-in integrity lets veterans, physicians, and hospitals trust the data they see.

For the VA, blockchain's real power comes from smart contracts—self-executing code that runs when preset rules are met. They can automatically verify eligibility, calculate benefits, and release payments, slashing paperwork and wait times. Because the ledger is decentralized across multiple computers, there's no single point of failure; the entire ecosystem of hospitals, clinics, benefits offices, and external partners views the same tamper-evident information in real time, strengthening both resilience and transparency.

Five Ways Blockchain Solves VA Pain Points

Blockchain offers a promising suite of tools to address several enduring challenges encountered by the VA.

- 1) **Blockchain would allow for secure and portable health records:** Veterans often face gaps in their health records across the military, VA, and private providers. Blockchain can ensure that a veteran's medical history is tamper-proof, securely logged, and portable, which will enable faster, safer care across any provider while giving the veteran control over who sees their records.
- 2) Blockchain would speed up and secure benefit delivery: From disability claims to GI bill payments, VA benefits are often delayed by outdated systems and paperwork. Blockchain can automate eligibility checks and streamlines disbursement through smart contracts, resulting in faster, trackable, and more reliable benefits processing for veterans.
- 3) **Strengthen identity verification and reduce fraud**: The VA invests heavily in confirming veteran identity, yet fraud remains a challenge. Blockchain-based digital IDs, linked to verified service and health data, can reduce identity theft and ensure benefits go only to the right person.
- 4) Enhance transparency and audit readiness: Many VA systems lack a reliable audit trail. Blockchain creates a transparent, time-stamped log of every action, like data access or record edits.
- 5) **Increase system resilience and trust:** By decentralizing critical data, blockchain reduces reliance on a single point of failure. It helps modernize infrastructure to ensure continuity across VA hospitals, clinics, benefit offices, and partners, building confidence that veterans' data and benefits are secure and properly managed.

It is crucial to note that blockchain is not a cure-all. Implementing innovation requires careful planning, robust privacy and security controls, and pilot programs to validate scalability within the VA's unique environment. The Digital Chamber and industry partners are ready to assist and share expertise as the VA and Congress explore these applications. The proposed Veterans Affairs Distributed Ledger Innovation Act of 2025 is a prudent first step in identifying high-

value opportunities and addressing any associated risks. Ultimately, blockchain should be seen as a tool in service of the VA's broader mission:" *to care for those who have borne the battle*."

Where Blockchain is Already Making A Difference

By enhancing data integrity, accelerating processes, and enabling trusted collaboration, this technology can help the VA – and broader federal government – deliver benefits with the accuracy, security, and responsiveness that our veterans deserve in the digital age.

From the expedited processing of GI Bill payments and the safeguarding of medical records to the automation of insurance claims and the prevention of fraud, each addresses significant challenges faced by veterans and the VA in contemporary settings.

It is crucial to note that these promises and innovations provided by blockchain are not science fiction hypothetical situations; instead, they are rooted in pilot programs and initiatives that have already been tested either within the federal government or by industry leaders, demonstrating measurable improvements in efficiency, transparency, and trust:

- In **education**, blockchain is empowering students (including veterans) to own and share their learning credentials. These credentials live as tamper-proof digital certificates held by the student, letting schools and employers verify them instantly.
- In **healthcare**, blockchain networks have demonstrated their ability to handle large transaction volumes in drug supply chains. They can help save billions by simplifying provider data management, which directly aligns with the VA's need to modernize electronic health record (EHR) and provider systems.
- In **financial services**, such as home loans and insurance, blockchain solutions are already reducing settlement times from days to seconds, which translates to better, faster outcomes for veterans awaiting a home closing or an insurance payout.
- In **benefits processing and anti-fraud efforts**, the tamper-proof audit trails and crossagency visibility that blockchain offers could help VA sustain the record-breaking output it achieved in 2024¹ while minimizing errors, overpayments, and fraud that undermine public confidence.

Why Security and Privacy Improve – Not Suffer – Under Blockchain

Veterans' medical and personal information is exceedingly sensitive in nature. At the same time, our government is exceedingly vulnerable to cyberattacks, which not only pose risks of privacy breaches but also have the potential to erode trust in the VA's systems. Blockchain technology has the capacity to enhance security in several ways.

1) Its decentralized architecture eliminates the existence of a single hackable database; an assailant would need to simultaneously compromise multiple nodes [or computers], which presents a significantly greater challenge than infiltrating a central server.

¹ *HELIX Protocol: A Blockchain Architecture for Healthcare Finance."* SSRN, papers.ssrn.com/sol3/papers.cfm?abstract_id=5198764.

- 2) Blockchain employs robust cryptographic techniques to link blocks of data; any attempts to modify a historical record would be promptly identifiable to the network, thereby alerting administrators to possible tampering. In simplest terms, each block is digitally "locked" to the one before it, so if anyone tries to change an old entry the chain immediately shows the break and signals that something's wrong.
- 3) Blockchains can utilize contemporary encryption methods such that data is exclusively accessible to individuals possessing the appropriate cryptographic keys. For example, a veteran's identity or health record could be represented by an encrypted token on the ledger, with decryption of the actual data available solely to clinicians or systems authorized by the veteran. It puts ownership of the data back in the hands of the veteran or individual and out of the hands of a centralized entity, like the government. This framework aligns effectively with the zero-trust security principles that are increasingly endorsed within government systems.

Moreover, as every access event can be recorded immutably, blockchain facilitates unparalleled accountability; the identity of individuals accessing specific data is both transparent and auditable in real-time.

Empowering Veterans Through Data Ownership

Blockchain is not simply an efficiency upgrade for the VA; done right, it flips the power dynamic in favor of the veteran. Utilizing blockchain technology would let each veteran carry verifiable proof of service, disability rating, medical credentials, or GI bill status on their phone – each easily proven or verifiable through the underlying infrastructure and programmable smart contracts on top of it. No more mailing papers or waiting weeks for verification letters; the blockchain ledger confirms authenticity instantly while the veteran remains the sole custodian of the underlying data.

For example, blockchain can enable a digital identity or self-sovereign identity (SSI), specifically designed for veterans; this essentially refers to a portable, blockchain-secured digital identity that is entirely controlled by the individual. Veterans would have access to a digital wallet available via smartphone or computer that contains verifiable credentials, which may include proof of military service (e.g., DD-214 data), VA health patient credentials, disability rating, and other essential records.

Through the utilization of blockchain technology, each credential is signed and can be verified without the necessity for the veteran to request official letters or carry physical documentation repeatedly. When a veteran is required to demonstrate their status to access various services, such as consulting with a new healthcare provider, obtaining benefits from an educational institution under the GI Bill, or receiving a veteran discount from a private business, they could share a tamper-proof credential from their digital wallet. The recipient can confirm its authenticity through the blockchain instantaneously and cryptographically, thus eliminating the need for the veteran to navigate VA channels for verification. This approach not only empowers veterans, granting them greater control over their personal data and the ability to dictate who may access their information, but also reduces the administrative burden on VA offices that presently process thousands of verification requests.

Moreover, a blockchain-based identity could facilitate streamlined logins across VA digital services. Rather than managing multiple accounts for VA healthcare, the benefits portal, and other services, a veteran's SSI could function as a singular, secure login, implemented across various systems, similar to LOGIN.GOV but utilizing user-controlled credentials.

Countries such as Canada and the Netherlands are currently experimenting with SSI systems for their citizens to interact with government services², and the U.S. Department of Homeland Security has invested in pilot programs for SSI for veterans³ (for instance, to validate their training credentials with employers). The VA could actively participate in these initiatives, ensuring that veterans retain ownership of their data and agency in the digital landscape while maintaining privacy through blockchain's encryption.

In short, blockchain transforms veterans from passive recipients of benefits into active owners of their digital identity.

From Pilots to Scaled Solutions

The shift in ownership and control in not only empowering, but essential in a time of rising data breaches and privacy risks. Blockchain's potential to strengthen Health Insurance Portability and Accountability Act (HIPAA)⁴ compliance and auditability comes at a critical moment. Significant healthcare data breaches continue to be reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). In 2024, the OCR data breach portal indicates that there were 725 data breaches involving 500 or more records, marking the third consecutive year with more than 700 major incidents. ⁵

The VA itself has experienced breaches involving veterans' data in the past. Adopting blockchain technology could aid in preventing breaches by eliminating central points of failure and by encrypting and dispersing access control, thereby rendering unauthorized access exceedingly challenging. In conclusion, blockchain has the potential to construct a robust framework of integrity around sensitive data, maintaining its privacy and security, and ensuring that it remains solely within the purview of authorized entities.

Modernizing Benefits Delivery and Fraud Prevention

The VA administers a multitude of benefits, which encompass disability compensation, pension payments, caregiver stipends, and insurance programs. These processes necessitate the verification of eligibility, claims processing, and fund disbursement. Regrettably, they also serve

² The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel. World Economic Forum, www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.

³ Silicon Valley Innovation Program – Blockchain & Distributed Ledger Technologies. "U.S. Department of Homeland Security, decentralized-id.com/government/usa/dhs/.

⁴ *Health Insurance Portability and Accountability Act of 1996.* Pub. L. 104-191, 110 Stat. 1936. 21 Aug. 1996. Congress.gov, www.congress.gov/bill/104th-congress/house-bill/3103.

⁵2024 Healthcare Data Breach Report. HIPAA Journal. Retrieved from https://www.hipaajournal.com/2024-healthcare-data-breach-report/

as potential targets for fraud, waste, or abuse if not adequately controlled. The implementation of blockchain technology can significantly enhance transparency and automation, thereby mitigating these risks.

In the context of disability claims, the utilization of smart contracts on a blockchain would enable the automatic cross-verification of service records, medical evidence, and policy regulations upon the submission of all requisite data. This approach could expedite the adjudication process while flagging any anomalies, such as duplicate claims or inconsistent information, for manual review and verification. Crucially, once a claim decision is documented on the ledger, it is time-stamped and tamper-proof, making it ideal for audit purposes or appeals. In terms of fraud prevention, an immutable ledger of transactions facilitates the detection of patterns indicative of suspicious activity.

An example is that if an individual attempts to reroute veteran benefit payments or fabricate a beneficiary record, the inherent transparency of the blockchain would make such malicious alterations obvious and traceable, thereby deterring such actions by design. A legislative report accompanying the Veterans Affairs Distributed Ledger Innovation Act could note that blockchain could facilitate the "streamlining of the insurance claim process" and enhance the integrity of benefits delivery. This is not merely theoretical. The Centers for Medicare & Medicaid Services (CMS) have conducted experiments using blockchain technology in provider credentialing to combat fraudulent billing practices.⁶ Simultaneously, private health insurers, through the Synaptic Health Alliance (founded by Aetna, Humana, MultiPlan, Quest Diagnostics, and UnitedHealth Group), are employing a blockchain ledger to ensure accurate provider directories, consequently reducing false claims regarding in-network providers.⁷ These preliminary initiatives suggest that billions in improper payments could be prevented by transitioning from paper-based, opaque processes to transparent, rules-based digital ledgers.

Securing the Medical Supply Chain

The Veterans Health Administration operates one of the nation's largest pharmacy networks, providing medications and medical devices to millions of veterans. That scale makes it vulnerable to counterfeit products, recalls, and costly inventory delays.

Blockchain-based track-and-trace systems have already proven they can close those gaps. In accordance with the Drug Supply Chain Security Act (DSCSA)⁸, the Food and Drug Administration (FDA) has urged the industry to establish unit-level tracking for prescriptions. During a pilot program conducted by the FDA in 2019–2020, four prominent companies (IBM, KPMG, Merck, Walmart) developed a blockchain system aimed at tracing drug shipments.⁹ The

⁶ Mackey, Tim Ken et al. "Combating Health Care Fraud and Abuse: Conceptualization and Prototyping Study of a Blockchain Antifraud Framework." *Journal of medical Internet research* vol. 22,9 e18623. 10 Sep. 2020, doi:10.2196/18623

⁷ Improving Provider Data Accuracy. Synaptic Health Alliance. Retrieved from

https://f.hubspotusercontent40.net/hubfs/4801399/Synaptic_Health_Alliance_BlockchainWhite_Paper.pdf ⁸ Drug Supply Chain Security Act. Pub. L. 113-54, 127 Stat. 587. 27 Nov. 2013. Congress.gov,

www.congress.gov/bill/113th-congress/house-bill/3204.

⁹ Blockchain Interoperability Pilot Project Report. KPMG. Retrieved from https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/blockchain-interoperability-pilot-project-report.pdf

outcome determined that the blockchain surpassed the FDA's interoperability benchmarks for pharmaceutical tracking, prompting regulators to label it "safety-enhancing answer" for drug traceability.

Should the VA integrate with analogous blockchain networks (or operate its own for internal supply chains), it could secure the authenticity of medications and devices administered to veterans in second. This is particularly critical, given the known issue of counterfeit or substandard drugs within global supply chains. The same ledger could track high-value medical equipment such as prosthetics and implants, giving logistics teams real-time visibility into stock levels, expiration dates, and bottlenecks. In short, a single, tamper-proof record from factory to frontline clinic would cut waste, deter fraud, and ensure veterans receive genuine, safe products exactly when they need them.

Streamlining Provider Credentialing

Another administrative burden in the healthcare sector is verifying the credentials of medical professionals and ensuring that these credentials remain current. The VA, which employs thousands of doctors, nurses, and technicians while collaborating with community providers through the VA Community Care Network, must continuously verify licenses, certifications, training, and hospital privileges. Traditionally, this process involves repeated manual checks and isolated credential databases, which can result in delays in onboarding providers or even service gaps if a provider's credentials lapse without notice. Blockchain technology offers a collaborative solution: a credentialing ledger wherein accreditation bodies, such as state medical boards, nursing boards, and specialty boards, can issue cryptographic attestations regarding a professional's credentials. Each VA facility or partner can promptly consult the ledger to confirm a provider's qualifications and determine whether any sanctions or expirations have occurred, all in real-time.

Improving GI Bill Benefits and Credential Portability

One of the fundamental programs of the VA is educational assistance, commonly referred to as the GI Bill. The administration of GI Bill benefits requires verifying veteran eligibility, tracking enrollments, and processing tuition and housing payments across hundreds of educational institutions and training providers. At times, these processes have encountered challenges due to outdated information technology systems. For instance, upon the enactment of the Forever GI Bill in 2017 (Harry W. Colmery Veterans Educational Assistance Act)¹⁰, the VA discovered that the implementation of its provisions required modifications to twenty-two separate systems, at a projected cost of \$70 million; in the absence of such updates, nearly one thousand additional personnel would have been required to process claims manually.

¹⁰ *Harry W. Colmery Veterans Educational Assistance Act of 2017.* Pub. L. 115-48. 16 Aug. 2017. Congress.gov, www.congress.gov/bill/115th-congress/house-bill/3218.

Additionally, in 2018, technical malfunctions resulted in tens of thousands of veterans facing delays in their GI Bill payments, underscoring the urgent need for more resilient, modern technology.¹¹

Blockchain can help address these issues in two ways: streamlining benefit processing and verifying credentials. A permissioned blockchain ledger could connect the VA, schools, and student veterans, enabling real-time tracking of enrollments and triggering automated stipend payments using smart contracts. Rather than relying on batch processing or manual certification at the end of each semester, educational institutions could upload enrollment confirmations directly to a shared ledger accessible by the VA. Each transaction would be time-stamped, immutable, and auditable, which would improve clarity, reduce disputes, and help veterans receive payments on time.

Additionally, blockchain can transform how veterans prove their educational achievements. Today, verifying credits, certifications, or military training equivalencies often relies on paper records and siloed systems. Using blockchain, schools could issue tamper-proof, digitally signed credentials – such as diplomas or course completions – that veteran's control and can share securely with employers, licensing bodies, or other schools. The Department of Education's Education Blockchain Initiative has already piloted this approach, including a project to convert military training into civilian credit via blockchain wallets. These tools would reduce friction, fraud, and redundancy, helping veterans get credit for what they've already earned and easing their transition to new careers or degrees.

Modernizing the GI Bill with blockchain supports the VA's 21st-century mission – ensuring accurate payments, portable credentials, and veteran-first systems built on transparency and trust.

Recommendations

Like any transformative technology, blockchain is often misunderstood. To maintain a balanced perspective, it is imperative to address the prevalent concerns that policymakers or stakeholders may harbor regarding the implementation of blockchain within federal healthcare systems. To fully harness blockchain for modernizing veteran services, Congress, the VA, and interagency partners can take several steps. Below are our recommendations, aligned with fostering innovation while managing risk:

1. Enact and fund the VA Blockchain Study (Distributed Ledger Innovation Act of 2025)

Congress should enact the legislation proposed by Representative Mace, which mandates a comprehensive study on blockchain technology by the VA. This study, which must be completed within a one-year timeframe for reporting, will provide a clear framework outlining the potential role of blockchain technology in the VA's modernization initiatives for both a five-year and a ten-year timeline. It is essential that the provisions of the bill be supported with adequate funding and expert resources. The VA should form partnerships with academic institutions and federally

¹¹ Horton, Alex. "Veterans Aren't Getting Their GI Bill Payments — Because VA's 50-Year-Old Computer System Broke." *The Washington Post*, 15 Nov. 2018.

funded research and development centers (FFRDCs) that possess expertise in blockchain technology to assist in conducting the feasibility study. The resulting report will serve as a valuable resource for this Committee to oversee subsequent actions. By thoroughly analyzing both the advantages and risks, the study will promote an informed approach to any adoption of the technology, considering potential implications.

Furthermore, we recommend that the study solicit feedback from veterans and VA field offices to ensure that the perspectives of end-users are duly considered.

2. Launch Pilot Programs in High-Impact Areas:

Following the study (or even concurrently, as some groundwork is laid), the VA should initiate a series of pilot programs or proof-of-concept projects. Pilots enable real-world testing on a small scale without risking disruption to the entire system.

We recommend pilots in at least three domains: (a) Health Data Exchange, (b) Supply Chain Management, (c) Claims Automation.

- (a) Health Data Exchange Pilot: Select a region (perhaps a VISN Veterans Integrated Service Network) where several VA Medical Centers and community care providers agree to participate. Implement a blockchain-based referral and medical record exchange system between them. Use synthetic patient data first, then opt-in real patient data with consent. Measure improvements in data retrieval time, reduced duplicative tests, and patient satisfaction.
- (b) Supply Chain Pilot: At one VA pharmacy depot or hospital, integrate a blockchain solution to track one high-value medication or medical device from manufacturer to point of use. Work with industry partners (which could include manufacturers who participated in FDA's DSCSA pilots). Evaluate if the blockchain reduces time to authenticate shipments, improves inventory accuracy, or flags any supply issues proactively.
- *(c) Claims/Benefits Pilot:* Use a controlled environment to process a sample of straightforward benefit claims (e.g., travel reimbursements or education benefit disbursements) through a blockchain-based smart contract system. Compare processing times and error rates against the traditional system. This could also be done for something like verifying veteran-owned small business status for procurement using blockchain credentials to streamline verification in contracting (which is a VA responsibility as well).

Congress has the capacity to facilitate these pilot programs by granting explicit authority and appropriating funds within the VA budget. The establishment of a specific line item designated as "Emerging Tech Pilots – Blockchain," with a modest financial allocation, would enable VA's Office of Information and Technology, along with the Innovation Center, to implement these initiatives in collaboration with external partners.

Furthermore, instituting a requirement for reporting on the outcomes of the pilot programs back to Congress would promote transparency and accountability.

3. Support for Interagency Collaboration and Standards Development

The VA should not operate in isolation. Healthcare data interoperability, cybersecurity, and digital identity represent cross-cutting issues. We recommend that Congress encourage the VA to collaborate with agencies such as the Office of the National Coordinator for Health Information Technology (ONC) to establish interoperability standards that incorporate blockchain technology, as well as with the National Institute of Standards and Technology (NIST) to develop federal guidelines on blockchain security and best practices (NIST has already published preliminary guidance on blockchain for identity management¹²; this could be expanded).

The Department of Defense (DoD) is another key partner; the DoD's health system (MHS Genesis) and the VA are expected to seamlessly share records as service members transition to veteran status. A joint VA-DoD blockchain pilot project could specifically target the transition of health records and credentials from active duty to VA care, ensuring that no information is lost when a service member transitions to VA care. The Department of Health and Human Services (HHS) could be involved in broader health data exchange frameworks. International standards bodies, such as the Institute of Electrical and Electronics Engineers (IEEE)¹³ and the International Organization for Standardization (ISO)¹⁴, have blockchain working groups in which input from U.S. federal agencies would also be valuable. Congress may consider directing the VA to provide an update regarding its engagement in such collaborative efforts.

4. Address Regulatory and Legal Clarity

If any legal barriers to the utilization of blockchain technology are present, it is imperative to identify and eliminate them. For example, existing regulations concerning VA records management may presume the use of centralized databases; therefore, Congress could take preemptive action to update laws, explicitly permitting the use of distributed ledger technology to satisfy record-keeping obligations.

Furthermore, it is essential to ensure that records generated through smart contracts are acknowledged as valid and enforceable, possibly referencing the work related to the Electronic Signatures in Global and National Commerce Act (E-SIGN) and various state-level modifications pertaining to blockchain. Adjustments may also be necessary regarding privacy laws to facilitate the type of controlled data sharing made possible by blockchain technology; for instance, it should be clarified that consent obtained from a veteran through a blockchain smart contract constitutes a valid HIPAA authorization. While these are complex areas, proactive legal measures can help circumvent bureaucratic obstacles in the future. The Digital Chamber is prepared to collaborate with lawmakers in identifying such requirements.

¹² Blockchain Identity Management Approaches. NIST Cybersecurity White Paper (Draft), National Institute of Standards and Technology, 9 July 2019.

¹³ *IEEE Blockchain Technical Community*. IEEE Standards Association. Includes standards such as IEEE 2140.1–2020, 2140.2–2021, 2140.4–2023, 2140.5–2020. *IEEE Blockchain Technical Community*, blockchain.ieee.org/standards.

¹⁴ *ISO/TC 307 – Blockchain and Distributed Ledger Technologies*. International Organization for Standardization. iso.org/committee/6266604.html.

5. Promotion of Education and Training

It is imperative that both VA personnel and veterans receive education regarding this new technology to facilitate its smooth adoption. We strongly recommend that Congress provide support for training programs, potentially as a component of the pilot funding, aimed at training VA IT staff and clinicians on the foundational aspects of blockchain utilization within their workflow. For veterans, the VA should disseminate clear communications, utilizing existing outreach channels, to explain any new blockchain-based tools. If a veteran is to use a digital wallet for their health records, it is essential that they understand the safe usage of such technology. Engaging with organizations such as Operation Bitcoin or Veterans in Blockchain groups can help create educational materials that are accessible and beneficial to veterans.

Furthermore, establishing scholarships or grants for veterans to pursue education in blockchain development or cybersecurity should be considered, as these skills can be employed within the VA or other governmental agencies, thereby cultivating a pipeline of talent that possesses a profound understanding of the veteran experience.

6. Oversight and Metrics

As blockchain initiatives advance, it is essential to define success metrics and meticulously monitor them. We recommend that the VA, in its reports to Congress, includes quantifiable outcomes such as the reduction in data exchange time, the number of fraud incidents before and after the implementation of blockchain technology, the percentage decrease in supply chain discrepancies, and the improvement in patient satisfaction scores. This data-driven approach will assist in making a compelling case for, or transparently outlining the limitations of, further investment. Additionally, it will identify areas that require adjustment. Congress may wish to consider mandating an annual "Emerging Technology in VA" hearing or report, wherein blockchain projects are included, to sustain momentum and ensure proper oversight.

Our policy recommendations focus on facilitating innovation, bolstered by prudent supervision. By establishing a foundation through comprehensive research, initiating targeted pilot programs, nurturing partnerships, and revising regulations, Congress can help the VA advance technologically while mitigating risks. The ultimate objective remains consistently in view: to provide enhanced, expedited, and safer services to our veterans.

Conclusion

In conclusion, Chairwoman, I would like to express my gratitude to you and the Subcommittee for your exemplary leadership in examining emerging technologies related to veteran services and opportunities to reduce government waste. The VA has been a leader in innovation as mentioned at the outset, and blockchain technology represents the next frontier in this journey of innovation.

With prudent adoption, it has the potential to strengthen the sacred trust that exists between veterans and their government by ensuring that every benefit earned is a benefit delivered efficiently, transparently, and faithfully.

I am appreciative of the opportunity to provide testimony today on this significant matter. I am prepared to respond to any inquiries and to continue collaborating with you and the Subcommittee in the effort to improve the systems that support our veterans.