Cyber Security In Higher Education

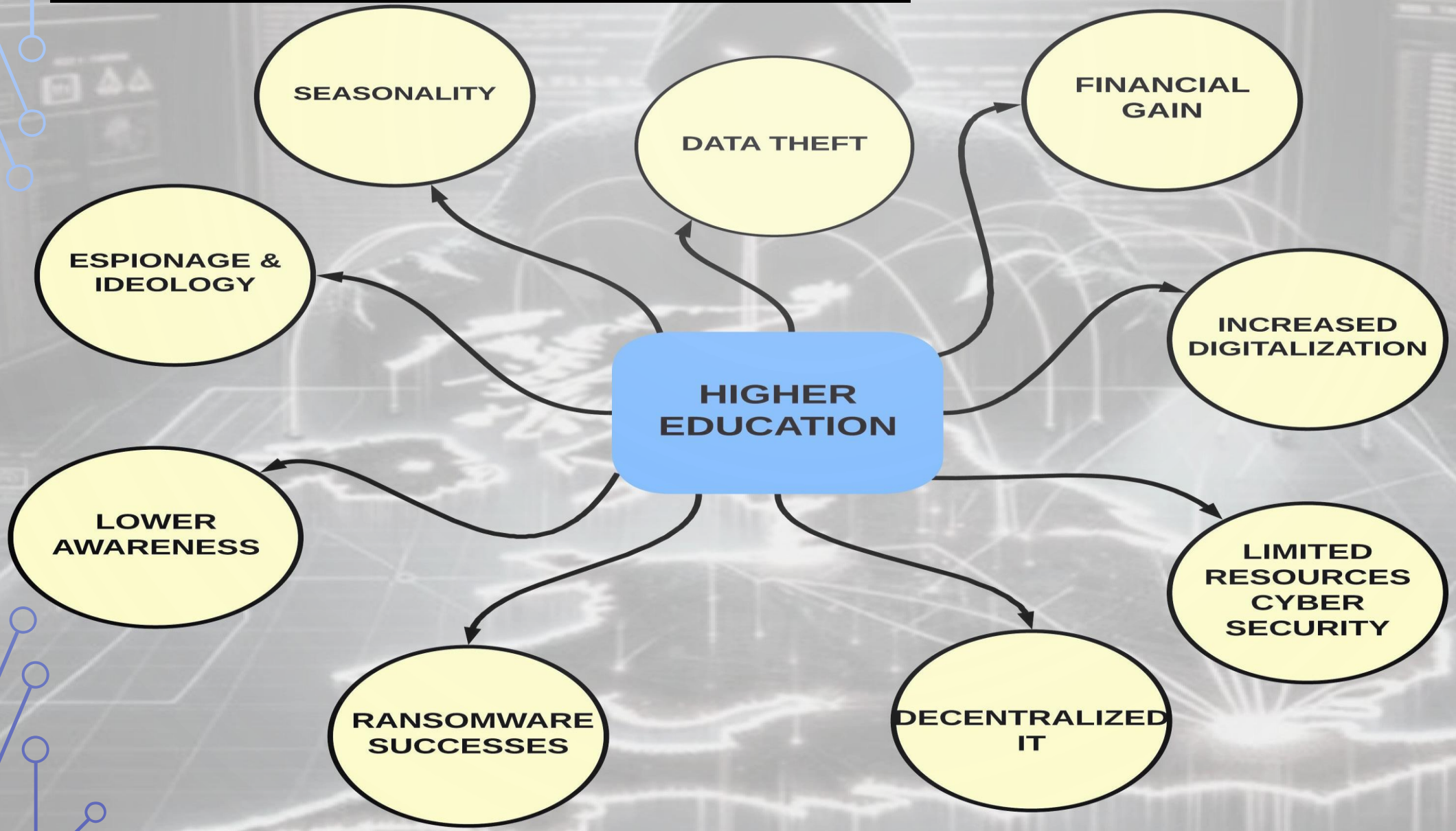
Protecting Users With Decentralized Digital Identities

STEFAN KENDZIERSKYJ

NOV 2024

Maverick Publishing Specialists
SK CONSULTANCY

WHY EDUCATION IS UNDER THREAT



TOP SECTORS FOR CYBER ATTACKS

Where does the Education Sector rank in cyber attacks?

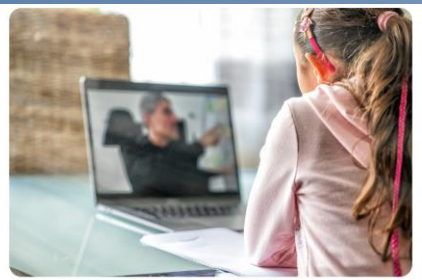
Top 3 are Healthcare / Finance / Government

Education is closely behind the Top 3

- 93% increase UK Education (NCSC, 2022)
  - 62% of Higher Education (HE) institutions reported experiencing breaches or attacks at least weekly
  - 71% of HE institutions had experienced a negative outcome, such as a loss of money or data from a breach
  - 50% of HE institutions – accounts/systems had been compromised and used for illicit purposes

NUMEROUS EDUCATION CYBER ATTACKS

Education has been hit the hardest by the increase in cyber-attacks



Cambridge among universities hit by 'malicious' cyber attack

The attack meant internet access was intermittent and some services for staff and students were 'degraded'

University confirms 'cyber security incident'

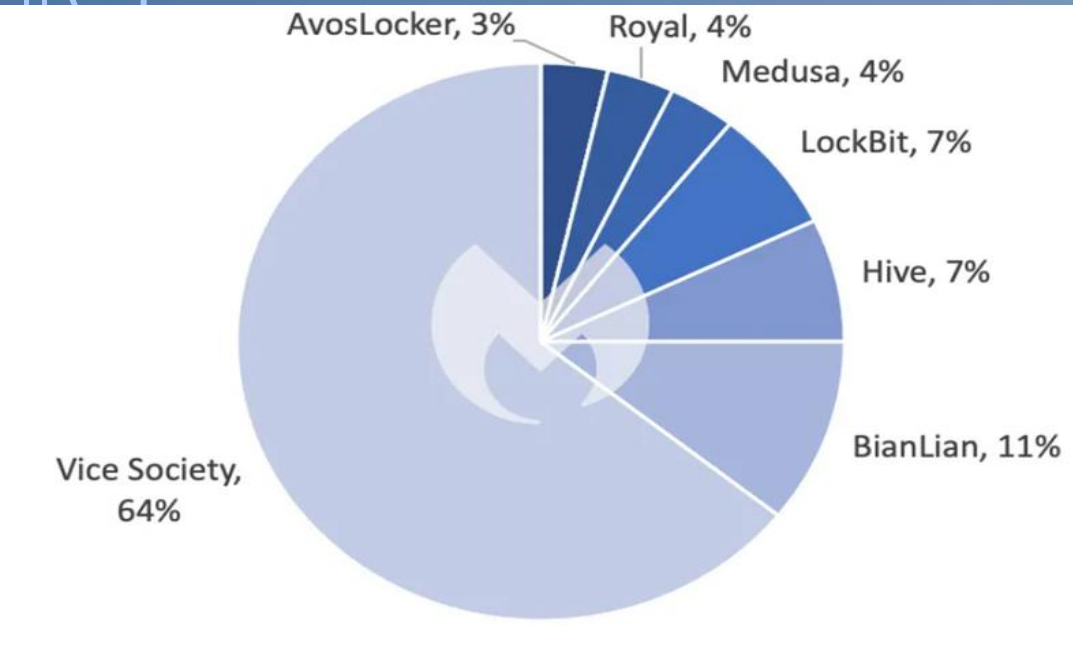
Scottish university UWS targeted by cyber attackers

28 July 2023

University confirms 'Cyber Security Incident'

By Ellis Peters | March 13, 2024 | Cyber Security

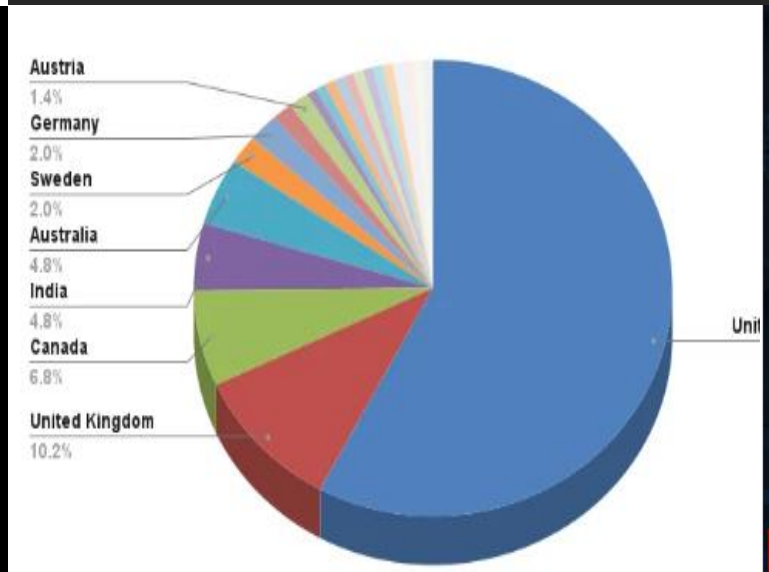
TYPES OF EDUCATION CYBER ATTACKS



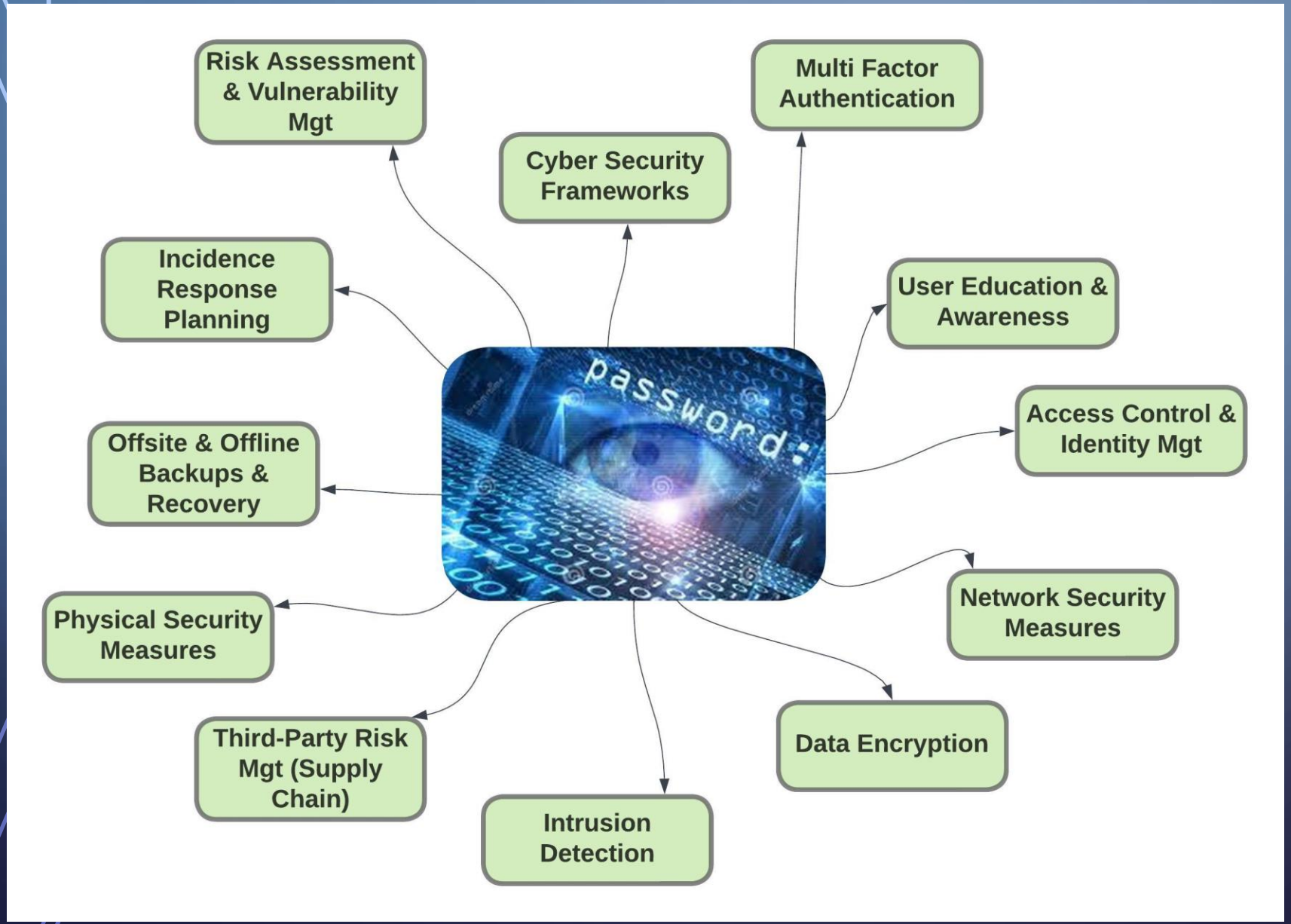

```
ALL YOUR FILES HAVE BEEN ENCRYPTED BY VICE SOCIETY
All your important documents, photos, databases were stolen and encrypted.
If you do not contact us in 7 days we will upload your files to darknet!
The only method of recovering files is to purchase an unique private key.

We are the only who can give you tool to recover your files.
To proove that we have the key and it works you can send us 2 files and we decrypt it for free (not more than 2 MB each).
This file should be not valuable!
Write to email: CoryFrempton@onionmail\.org
Alternative email: DanyTron@onionmail\.org
v-society.official@onionmail\.org
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.
Visit our website 4hzyuotli6maqa4u\.onion
Use tor browser to open
```

Types of Education Cyber Attacks

- Phishing
- Malware
- Ransomware
- Spam
- DDOS
- Supply chain attacks



WHAT ACTIONS CAN BE TAKEN – TRADITIONAL METHODS



- User Awareness & Education
- Technology Landscape Review
- Implement GRC & Cyber Security strategy

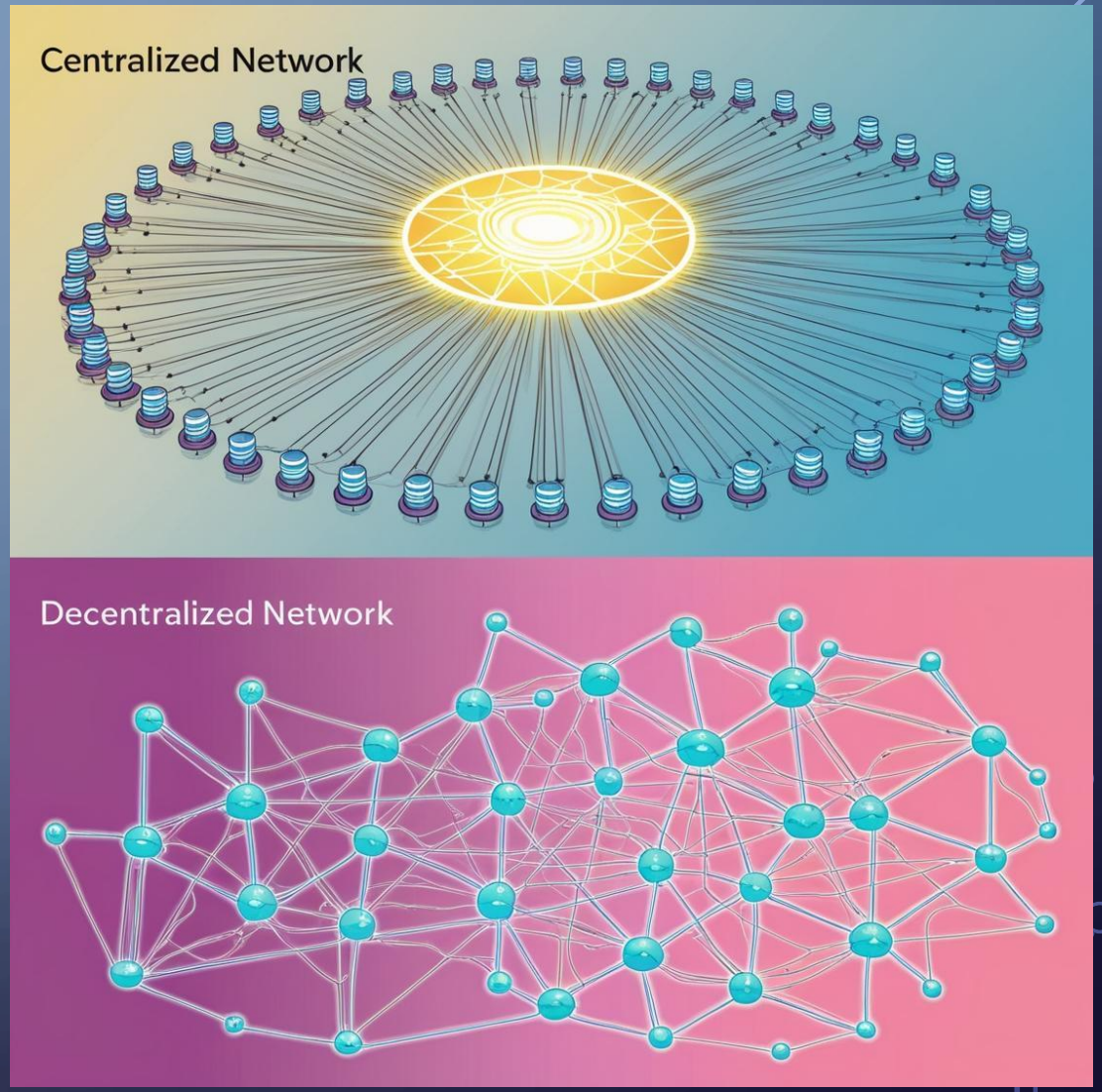
WHAT OTHER APPROACHES CAN BE TAKEN

Centralized – All nodes connected to single servers under one Authority

- ✅ Easy to Manage, Cost-effective & Performance Optimization
- ❌ Single Point of Failure, Scalability Issues, Data Security, Limited User Controls

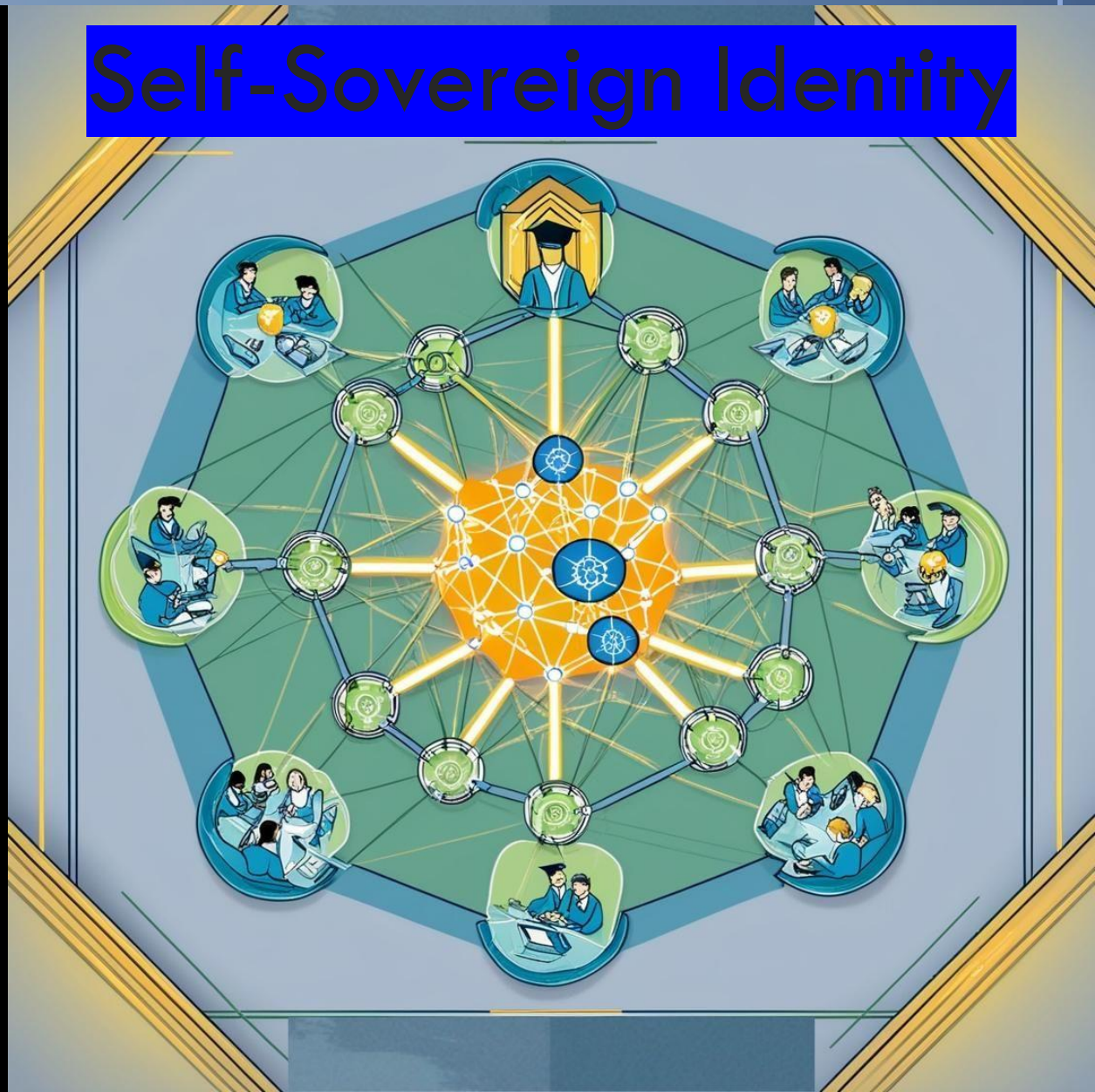
Decentralized – Distributes data and Authority across multiple nodes: there is no single Authority

- ✅ Resilience, Scalable, Enhanced Security, User Autonomy
- ❌ Complex Protocols, Requires Advanced Data Techniques, Performance Issues, Potential Higher Costs



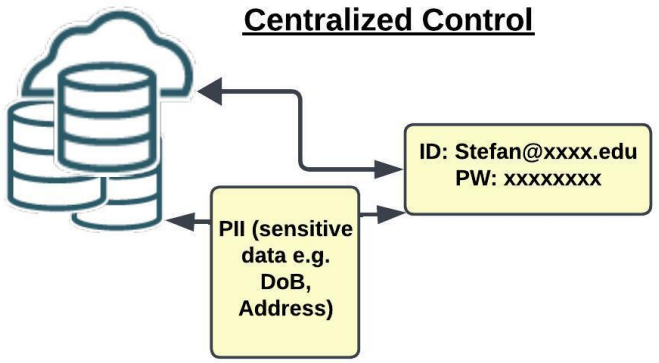
DECENTRALIZED APPROACH – BLOCKCHAIN CHARACTERISTICS

- **Education -** Data breaches are increasing! It is easier to manipulate data
  - Centralized systems puts data at risk of large-scale hacks and breaches
    - Federated model enables companies to track user data without their knowledge
  - Outdated verification systems and reduced security with traditional identity management systems
  - Academic records are maintained by schools/universities
  - Verification by other institutions is often slow & cumbersome
  - No guarantee of accuracy or timeliness of records
- **Identity -** is a key issue: every student has a unique identity used to identify them in the system, and track educational progress, financial and personal records
- **Decentralized: Blockchain As Alternative Solution**
  - Immutability: Elevated level of security (Tamper-Proof)
  - Interoperable: Different institutions can share data securely & efficiently
  - Transparency, Privacy & Security: Gives individuals more control
  - Chain of Custody: Decentralized Digital Identities (DIDs)
  - Enables secure, decentralized digital identity for each student
  - Facilitates easy and quick sharing of academic records with any institution
  - Eliminates the need for slow and expensive background checks



SELF-SOVEREIGN IDENTITY (SSI)

What is it?



- Centralized: entity controls data and where it goes
- Federated login is not in the Users control: Google may use people's personal data to store and track their online activity without their knowledge, or present access issues

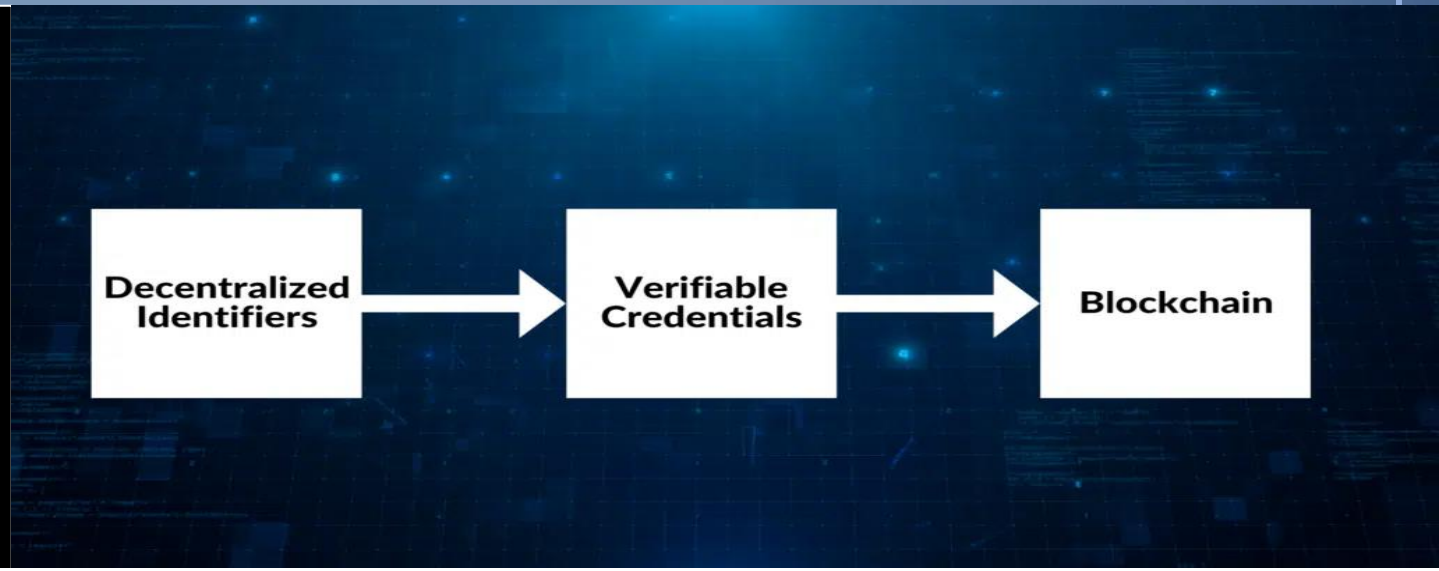
SSI

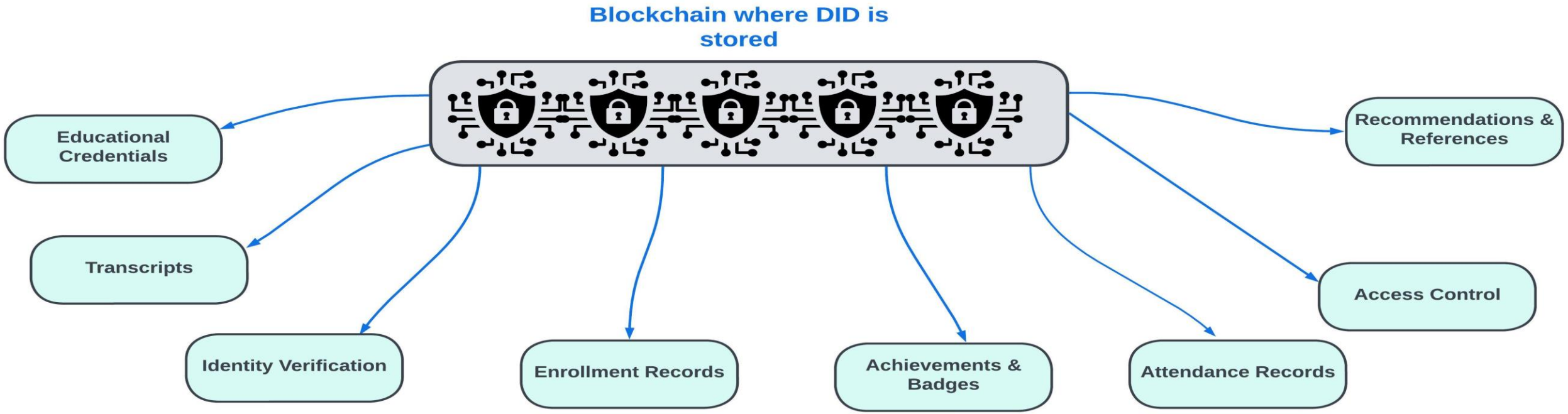
- Empowers individuals with complete ownership and control over their digital identities
- Determine who can access your data & flexibility to revoke access
- SSI credentials are not tied to one issuer and can be taken from University to other Education provider or employer to employer (degrees, certifications, etc) without having to send requests to verify to each institution
- Reduces opportunity for fraud and tampering. Once information is published on the blockchain, it is cryptographically verified and can't be modified by the end user
- Expands beyond just education verification to broader applications in the education ecosystem (e.g., smart devices, IoT, banking, social media)

SELF-SOVEREIGN IDENTITY IN EDUCATION

Three Pillars in SSI

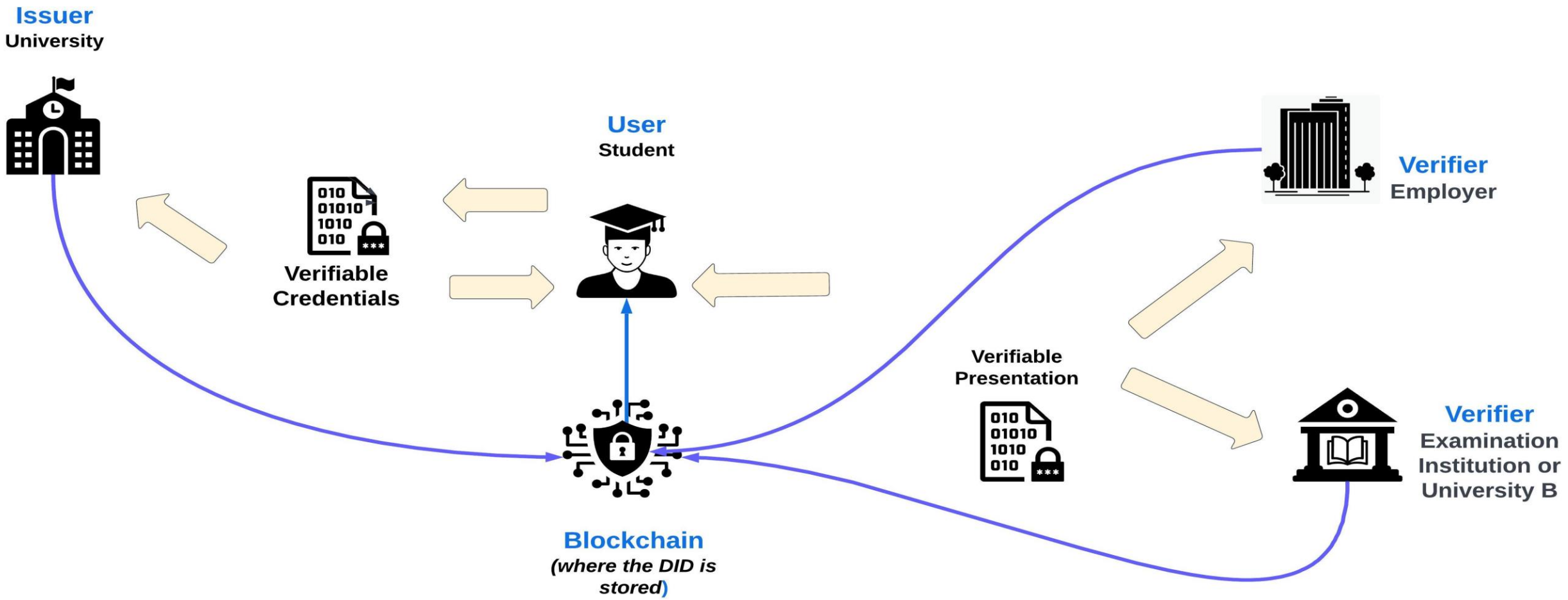
- 1. Blockchain: A secure, decentralized ledger shared across a network of computers that resists tampering and hacking
- 2. Decentralized Identifiers (DIDs): A method for online identity verification that doesn't depend on centralized organizations, using a unique blockchain-stored code for greater control over personal information
- 3. Verifiable Credentials (VCs): Digitally-secured versions of traditional credentials that can be presented to verifiers for authentication





- Student (User) has a decentralized digital identifier (DID) stored on blockchain with digital identity wallet for professional purposes and the DID automatically comes with a private and public key pair
- User stores & manages credentials (degree, courses, etc), select/send from DID
- Issuer (University) and Verifier (e.g., Employer) can confidently check the DID and see it is authentic

- Ensures secure and private verification of necessary data with no risk to the student
- Data Control: Students maintain control over their personal data, with the ability to grant or revoke access permissions
- Secure Research Sharing: Decentralized system for storing and sharing academic research, facilitating easier data access while preventing fraud



SUMMARY

- Data breaches in HE are increasing
- Needs more investment as per other sectors (e.g., Finance, Healthcare)
- Centralized Model - Mitigate issues by evaluating its technologies, more disciplined education & awareness & strengthening with cyber security solutions
- Decentralized Model - Offer alternative ways to protect data security, users' privacy and identity


Questions?
LN: www.linkedin.com/in/stefankend
SK CONSULTANCY