FNS (M) SDN.BHD.
Feasible Network System

Next Generation Passwordless Blockchain Secure Authentication

20 February 2023

ITU-T Workshop on
"DLT Identity Management"

Radhilufti Madehi | Director Marketing
FNS (M) Sdn Bhd

Secure . Fast . Convenient

Table of Contents

1. Issues of the Digital World
2. Why Blockchain Secure Authentication
3. Blockchain Technology in Authentication
4. What’s Next

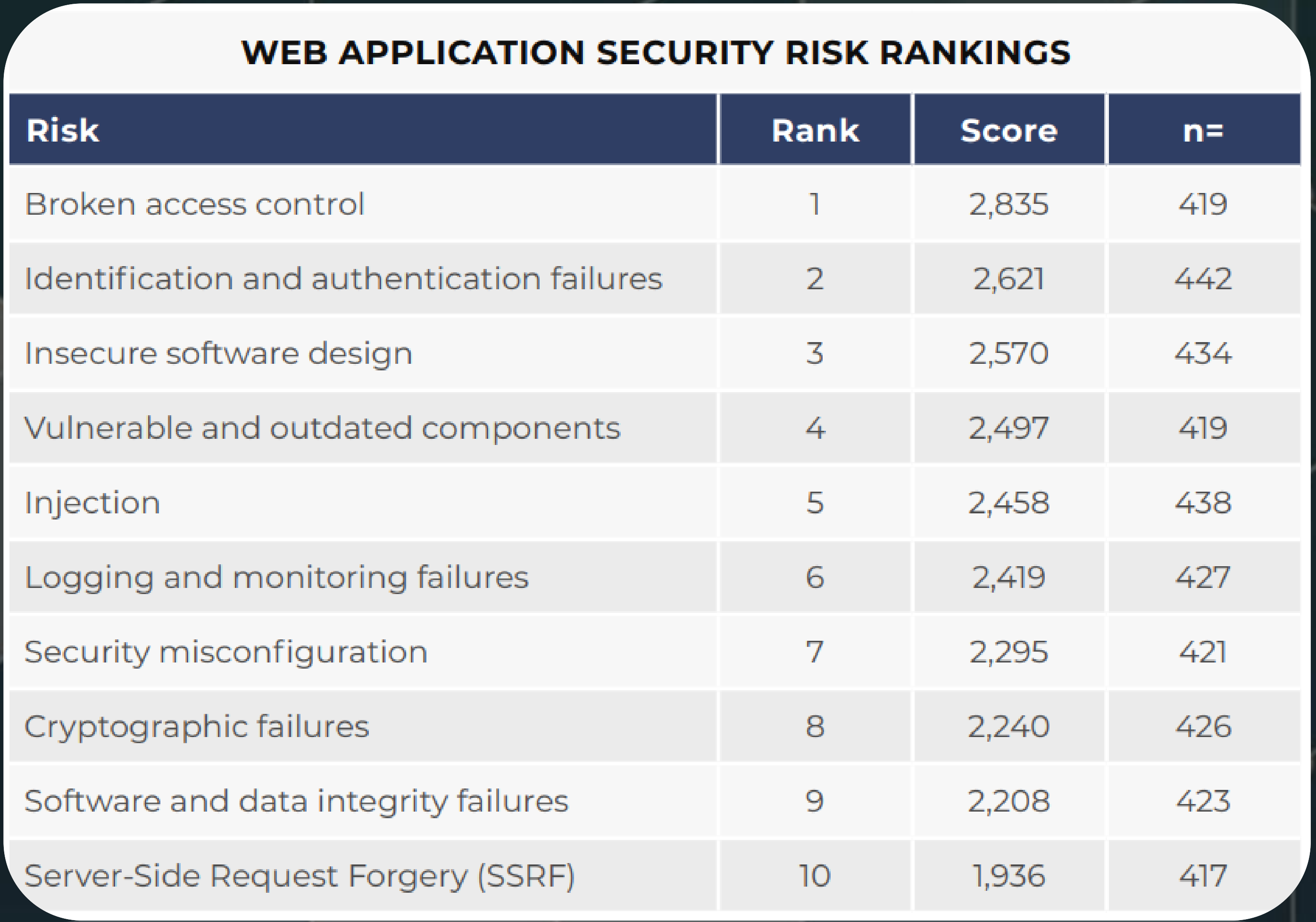
01

Issues of the Digital World Today & Tomorrow

Issues (1/4) | OWASP’s Top 10 Web App Security Risks in 2021

Web Application Security has been one of the most prominent attack magnets for the threat adversaries

1. Broken Access Controls
2. Identification / authentication failures and vulnerable/outdated components are ranked more problematic
3. Cryptographic failures and injection are ranked less problematic



WEB APPLICATION SECURITY RISK RANKINGS

Risk	Rank	Score	n=
Broken access control	1	2,835	419
Identification and authentication failures	2	2,621	442
Insecure software design	3	2,570	434
Vulnerable and outdated components	4	2,497	419
Injection	5	2,458	438
Logging and monitoring failures	6	2,419	427
Security misconfiguration	7	2,295	421
Cryptographic failures	8	2,240	426
Software and data integrity failures	9	2,208	423
Server-Side Request Forgery (SSRF)	10	1,936	417

Courtesy of | OWASP Report 2021

Issues (2/4)| Cyber Attack on Supply Chain Ecosystem Process, People, Organisations & Distribution

In cybersecurity, supply chain involves resources (hardware and software), storage (cloud or local), distribution mechanisms (web applications, online stores) and management software.

Key elements in a supply chain:

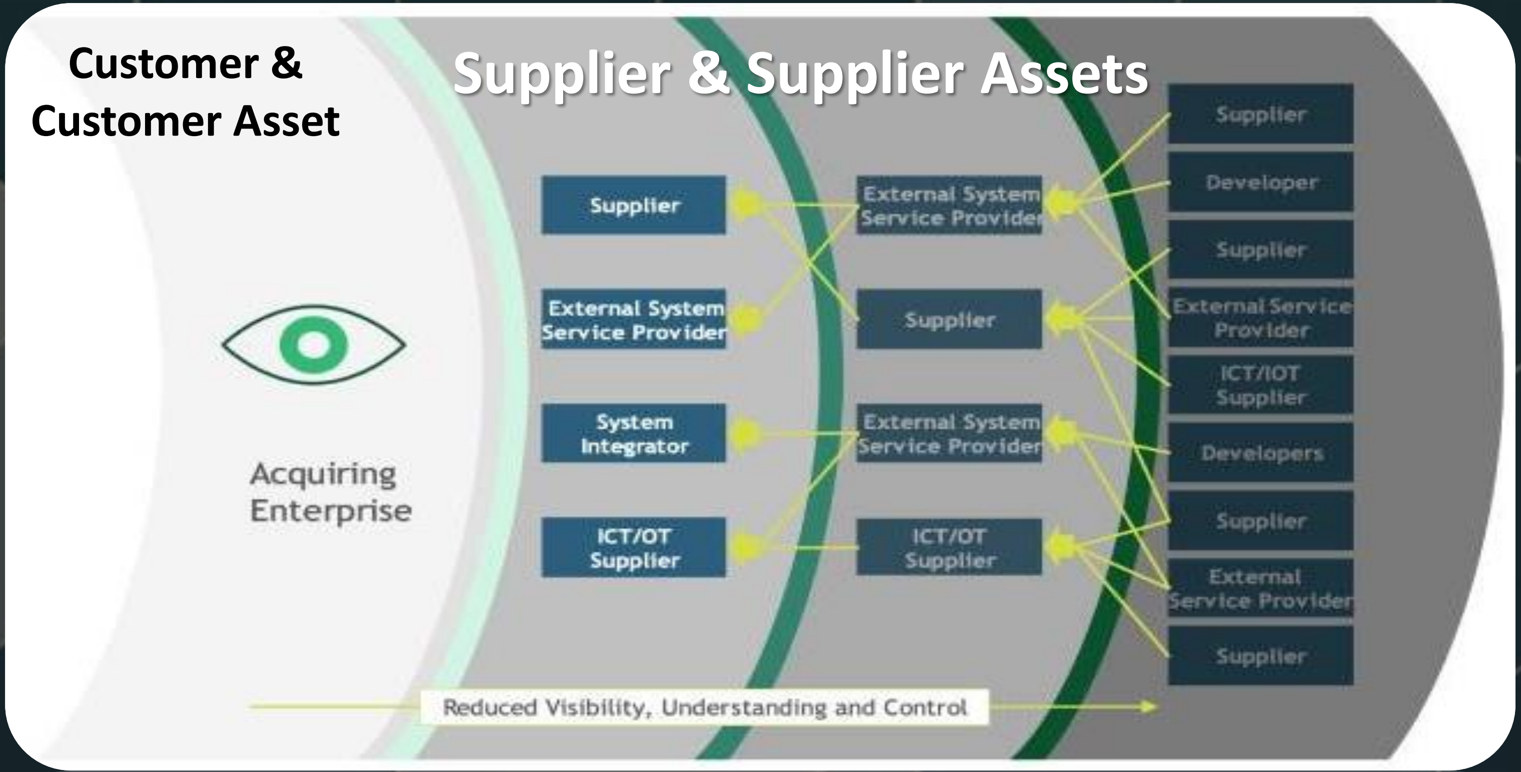
Supplier: An entity that supplies a product or service to another entity.

Supplier Assets: Valuable elements used by supplier to produce the product or service.

Customer: Entity that consumes the product or service produced by the supplier.

Customer Assets: Valuable elements owned by the target.

An entity can be individuals, groups of individuals, or organizations. Assets can be people, software, documents, finances, hardware, or others.


Customer &
Customer Asset
Supplier & Supplier Assets
Acquiring Enterprise
Supplier
External System Service Provider
System Integrator
ICT/OT Supplier
External System Service Provider
Supplier
External System Service Provider
ICT/OT Supplier
Supplier
Developer
Supplier
External Service Provider
ICT/IOT Supplier
Developers
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

Enterprise's visibility and ability to understand and control its supply chain

Issues (3/4)| Believes, Threats, Controls & Passwords

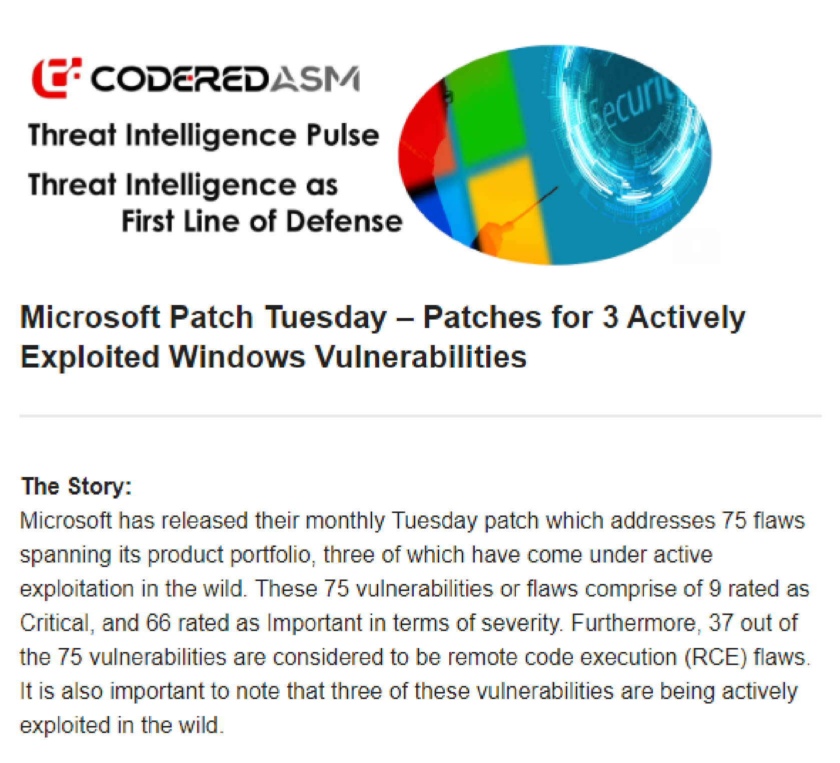
Businesses Believes

- Believe they are too small to be a target
- Believe they have sufficient protection in place?
- Perception that security is too expensive, complex, and demanding

42% of SMBs blame their security issues on lack of trainings

– SMB Security Report 2022, Datto

Threats and Vulnerabilities



CODEREDASM

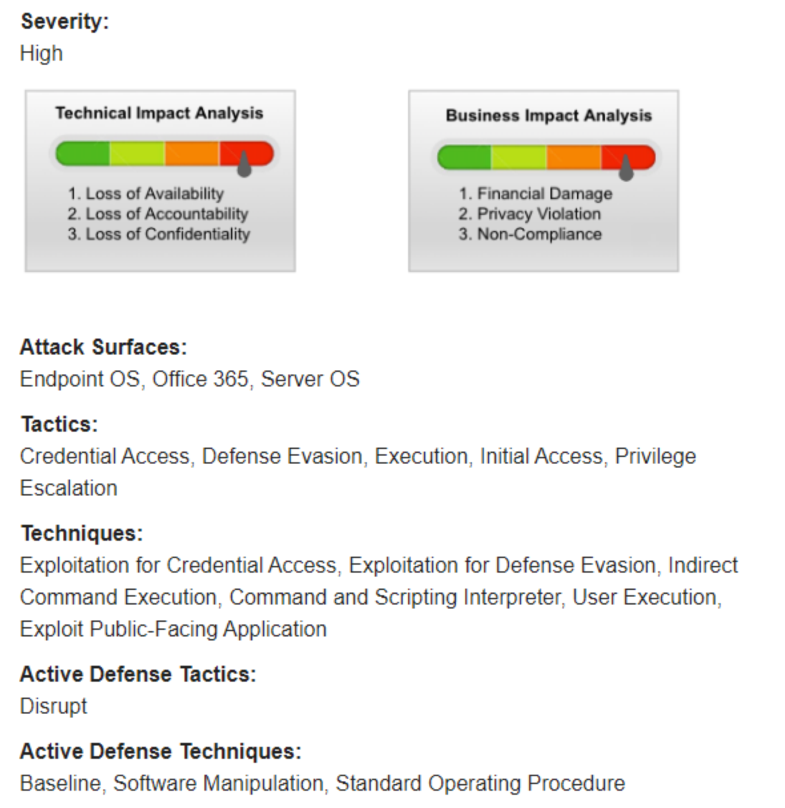
Threat Intelligence Pulse

Threat Intelligence as First Line of Defense

Microsoft Patch Tuesday – Patches for 3 Actively Exploited Windows Vulnerabilities

The Story:

Microsoft has released their monthly Tuesday patch which addresses 75 flaws spanning its product portfolio, three of which have come under active exploitation in the wild. These 75 vulnerabilities or flaws comprise of 9 rated as Critical, and 66 rated as Important in terms of severity. Furthermore, 37 out of the 75 vulnerabilities are considered to be remote code execution (RCE) flaws. It is also important to note that three of these vulnerabilities are being actively exploited in the wild.



Severity:
High

Technical Impact Analysis

1. Loss of Availability
2. Loss of Accountability
3. Loss of Confidentiality

Business Impact Analysis

1. Financial Damage
2. Privacy Violation
3. Non-Compliance

Attack Surfaces:
Endpoint OS, Office 365, Server OS

Tactics:
Credential Access, Defense Evasion, Execution, Initial Access, Privilege Escalation

Techniques:
Exploitation for Credential Access, Exploitation for Defense Evasion, Indirect Command Execution, Command and Scripting Interpreter, User Execution, Exploit Public-Facing Application

Active Defense Tactics:
Disrupt

Active Defense Techniques:
Baseline, Software Manipulation, Standard Operating Procedure

CODEREDASM @ 2023

Vulnerabilities:

(1) Office Security Feature Bypass Vulnerability (2) Windows Graphics Component Elevation of Privilege (3) VulnerabilityWindows Common Log File System (CLFS) Driver Elevation of Privilege Vulnerability

Issues (4/4)| Believes, Threats, Controls & Passwords

Passwords?

Common Passwords Are Bad Passwords

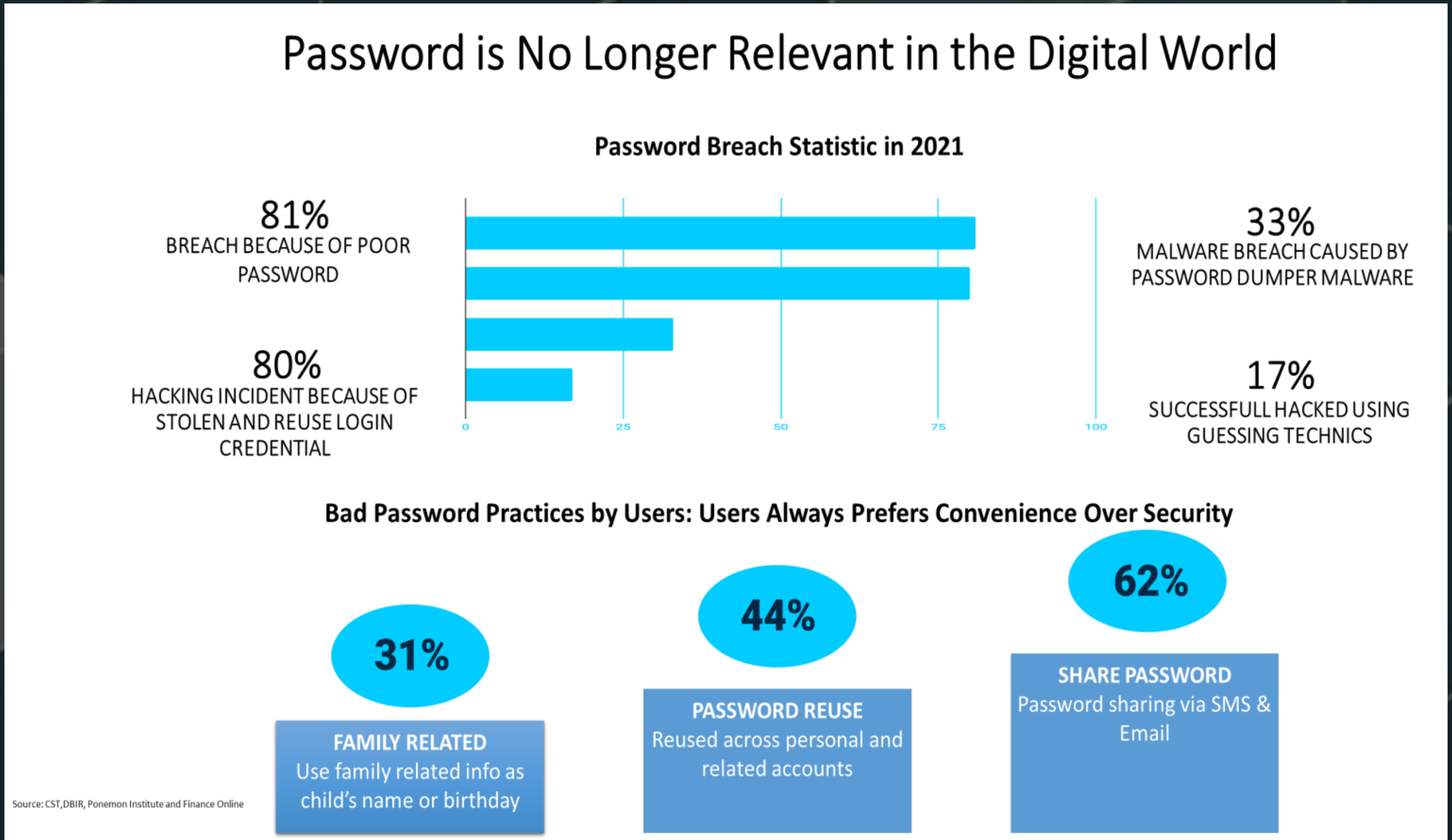
Passwords are your first line of security defense. Weak passwords and access management continue to remain in the top 5 issues for SMBs when it comes to security. Cybercriminals attempting to infiltrate your network will start by trying the most common passwords. The folks over at Safety Detectives captured the top 30 most used passwords in the world. See those below.

BEST PRACTICE: Ensure use of long (over 8 characters), complex (include lower case, upper case, numbers and non alpha characters) passwords.

The 30 Most Common Passwords

(If you have one of these, change it NOW!)

123456
password
123456789
12345
12345678
qwerty
1234567
111111
1234567890
123123
abc123
1234
password1
iloveyou
1q2w3e4r
000000
qwerty123
zaq12wsx
dragon
sunshine
princess
letmein
654321
monkey
27653
1qaz2wsx
123321
qwertyuiop
superman
asdfghjkl



Password is No Longer Relevant in the Digital World

Password Breach Statistic in 2021

81%
BREACH BECAUSE OF POOR PASSWORD

80%
HACKING INCIDENT BECAUSE OF STOLEN AND REUSE LOGIN CREDENTIAL

33%
MALWARE BREACH CAUSED BY PASSWORD DUMPER MALWARE

17%
SUCCESSFULL HACKED USING GUESSING TECHNICS

Bad Password Practices by Users: Users Always Prefers Convenience Over Security

31%
FAMILY RELATED
Use family related info as child's name or birthday

44%
PASSWORD REUSE
Reused across personal and related accounts

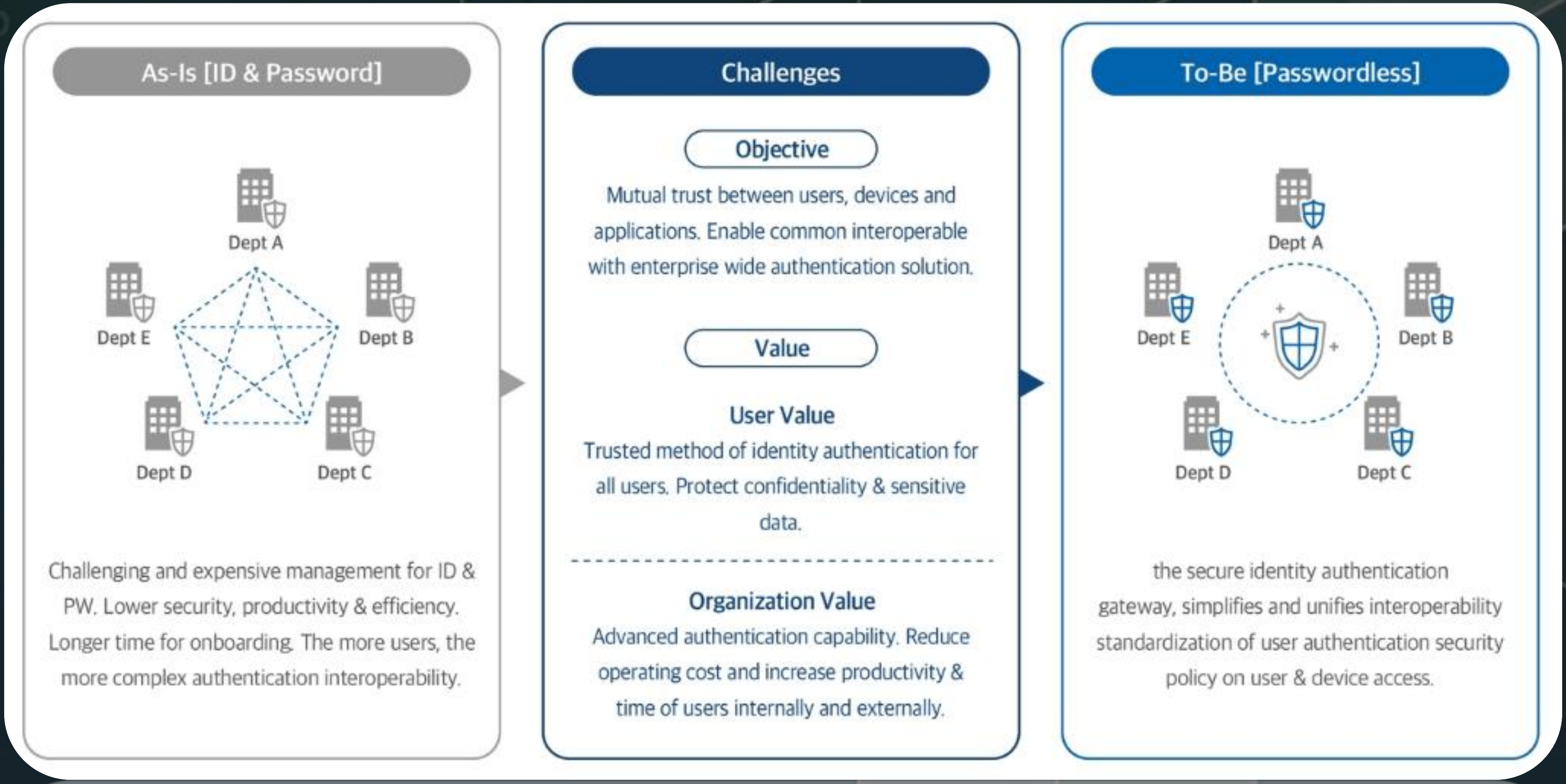
62%
SHARE PASSWORD
Password sharing via SMS & Email

Source: CST,DBIR, Ponemon Institute and Finance Online

02

What & Why Blockchain Authentication Secure Authentication is Critical

Harmonizing both Convenience and Security at highest level



As-Is [ID & Password]

Challenging and expensive management for ID & PW. Lower security, productivity & efficiency. Longer time for onboarding. The more users, the more complex authentication interoperability.

Challenges

Objective

Mutual trust between users, devices and applications. Enable common interoperable with enterprise wide authentication solution.

Value

User Value

Trusted method of identity authentication for all users. Protect confidentiality & sensitive data.

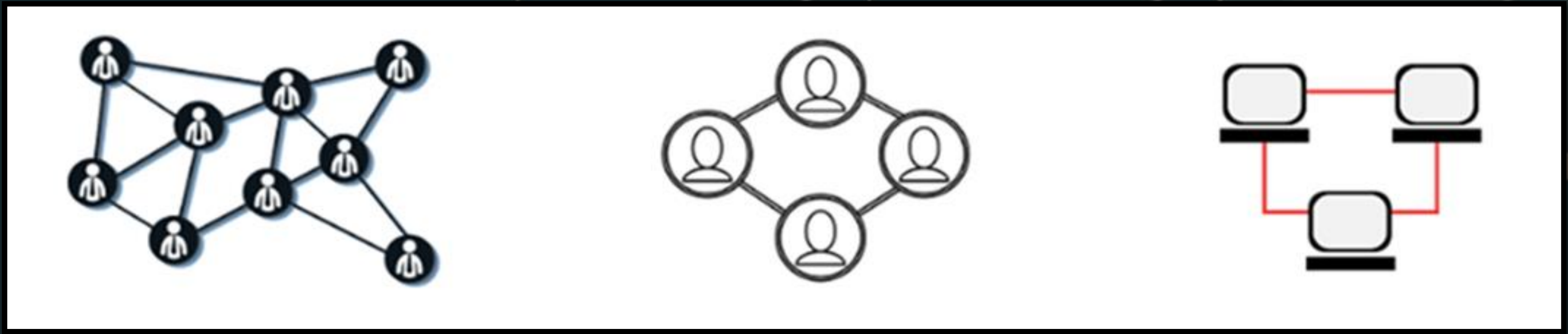
Organization Value

Advanced authentication capability. Reduce operating cost and increase productivity & time of users internally and externally.

To-Be [Passwordless]

the secure identity authentication gateway, simplifies and unifies interoperability standardization of user authentication security policy on user & device access.

Main Characteristics of Blockchain in Securing Authentication



Decentralized

- The control/power is not held by single entity. Instead it is distributed among multiple participants.
- Even if one node is corrupted/fails – the network repair itself

Peer-to-Peer

- Direct peer-to-peer transaction of data.
- Decentralized nature of blockchain instils trust in the process such that two unknown parties can directly interact/transact with each other

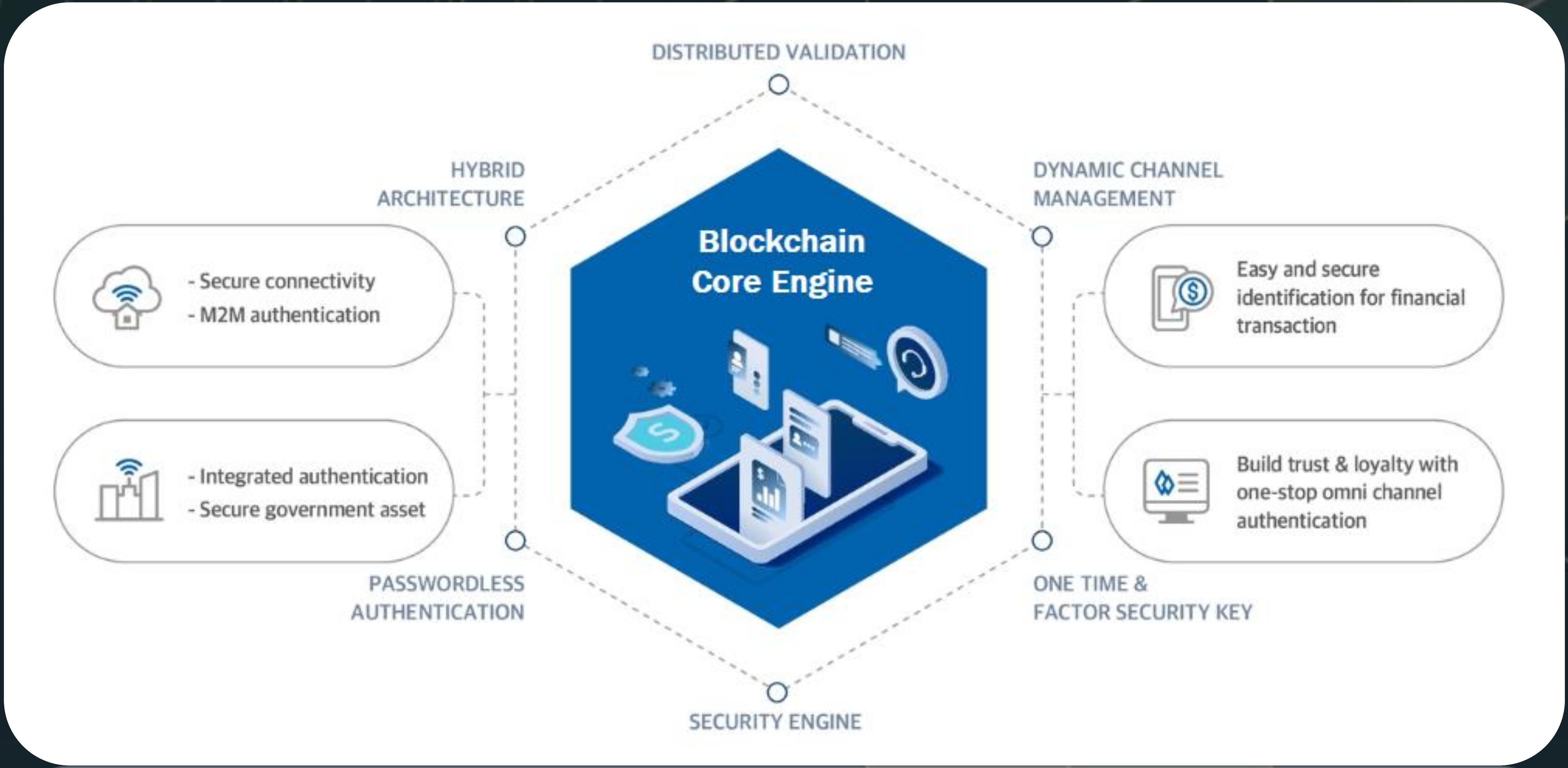
Distributed

- Data is distributed among the nodes (computers / hard drives).
- Even if one node is tampered, the data does not get compromised

03

Technology

Technology Deployment with Passwordless Blockchain Authentication & Verification



DISTRIBUTED VALIDATION

HYBRID ARCHITECTURE

DYNAMIC CHANNEL MANAGEMENT

Blockchain Core Engine

- Secure connectivity
- M2M authentication

- Integrated authentication
- Secure government asset

Easy and secure identification for financial transaction

Build trust & loyalty with one-stop omni channel authentication

PASSWORDLESS AUTHENTICATION

ONE TIME & FACTOR SECURITY KEY

SECURITY ENGINE

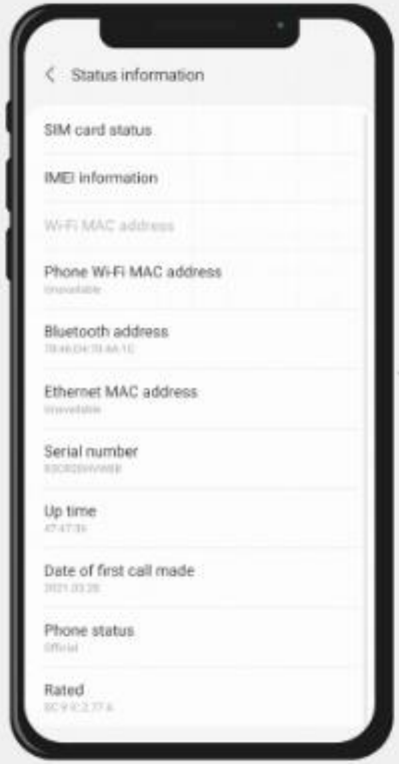
Tech 1 | Run Multi Identifier at random at all times

01 Mobile Device : Major Source of Authenticator

02 Extract Multiple Unique Identifiers from User's Mobile Device

03 Combination from Identifier Ecosystem across Location, Ownership Identifier, Device Identifier & Knowledge Base Information

04 Unhackable Passwordless Authentication



Status information

SIM card status

IMEI information

Wi-Fi MAC address

Phone Wi-Fi MAC address
Unavailable

Bluetooth address
78:46:D4:78:4A:1C

Ethernet MAC address
Unavailable

Serial number
R3CR20HVWBB

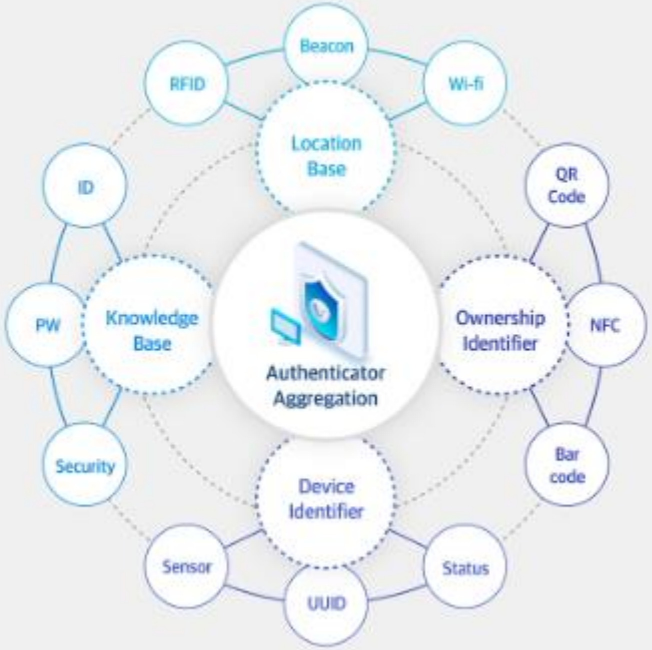
Up time
47:47:36

Date of first call made
2021.03.28

Phone status
Official

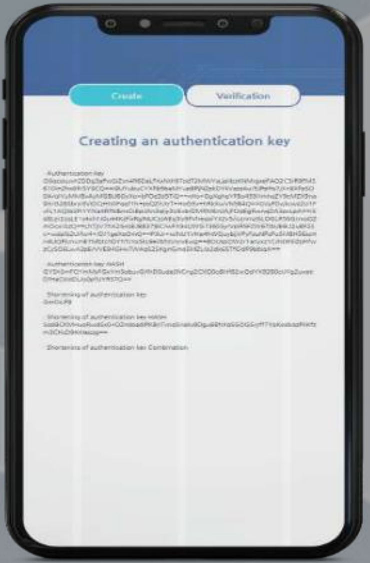
Rated
DC 9 V 2.77 A

Mobile number 010-1234-5678	Sound sensor 15 | 11 | 0 | 0 | 0 | 0 | 4
MAC address 50:77:05:3f:81:49	Bluetooth address 20:00:00:00:00:00
Wi-fi info FNS iptime	Proximity sensor 8
Brightness sensor 990	Terrestrial magnetism sensor 13|52|-39
Device unique No 00000000-7849-0649-f202-3db11c503a2e	



Authenticate with unique user device

Tech 2 | Creation of Security Key of One-Times Used



Creating an authentication key

Authentication key
[illegible]

Authentication key HASH
[illegible]

Shortening of authentication key
[illegible]

Shortening of authentication key HASH
[illegible]

Shortening of authentication key Confirmation

1st Key Generation

STEP 01

Key generation

Generating 300+ numeral security key

STEP 02

Encryption

Encryption of the security key generated at step1

2nd Key Generation

STEP 03

Key generation

Abstracting security key generated at step2

STEP 04

Encryption

Re-encryption of the abstracted security key generated at step3

3rd Key Generation

STEP 05

Key generation

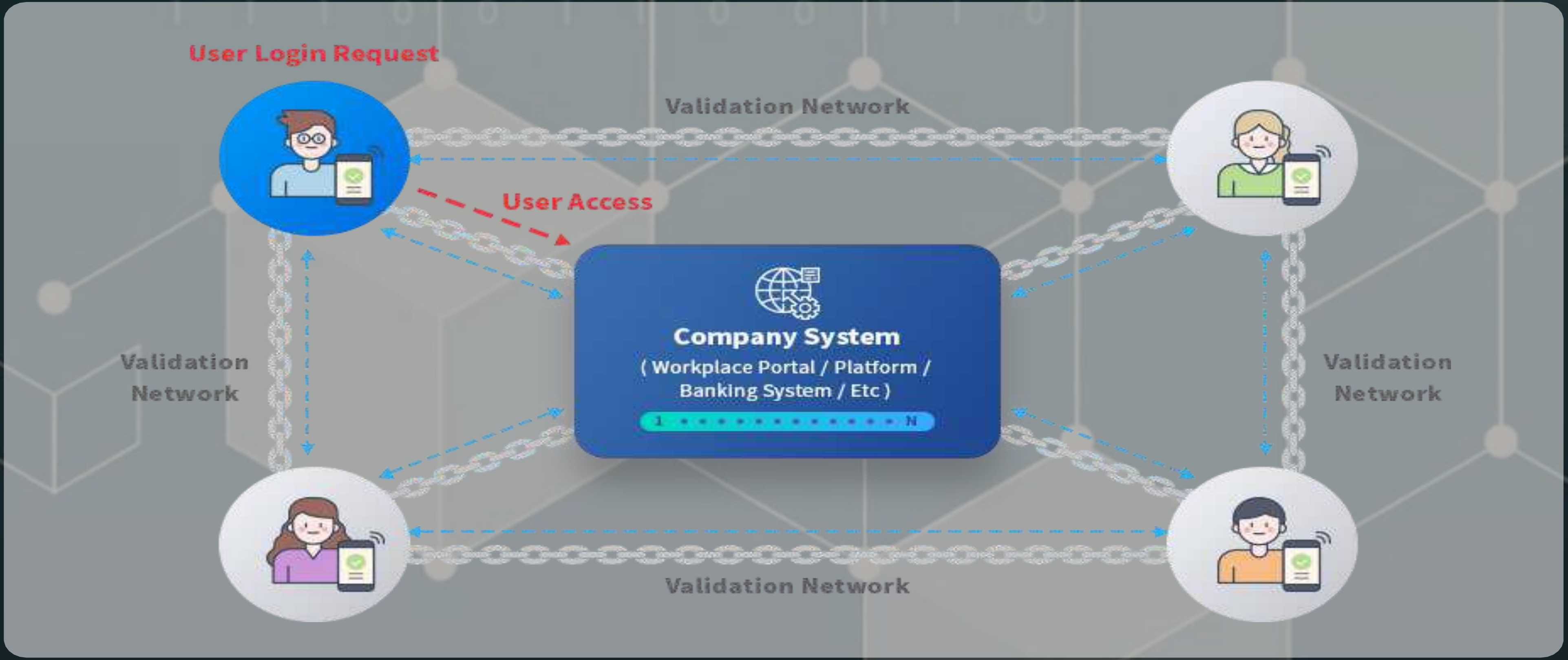
Merging the encrypted security keys generated at step2 and step4

STEP 06

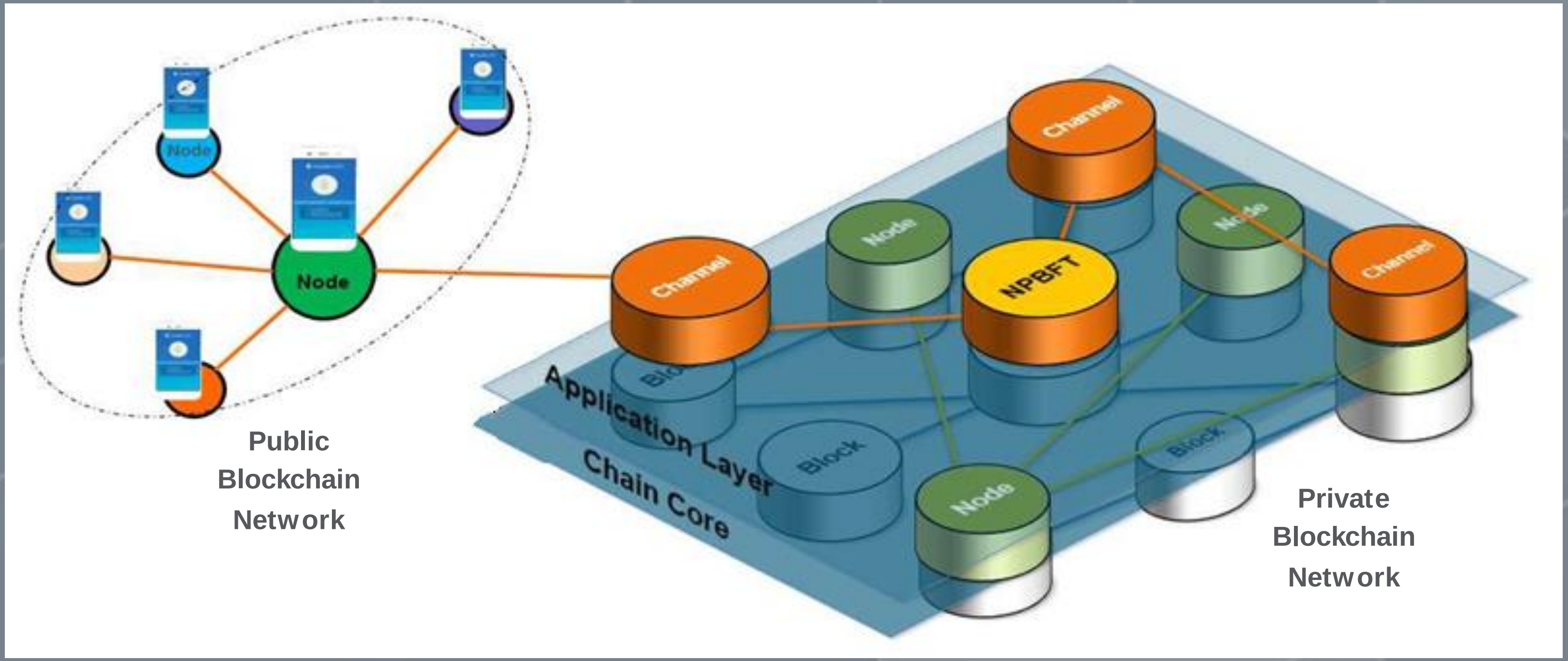
Encryption

Re-encryption of the security key merged at step5

Tech 3 | Randomized Distribution for Verification



Tech 4 | Security by Designed Hybrid Blockchain Network Environment



04

What is Next?

The Future | Going Forward with Blockchain Technology

1. **Efficiency and Competitive Advantage**
   - Organizations are adopting blockchain solutions to enhance their operations efficiency and to gain competitive advantage.
2. **Blockchain Development Challenges & Risks**
   - Developing blockchain technology have its challenges in terms of skillsets, available experts and the supports required.
   - Global standards, governance, regulatory and risks compliance
3. **Security, Trust, Privacy and Cost Savings**
   - Blockchain technology promote security, trust and privacy and eliminate intermediaries, human interventions and reduce costs.
   - Blockchain data and transactions are immutable, unchangeable, accurate and secure.
   - Blockchain architecture eliminate issues related to trust due to decentralized and tamper-proof technological environment; transactions are fully trusted in incorruptible and failure-proof blockchain network.
4. **Blockchain and Quantum Resistant Technology as key stronghold for data, process and infrastructure**
   - Ensuring next-generation evolution will endure quantum threats for better mitigations, controls and maintain sustainability.

BSA

Thank you!

FNS (M) SDN.BHD.
FEASIBLE NETWORK SYSTEM