ENABLER OR HINDRANCE

# CYBERSECURITY'S FUTURE WITH BLOCKCHAIN?

@SONYAMOISSET 🦄🌍

.SR FULLSTACK SOFTWARE ENGINEER
.APPLICATION SECURITY ENGINEER
.ANDROID DEVELOPER
.TECH ADVOCATE

.CYBER ATTACKS ARE COMPLEX AND TARGETED
.CYBER CRIMINALS ARE STEALING VALUABLE DATA
.HIGHLY PROFITABLE STRATEGIES TO MONETISE DATA ACCESS

.POTENTIAL TO DISRUPT MULTIPLE INDUSTRIES
.BILLIONS INVESTED BY FINANCIAL SERVICES AND TECH FIRMS GLOBALLY
.INVESTMENTS ARE PREDICTED TO INCREASE EXPONENTIALLY OVER THE NEXT 5 YEARS

> “Blockchain can help cyber defence by providing a secure platform, by preventing fraudulent activities, and by detecting data tampering”

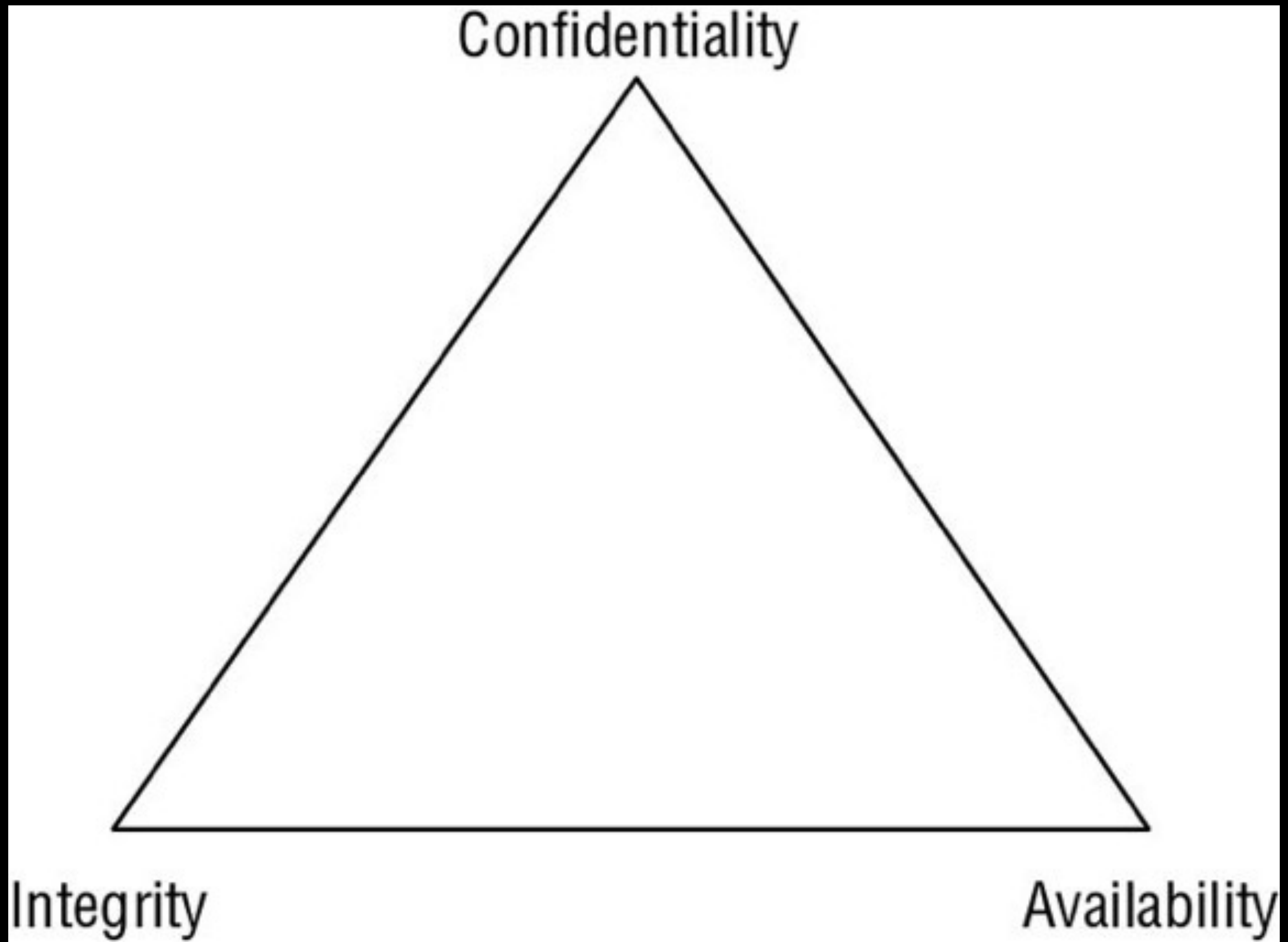
–IS IT THE PERFECT SOLUTION?

# KEY CONSIDERATIONS

- Number & types of participants in the network
- Untrusted or unauthorised persons who participate in the network
- Design and robustness of the consensus validation rules and processes
- Strength of the encryption protocols
- Extent of reliance on externally-sourced data
- Sensitivity of the records or transactions recorded in the electronic ledger
- Ability to correct fraudulent, malicious or erroneous records

CYBERSECURITY IS MEANT TO PROTECT YOUR ONLINE INTELLECTUAL PROPERTY FROM ANY FORM OF CYBER ATTACKS, DAMAGE, OR UNAUTHORISED ACCESS

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY ARE VIEWED AS THE PRIMARY GOALS AND OBJECTIVES OF A SECURITY INFRASTRUCTURE



# CONFIDENTIALITY

ONLY AUTHORISED PARTIES ACCESS THE CORRECT AND APPROPRIATE DATA TO THEM

# CONFIDENTIALITY

- Network Access
  - Private blockchains require appropriate security controls in place to protect network access
  - Security best practices recommend security controls
  - Organisations must determine what level and type of cyber risks are acceptable

# CONFIDENTIALITY

- Data Access
  - E2E encryption where only those authorised to access the encrypted data through their private key can decrypt and see the data
  - Implement secure communication protocols
  - Accessing blockchain account from multiple devices creates a higher risk of losing control of private keys
  - Today's cryptographic algorithms used for public/private key generation rely on integer factorisation problems which are hard to break with current computing power

# INTEGRITY

MAINTAIN DATA CONSISTENCY AND GUARANTEE INTEGRITY DURING ITS ENTIRE LIFE CYCLE

# INTEGRITY

- Immutability & Data Quality
  - Challenging to tamper with it
  - Consensus mechanisms improve the overall robustness and integrity of shared ledgers
  - Blockchain technology does not guarantee or improve data quality

# INTEGRITY

- Traceability & transparency
  - Every transaction added to a public or private blockchain is digitally signed and timestamped
  - Non-repudiation
  - Audit capability provides a level of transparency over every interaction
  - Compliance & regulations

# AVAILABILITY

AUTHORISE SUBJECTS ARE GRANTED TIMELY AND UNINTERRUPTED ACCESS TO OBJECTS

# AVAILABILITY

- No Single Point of Failure
  - The distributed nature of the technology solves the Byzantine general’s problem of false consensus
  - Organisations can still face risks from external events outside of their control
  - Private blockchain network with a lower number of nodes

# AVAILABILITY

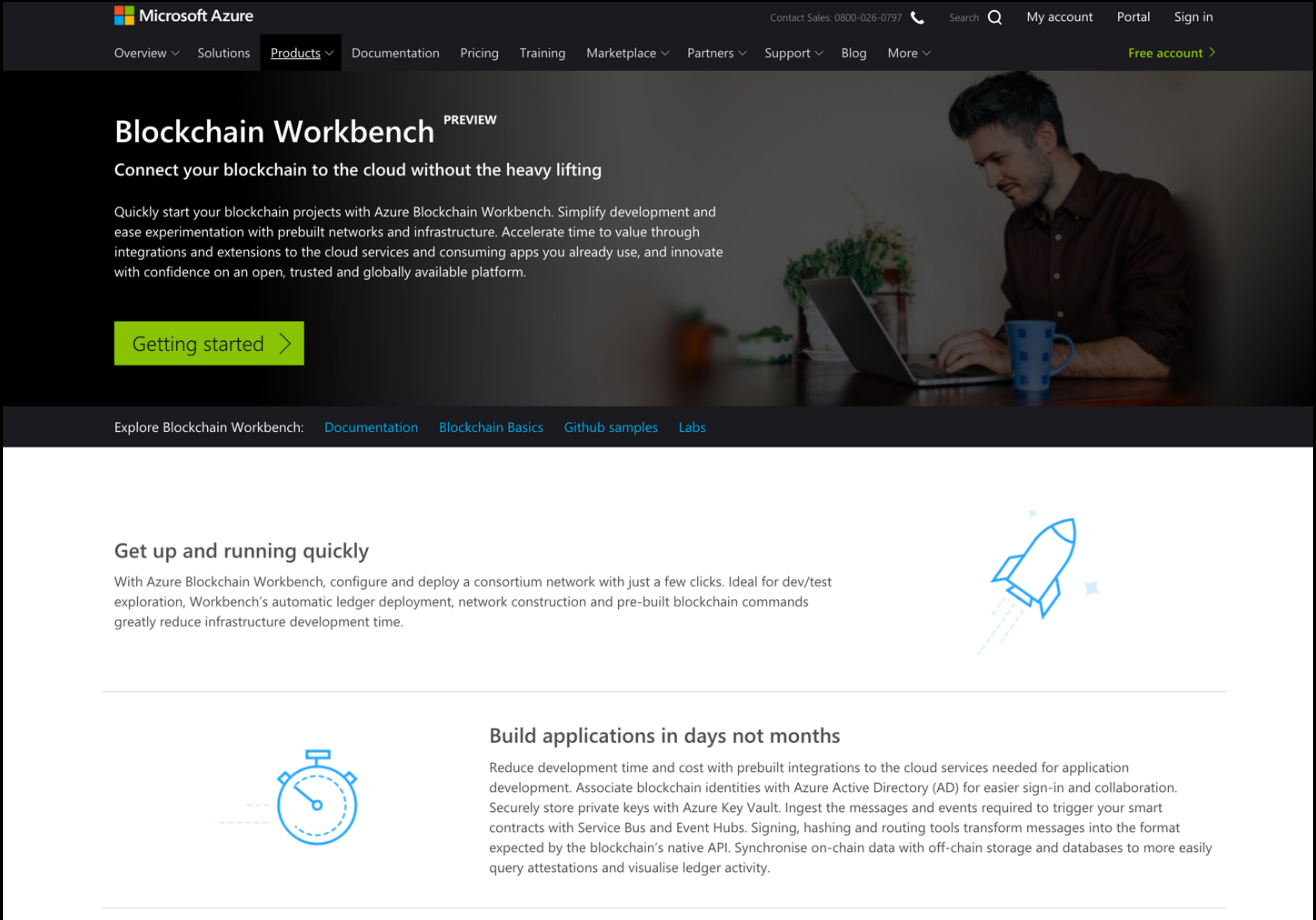
- Operational resilience
  - Blockchains consist of multiple nodes, organisations can make a nodes under attack redundant and continue to operate as BAU
  - Even if a major part of the blockchain network is under attack, it will continue to operate due to the distributed nature of the technology

.BLOCKCHAINS REMAIN SUBJECT TO CYBERSECURITY RISKS

.MANY OF THESE RISKS INVOLVE A HUMAN ELEMENT

.A ROBUST CYBERSECURITY PROGRAM REMAINS VITAL TO PROTECT THE NETWORK & ORGANISATIONS

# WHAT ABOUT CLOUD SOLUTIONS?



# Blockchain Workbench PREVIEW

## Connect your blockchain to the cloud without the heavy lifting

Quickly start your blockchain projects with Azure Blockchain Workbench. Simplify development and ease experimentation with prebuilt networks and infrastructure. Accelerate time to value through integrations and extensions to the cloud services and consuming apps you already use, and innovate with confidence on an open, trusted and globally available platform.

## Get up and running quickly

With Azure Blockchain Workbench, configure and deploy a consortium network with just a few clicks. Ideal for dev/test exploration, Workbench's automatic ledger deployment, network construction and pre-built blockchain commands greatly reduce infrastructure development time.

## Build applications in days not months

Reduce development time and cost with prebuilt integrations to the cloud services needed for application development. Associate blockchain identities with Azure Active Directory (AD) for easier sign-in and collaboration. Securely store private keys with Azure Key Vault. Ingest the messages and events required to trigger your smart contracts with Service Bus and Event Hubs. Signing, hashing and routing tools transform messages into the format expected by the blockchain's native API. Synchronise on-chain data with off-chain storage and databases to more easily query attestations and visualise ledger activity.

Products
Solutions
Pricing
Learn
Partner Network
AWS Marketplace
Explore More
Contact Sales
Support
English
My Account
Sign Up
Blockchain
Overview
AWS Blockchain Templates
Partners

# Blockchain on AWS

Shared ledgers for trusted transactions among multiple parties

Blockchain is a technology that makes it possible to build applications where multiple parties can record transactions without the need for a trusted, central authority to ensure that transactions are verified and secure.

Blockchain enables this by establishing a peer-to-peer network where each participant in the network has access to a shared ledger where the transactions are recorded. These transactions are by design, immutable and independently verifiable.

AWS gives you access to flexible and cost-effective resources to quickly deploy and experiment with blockchain networks in minutes, and pay only for what you use.

## Blockchain capabilities

### DISTRIBUTED TRUST

Multiple parties can transact with one another without having to know or trust each other.

### INDEPENDENTLY VERIFIABLE

All transactions are attributable to one or more entities and each entity can independently verify these records.

### IMMUTABLE

Transactions cannot be removed or altered.

### SECURE

Blockchain networks can be restricted to known parties, and can also limit what transactions each party can see.

### HIGHLY AVAILABLE

Blockchain networks are decentralized and do not have a single point of failure.

- Risk. Key Management
  - Private keys by design are not recoverable
  - Cloud solutions provide key management services
  - Majority of cyber attacks have not attacked the blockchains themselves but have targeted providers of key management services in attempts to steal private keys

- Risk. Vendor Risks
  - The market for 3rd party solutions is growing
  - Create potential for surface exposure through vendor risks
  - Experience and reputation will be key factors

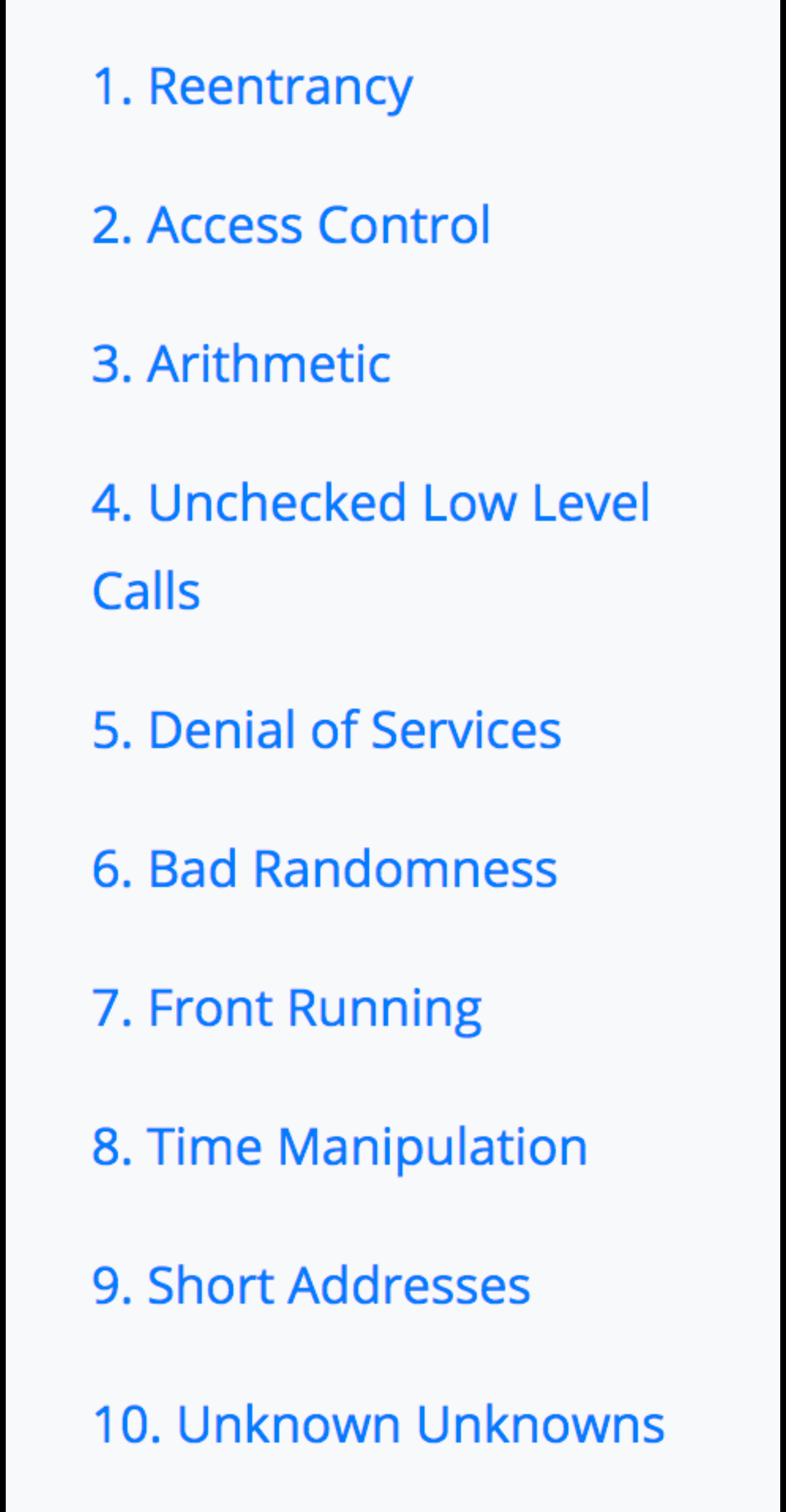
- Risk. Identity-based attacks
  - Take over a majority of the nodes in a network and undermine the consensus validation and distributed architecture protections of a network
  - Cloud-based services deploy their own cybersecurity protections and provide an additional layer of protection for the network

# WHAT ABOUT THE DEVELOPERS?

- Risk. Software coding errors/protocol vulnerabilities
  - As with any computer IT system, human coding errors can introduce cybersecurity risks into blockchains
  - No software is 100% free from defects

.DECENTRALISED APPLICATION SECURITY PROJECT | DASP TOP 10

.THIS PROJECT IS AN INITIATIVE OF NCC GROUP



1. Reentrancy
2. Access Control
3. Arithmetic
4. Unchecked Low Level Calls
5. Denial of Services
6. Bad Randomness
7. Front Running
8. Time Manipulation
9. Short Addresses
10. Unknown Unknowns

.OWASP TOP 10-2017

OWASP

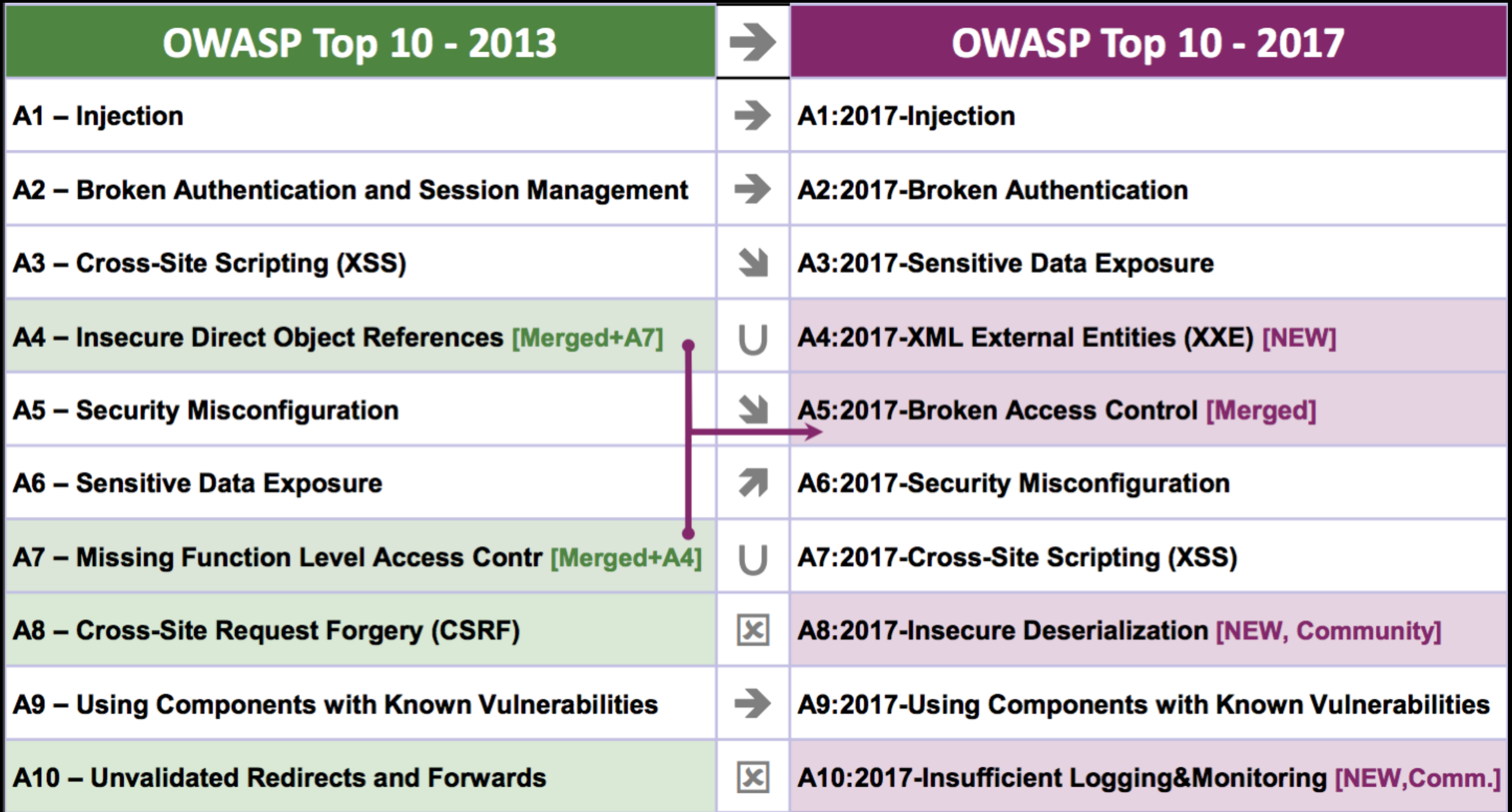
# OWASP Top 10 - 2017

## The Ten Most Critical Web Application Security Risks

https://owasp.org

WHAT HAS CHANGED FROM 2013 TO 2017?

# OWASP TOP 10



| OWASP Top 10 - 2013 | → | OWASP Top 10 - 2017 |
|---|---|---|
| A1 – Injection | → | A1:2017-Injection |
| A2 – Broken Authentication and Session Management | → | A2:2017-Broken Authentication |
| A3 – Cross-Site Scripting (XSS) | ↘ | A3:2017-Sensitive Data Exposure |
| A4 – Insecure Direct Object References [Merged+A7] | ∪ | A4:2017-XML External Entities (XXE) [NEW] |
| A5 – Security Misconfiguration | ↘ | A5:2017-Broken Access Control [Merged] |
| A6 – Sensitive Data Exposure | ↗ | A6:2017-Security Misconfiguration |
| A7 – Missing Function Level Access Contr [Merged+A4] | ∪ | A7:2017-Cross-Site Scripting (XSS) |
| A8 – Cross-Site Request Forgery (CSRF) | ☒ | A8:2017-Insecure Deserialization [NEW, Community] |
| A9 – Using Components with Known Vulnerabilities | → | A9:2017-Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards | ☒ | A10:2017-Insufficient Logging&Monitoring [NEW,Comm.] |

- Risk. Evolving attack vectors
  - Expect new strategies and threats to emerge to exploit unforeseen vulnerabilities in blockchains
  - Quantum computing-based attacks

# GET SECURE, BE SECURE AND STAY SECURE