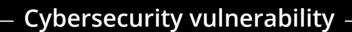# Deloitte's blockchain authentication security evidence platform

This platform provides authentication, authorization, and identity access management solutions to assist clients in managing cybersecurity risks.

Cybersecurity vulnerability

Non-consensual authentication

Single-entity point of failure

Logging integrity vulnerabilities

Reactive-Only logging

Blockchain's value/capability

Multi-signature/Threshold authentication
- Reduces bad actors' ability to exploit a single set of credentials
- Stronger than multi-factor authentication (MFA)
- Requires consesus among a minimum threshold of signatories
- Reduces Eliminates bad actors' ability to exploit a single set of credientials

Blockchain Distributed Identification (DID) Architecture
- Removes single-entity point of failure through the practice of distributing the various components of identity management

Immutable historical blockchain logging of ALL relevant events
- Provides full audit trail
- Everlasting, tamper-evident, timestamped registry of events

Immutable Proactive Blockchain logging
- "Announces" tamper-evident events
- Enables automated triggering of communications or actions based on a predetermined ruleset

Potential impact on your cybersecurity posture

Reduced breach impact
- By implementing threshold authentication, the effect of a breach can be minimized as malicious actors must compromise multiple users, applications, devices, or systems to achieve the threshold, thereby reducing the overall "blast radius" of a breach.

Enhanced access control
- Active directory no longer stores usernames and passwords, making it harder for a hacker to gain full credential access.

Secure privileges
- Information on user privileges is stored separately, limiting a hacker's ability to manipulate access controls even if they gain unauthorized access.

Distributed consensus mechanism
- Any changes to smart contracts (including unauthorized privilege modifications) need to be validated across multiple nodes. Single-actor changes are automatically rejected, maintaining the integrity of the system.