

BUILD *the Future*

Maintaining Data Integrity Across Platforms





The Challenge

Governments worldwide rely on accurate, secure data to execute daily functions. However, this information must also be shared within and across government agencies or departments, including one-to-one, one-to-many, and with the general public.

Achieving this degree of interoperability is particularly challenging for government entities that must share information while adhering to strict security requirements and agency protocols. While these safeguards protect mission-critical data from malicious actors, they can also prevent valuable integrations that support efficient decision-making.

In short, governments need solutions that prevent attacks on private messaging channels and eliminate the distribution of false information (i.e., fake news reports, deep fakes, falsified official documents). These safeguards are critical as only 57% global consumers indicated they could *detect a deepfake video* in 2022, while the remaining 43% could not. More concerning, forecasts suggest over *500,000 voice and video deepfakes* will circulate on global social platforms in 2023.

Since receiving its first Defense Advanced Research Projects Agency (DARPA) grant for secure messaging, SIMBA has continued to build blockchain solutions for multiple government agencies and departments.



43%
of consumers
could not detect
a deepfake video



500,000
deepfakes will
circulate in 2023

Case Studies



Secure Messaging

Militaries must communicate securely to mitigate the risk of data interception by domestic and foreign threats. In supporting this requirement, the Department of Defense (DoD) has established strict guidelines for ensuring secure communications and is constantly innovating to remain ahead of new threats.

DARPA has a long and productive history in seeding research initiatives that result in critical technological advancements, including the internet, GPS, graphical user interfaces, the computer mouse, and voice assistants like Siri. With a focus on emerging technologies, DARPA wanted to explore a blockchain solution capable of securely moving classified information for government and military purposes—that's how SIMBA Chain was born in 2016.

In collaboration with ITAMCO and the Center for Research Computing at the University of Notre Dame, SIMBA was awarded the DARPA grant to create a secure, unhackable messaging and transaction platform using blockchain.



Defence Assurance Platform

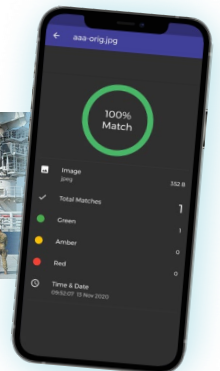
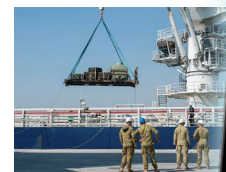
The Australian Defence Force (ADF) produces a range of public media products each week, including press releases, images of operations, and videos showcasing its activities. However, once this data is available online, it's susceptible to alterations and falsifications.

As a result, the ADF must ensure that documents and media released online are authenticated, accurate and genuine. This functionality is critical given the ADF shares content across multiple online-facing platforms. Without adequate oversight, AI-generated deep-fakes and other falsified press can undermine credibility and destabilize civilian life.

The goal of the Defence Assurance Platform is to allow content recipients to authenticate official public media releases, including images, videos, and press releases, verifying that each is legitimate ADF-released media. Two main processes are supported to facilitate this:

- **Registration Process:** The publically released media is stored by the platform and secured using the blockchain, ensuring it's tamper-proof.
- **Verification Process:** Arbitrary media is compared against officially released media previously registered.

Ensuring the authenticity of released media supports transparency and accountability while protecting the ADF's reputation as a trusted defense organization



Data Provenance and AI

As AI becomes more sophisticated, authenticating deep fakes and other falsified media will be critical to government activities. According to *US Homeland Security*, deep fakes and the misuse of synthetic content pose a clear, present, and evolving threat to the public across national security, law enforcement, financial, and societal domains.

Training AI Models

Today, the applications of AI are endless. For example, law enforcement can leverage AI for facial recognition, judges for sentencing, and data analytics providers for traffic management, population health, and more. However, how entities train their AI models is critical to the quality of their outputs. For this reason, machine learning models must utilize accurate data to avoid financial, social, and judicial oversights that negatively impact government experiences.

As an immutable ledger, blockchain is a robust way to establish this data provenance, ensuring the information used to train AI models is reliable and trustworthy. Without this data provenance, verifying the completeness and inputs used to train AI models can be difficult.

AI Application in Government

★★★★☆
RELEVANCE

★★☆☆☆
READINESS

According to *Deloitte*, AI's application in government has a 4/5 rating for relevance but only 2/5 for readiness.





Did You Know?

In 2022, the General Services Administration (GSA) awarded SIMBA Chain a Multiple Award Schedule (MAS) contract. This long-term, government-wide contract permits SIMBA to supply its blockchain solutions and services to all Federal US agencies for up to 20 years. This designation means that local and state governments across the US can leverage the power of SIMBA Blocks to build automotive titling solutions.



Why Blockchain?

With blockchain, governments can establish data provenance for AI solutions in multiple ways:

-  **Transparency** Blockchain networks are transparent, making it easy to audit data and ensure it's used reliably.
-  **Traceability** With blockchain, data changes or modifications can be tracked and recorded, providing a complete timeline of events.
-  **Immutability** Blockchain generates a permanent ledger, meaning governments can audit the data used to train AI models, ensuring accuracy and completeness.
-  **Speed** Blockchain-based smart contracts can enforce data provenance requirements, ensuring AI training models meet specific quality and accuracy standards.

Related Projects



Estonia

The country of Estonia has implemented a blockchain-based system called “X-Road,” which securely links various government databases and ensures the integrity and authenticity of data.

[Read More](#)

Sweden

Countries like Sweden are experimenting with blockchain-based land registry systems. These solutions aim to enhance the security and transparency of land records, reducing fraud and disputes.

[Learn More](#)

United Arab Emirates

Dubai has launched the “Dubai Blockchain Strategy,” which aims to make Dubai a blockchain-powered government. The initiative aligns with Smart Dubai’s mandate to become a global leader in the smart economy.

[See More](#)

About SIMBA

Incubated at the University of Notre Dame in 2017, SIMBA Chain (short for Simple Blockchain Applications) provides a scalable enterprise platform that simplifies blockchain development. With fewer barriers to entry, companies can build secure, scalable, enterprise-grade solutions that integrate seamlessly with existing data systems. SIMBA implementations generate value for major government organizations, enterprises, and blockchain companies as a production-grade platform that enables public, private, or hybrid deployments.

[Contact Us](#)

FAQ

Question:	Is blockchain safe?
Answer:	Yes, blockchain is generally considered safe due to its immutability, cryptographic security, and decentralized nature. However, it's important to implement additional security measures and follow best practices to mitigate potential vulnerabilities and risks.
Question:	I need privacy; will everyone on the blockchain see all my information?
Answer:	No, not everyone will see your information. Blockchain technology allows for different levels of privacy depending on the implementation. Private or permissioned blockchains can restrict access to information, ensuring that only authorized participants have visibility to specific data while benefiting from blockchain technology's security and transparency.
Question:	What lift is required to adopt such a system?
Answer:	A blockchain solution can enhance data integrity, immutability, and transparency. The level of lift required to implement a blockchain solution depends on various factors, including your organization's specific requirements, the complexity of the data being managed, and the scale of the implementation.
Question:	What are the upfront and ongoing costs?
Answer:	The upfront costs of implementing a blockchain solution typically include initial development, integration, and infrastructure expenses, which can vary depending on the complexity and scale of the project. Ongoing costs primarily involve maintenance, upgrades, and operational expenses, including network fees, governance costs, and security measures to ensure the continued functionality and security of the blockchain solution.
Question:	Is anyone else doing this?
Answer:	Several global governments have shown interest in exploring and implementing blockchain solutions for data integrity. Blockchain technology offers transparency, immutability, and decentralization, making it an attractive option for governments seeking to enhance the security and trustworthiness of their data.
Question:	What do I need to get started?
Answer:	You'll require a well-defined project scope, access to relevant data and documentation, and the necessary technological infrastructure to support blockchain implementation—that's where <i>SIMBA can help</i> .

