Deloitte.

Blockchain & Digital Assets

BASE

Why is Blockchain Authentication & Secure Evidence (BASE) critical?

BASE provides novel, "zero trust" solutions to critical challenges, helping to improving cybersecurity posture.

Why Deloitte and BASE to help improve your cybersecurity posture?

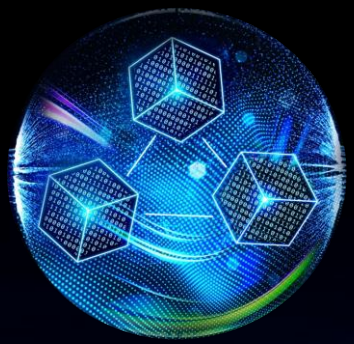
A stronger cybersecurity posture enabled by passwordless blockchain-based distributed identity (DID) subnet architecture can assist in efforts to mitigate internal and external cybersecurity risks, reduce the cost of attack remediation, and protect your company's brand and reputation. Deloitte has been serving the blockchain and digital asset ecosystem for over a decade and is a recognized leader in serving corporates, digital asset, blockchain, fintech, and payment companies.

12+ years
of experience navigating through dynamic digitall asset regulatory landscape

Trusted advisor
to the blockchain and digital asset ecosystem

Subject matter specialists
across the various risk domains

Experienced
serving clients from startups to global enterprise boardrooms



Distributed
Disperses control of authentication and authorization systems and data across multiple entities

Immutable
Ability of blockchain ledger to remain an indelible, unalterable history of events

Passwordless
Zero trust cryptographically-secured authentication

Adaptive
Leverages smart contracts to manage permissions checks, mitigating phishing and attacks

Performable
Able to function in accordance with cybersecurity requirements

Cost Effective
Can increase cost savings from attack mitigation by lessening the impact of a breach

Flexible
Easily modified to accommodate new or updated business requirements

COMPLEMENTARY

BASE's underlying technology is a suite of complementary "zero-trust" modules that enhance traditional enterprise security tools.

TRUSTWORTHY

- Performance tested
- Security tested

Our approach to identity access management (IAM)

Deloitte's BASE platform facilitates passwordless IAM in a streamlined, modular fashion.

Cryptoghraphic permissioning
Help enhance ability of smart contracts, in conjunction with privilege database, to determine user/system permissions, thereby enabling distributed passwordless authentication and authorization

Data health fingerprinting
Help enhance "trustworthiness" of event logging (e.g., stack function executions and DevOps pipeline commits) by hashing system logs to relevant public and/or permissioned blockchains

Public private key rotation
Help strengthen systems security via continual automated smart contract re-publishing in support of public/private key rotation

Authentication and identity provider integration
Help assist with integration of identity providers (IdPs) and IAM providers to facilitate simplified injection into existing authentication workflows

Deloitte.

Deloitte's Blockchain Authentication Security Evidence tool - BASE

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

Common cybersecurity threats BASE addresses can assist with

- Denial-of-service attack
- Phishing
- Malicious Rootkits
- Man-in-the middle attack
- Insider threat
- Social Engineering

Blockchain's Unique value

Multi-signature/threshold authentication
- Reduces bad actors' ability to exploit a single set of credentials
- Stronger than multi-factor authentication

Blockchain Distributed Identification (DID) Architecture
- Eliminates single-entity point of failure by distributing IAM components

Immutable reactive blockchain logging of all relevant events
- Provides full audit trail of tamper-evident, timestamped registry of events

Immutable proactive blockchain logging
- Enables automated triggering of communications or actions based on a predetermined ruleset

Potential impact on cybersecurity posture

Reduced breach impact: "Blast radius" of breach minimized, as malicious actors must compromise multiple users or systems to achieve the threshold, thereby reducing the overall breach impact.

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: Smart contract changes require multi-node validation. Unauthorized changes are automatically rejected, maintaining system integrity.

Let's Talk.

Tim Davis
Principal
Deloitte & Touche LLP
timdavis@deloitte.com

Kyle Burgess
Advisory Specialist Leader
Deloitte & Touche LLP
kyburgess@deloitte.com

Peder Muller
Solutions Architect
Deloitte & Touche LLP
pemuller@deloitte.com

Sean Peasley
Principal, Cyber and Strategic Risk
Deloitte & Touche LLP
speasley@deloitte.com