DC^3 Conference

From cryptocurrencies to CBDCs

25 – 27 January 2022

https://itu.int/go/dc3c

An event of the Digital Currency Global Initiative

Organized jointly:

FDCI | Future of Digital Currency Initiative

ITU

What is the purpose of a Security Audit/Assessment?

A SECURITY ASSESSMENT HELPS PROVE…

CONFIDENTIALITY

INTEGRITY

AVAILABILITY

…SAFETY… LEGALITY ?

A SECURITY ASSESSMENT HELPS SHOW…

THAT IN A WORLD WHERE EVERYTHING IS BECOMING DIGITAL….

YOU HAVE DELIVERED FEATURES THAT ARE **SAFE** TO USE…

ALLOWING USERS TO **TRUST** EVERY ELECTRONIC TRANSACTION

A SECURITY ASSESSMENT CHECKS THAT YOU HAVE..

TRUSTED MATH within
TRUSTED CODE which builds
TRUSTED SITES for
TRUSTED TRANSACTIONS used for
CONDUCTING COMMERCE by
UNTRUSTED HUMANS on the
PUBLIC INTERNET

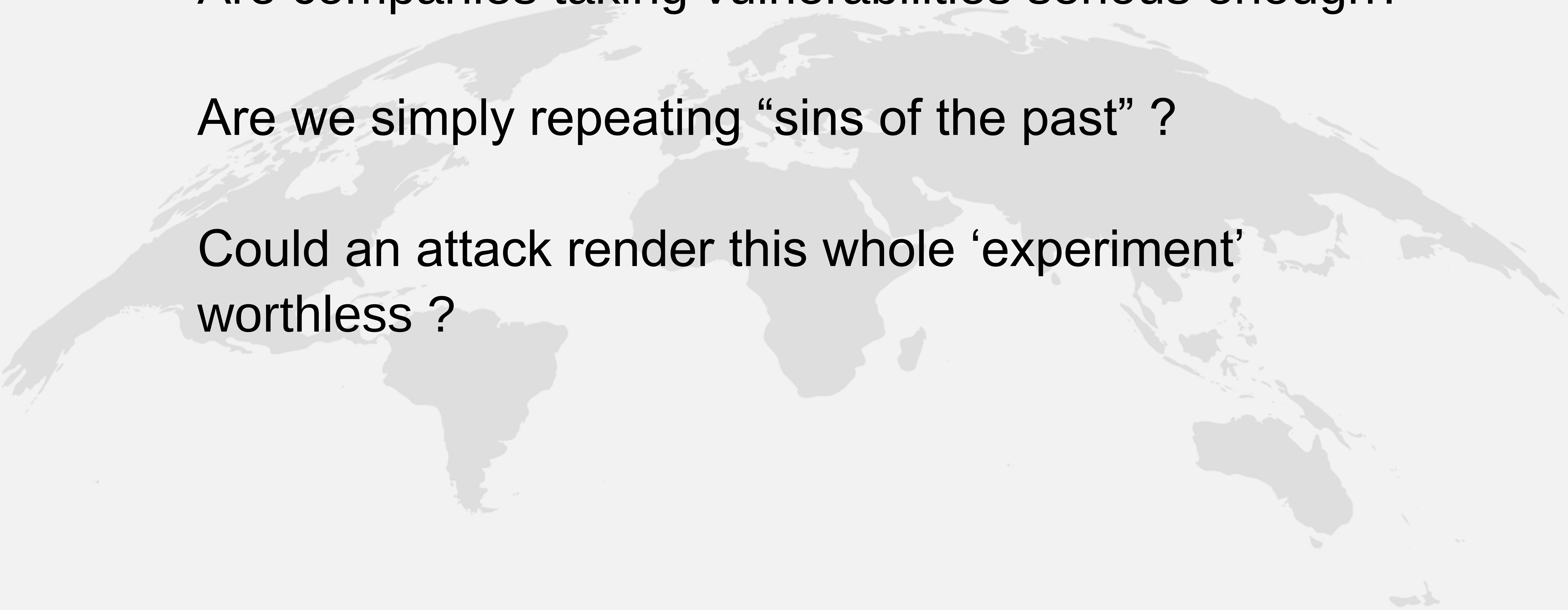
COMMON FLAWS…

- Using outdated software libraries
- Trusting unsafe external dependencies
- Basic mathematical errors in calculations
- Secrets Management (Key handling, Password exposures)
- Cryptograph collisions / miscalculations
- Lack of error handling, signature verification

Many crypto companies are using inexperienced coders who are ‘crypto native’ who might have forgotten lessons of the past

Following on from the two speakers earlier, how many audits have you done where the companies have specifically asked for advisory on privacy preserving blockchain technology, and quantum cryptography risks to their business?

Do you see this change as we head towards 2025?



Are companies taking vulnerabilities serious enough?

Are we simply repeating “sins of the past” ?

Could an attack render this whole ‘experiment’ worthless ?

COMMON SCENARIOS – USED TO EXPLOIT A NATION

CREDENTIAL THEFT – INSIDERS

- CONFIGURATION CHANGE, BACK-OFFICE THEFT
- KEY COMPROMISE, WALLET TAKE-OVER

CREDENTIAL THEFT – CONSUMERS

- DRAIN CONSUMER WALLET, SOW DISTRUST

SPENDING MONEY THAT DOES NOT EXIST

- DOUBLE SPENDING, COLLUSION, MALICIOUS NODES

Question: If a nation state had a bunch of digital currency stolen, couldn’t it simply “delete it” and re-issue replacement?

What can be done to prepare for a safe future using these technologies?

Adopt a cyber security strategy like NIST
Bring in multiple experts
Design, Assess, Remediate, Operate
Learn from Others
Preventative Controls vs Detective Controls

Design a system that can aim to react in “zero – 0” seconds because sometimes that’s all the time you have

Blockchain & Digital Asset Security – Strategic Topics

Advisory

Products and services to design, manage, measure and maintain robust blockchain/ledger enabled architectures.

- Strategy & Governance
- Threat, Vulnerability & Risk Management
- Incident Response and Cyber Resilience
- Strategic Cyber Staffing
- Table-top Exercises
- Full-stack Architecture

Audit / Testing

Audit and Testing of created code or products integrated within your existing CDBC / Blockchain solution

- Technology Audit and Support
- Code, Smart Contract Review
- Architecture Design & Assessment
- Cryptography Assessment
- Automation & Orchestration
- White paper analysis & review
- Logic validation

Architecture & Development

Full-stack review of architecture, design, documentation, code creation, operations monitoring

- Code Development
- Architecture review
- Third party integration services
- Table-top exercises
- High-availability design
- Scrum management, product delivery
- System Event monitoring
- Transaction handling

Research & Innovation

CDBC innovation as well as the development engine for proprietary products or government needs.

- Research
- Custom Development
- Monetary Policy
- Digital Sandbox Solutions
- Fraud Detection
- Malicious User Detection