JOANNEUM RESEARCH DIGITAL

Challenges of new Technologies – Distributed Ledger and Cybersecurity

Dr. Branka Stojanović
Senior Researcher, CISSP
branka.stojanovic@joanneum.at

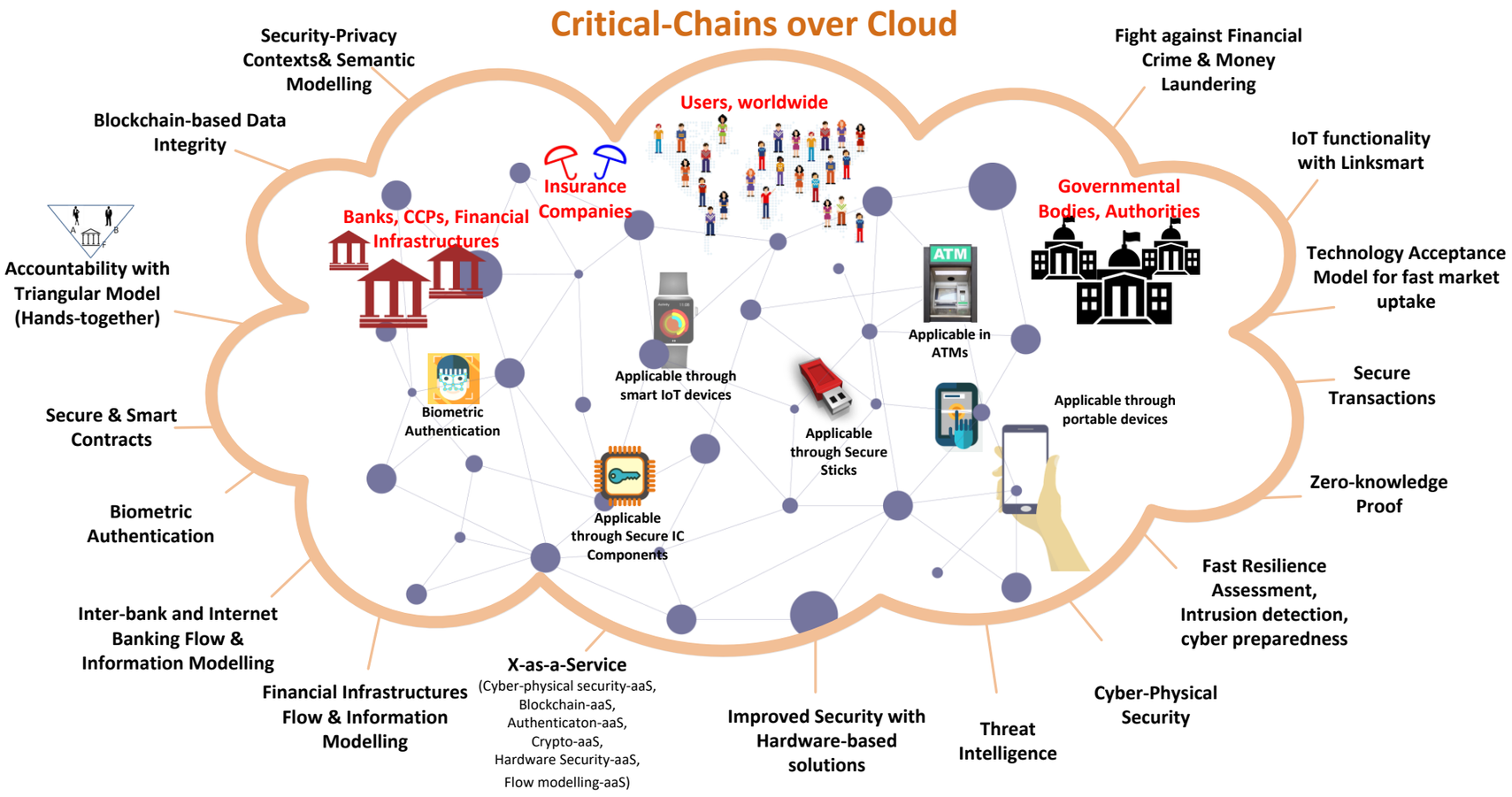
JOANNEUM RESEARCH DIGITAL

Critical Chains

IOT- & Blockchain-Enabled Security Framework for New Generation Critical Cyber-Physical Systems In Finance Sector, Grant No. 833326

- Topic:
  - H2020-SU-DS-2018 (IA): Digital Security, Privacy, Data Protection and Accountability in Critical Sectors
- Project timeline:
  - July 2019 – June 2022

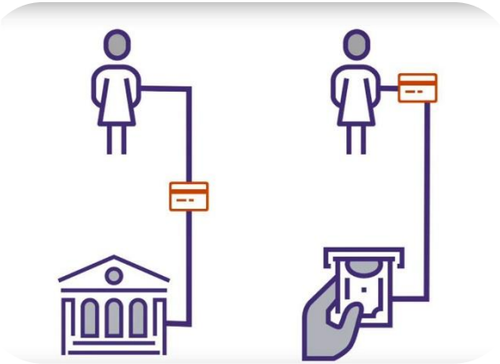
Critical Chains



Critical Chains

Banking

Insurance



Financial Market Infrastructure

Electronic Toll Collection

General

- **Fintech** is **evolving rapidly**, yet still have dependencies on **ancient technology standards**
- Legacy systems
  - Pros – stability, reliability, availability
  - Cons – cannot cope well with the enormous amounts of data and modern threat scenarios
- Our focus – the security of financial technologies in the Fintech domain
  - categorization and taxonomies of the main cyber-attack types, and suitable countermeasures

- Reference: Ankele, R., Nahrgang, K., Stojanovic, B. and Badii, A., 2020. **SoK: Cyber-Attack Taxonomy of Distributed Ledger- and Legacy Systems-based Financial Infrastructures**, available as preprint at https://eprint.iacr.org/2020/1440

Image source: https://www.fintechbusiness.com/data/1817-covid-heightening-bank-vulnerability-to-cyber-attack

Legacy Systems in Financial Infrastructures

- Most bank **mainframes** – old and based on outdated coding language
- A study by Reuters in 2017 about major US banking systems
  - 43% of banking systems were build in **COBOL**
  - 80% of all in-person transactions used COBOL
  - 95% of all ATM swipe transactions rely on COBOL
- Another tool that is widely used in the finance industry are huge **Excel sheets**
- **ATM's** running **outdated operating systems**

Data and image source: https://www.fnlondon.com/articles/banks-face-spiraling-costs-from-archaic-it-20170912

Distributed Ledger-based Financial Infrastructures

- A distributed ledger is a consensus of distributed, shared, and synchronized data that is spread and maintained across multiple different geographical locations
- The **general idea originates** from **1991** and work of Haber and Stornetta about how to practically validate the generation and modification of digital documents
- The groundwork for today's **blockchain** technologies was set by Satoshi Nakamoto, by introducing **Bitcoin** in **2008**
- Use-cases that can benefit the most include: ***global payments***, ***insurance claim processing***, ***trade finance***, ***automated compliance*** and ***clearing and settlement***

Advantages of Distributed Ledger Technologies

- Simplicity and efficiency
- Disruptive technology
- Transparency
- Trust in an untrusted setting
- Reduction of operational costs
- Less bureaucracy
- Faster clearing and settlement enabling real-time money transfers…

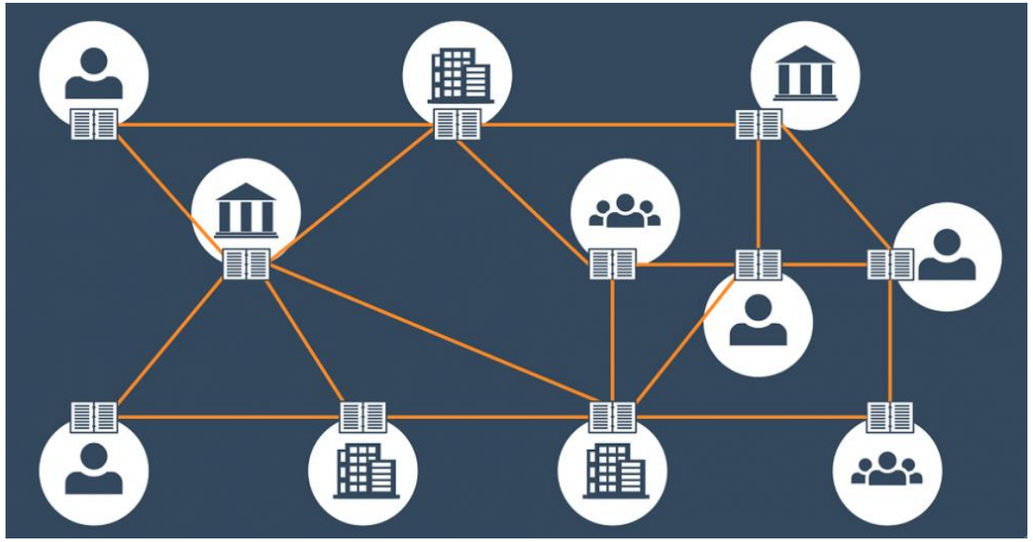


Image source: https://industrie.de/top/blockchain-kommt-unternehmen/

Cyber-Attack Taxonomy of Financial Infrastructures

- A detailed overview of threats for financial infrastructures
- Note: list is not exhaustive, and adversaries often exploit several vulnerabilities in a combination during an attack
- The threats are classified into seven categories: ***active cyber-attacks***, ***physical attacks***, ***unintentional damage***, ***scam/fraud/spoofing***, ***failure/malfunction/outage***, ***legal*** and ***targeted threats***

Active Cyber-Attacks

- Distributed Denial of Service
- **Ransomware**
- Web Application Attacks
- Hacking
- **Backdoors/Supply-Chain Attacks**
- Zero-Day Exploits/Vulnerabilities/Attacks
- Watering-hole Attacks
- Advanced Persistent Attacks
- Carding
- **Insider Threats**

Active Cyber-Attacks

- Distributed Denial of Service
- Ransomware
- Web Application Attacks
- Hacking
- Backdoors/Supply-Chain Attacks
- Zero-Day Exploits/Vulnerabilities/Attacks
- Watering-hole Attacks
- Advanced Persistent Attacks
- Carding
- **Insider Threats**

- In the finance sector the level of insider threats is as high as **58%**
  - 53% inadvertent
  - 5% malicious attacks
- These attacks do not necessarily have to originate from employees, but could as well be from third-party vendors, contractors and freelancers, trusted business partners, or former employees

Active Cyber-Attacks

- Distributed Denial of Service
- **Ransomware** →
- Web Application Attacks
- Hacking
- Backdoors/Supply-Chain Attacks

- **CryptoLocker** 2013-2014
  - via infected email attachments; MS Windows
  - extorted a total of around $3 million from victims
- **WannaCry** 2017
  - MS Windows exploit EternalBlue
  - 200.000 computers, 150 countries, hundreds of USD millions damage
- **Petya** 2016-2017
  - MS Windows exploit
  - damage more than $10 billion

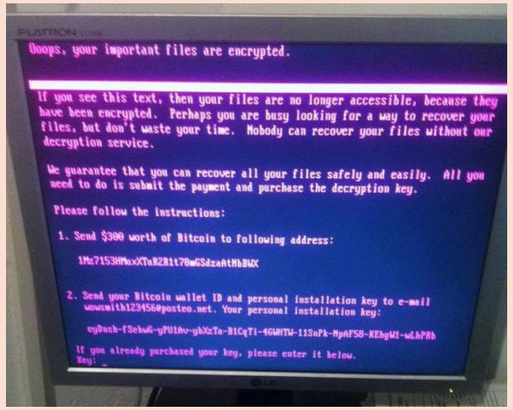


Image source: By User:Jbuket - https://uain.press/blogs/yevgen-buket-vitannya-petru-o-vid-pyeti-dnya-konstytutsiyi/, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=60473519

Physical Attacks

- Attacks against ATM's
- Bank Robbery
- Sabotage
- Vandalism
- Theft

Image source: https://www.lockpoint.co.uk/letter-to-northern-echo-after-darlington-gas-blast/

Unintentional Damage

- **Unencrypted Data**
- Insecure Third Party Services
- **Insecure Systems/Policies**
- **Human Error**
- Bad Security Audits
- Cascading Effects due to subordinate Threats

- Human error is represented as one of the major impact factors with **43%** in cyber security incidents
- Attacks are usually based on **hackers** that exploit **human weaknesses**, like lack of motivation, lack of awareness, risky behavior of employees and inadequate use of technology

Scam/Fraud/Spoofing

- Bank fraud
- Scam
- Spoofing
- **Social Engineering**
- Identity Theft
- Synthetic Fraud

Image source: https://www.pinterest.at/pin/705868941571180041/

Legal

- Regulations/Violation of Laws
  - Non-compliance and violation of regulations in the financial sector added up to penalties of US$ 36 billion globally in 2019
  - These fines include violations of regulations
    - Anti-Money Laundering (**AML**)
    - Know Your Customer (**KYC**)
    - Markets in Financial Instruments Directive (**MiFID**)
    - Global Data Protection Regulations (**GDPR**)
- Payment services directive
  - The payment services directive 2 (**PSD2**), also known as Directive (EU) 2015/2366 is a regulation with the purpose of improving the security, privacy of customers and integration of a better connected European payments market
  - Opening up API's for third-party developers adds additional security and privacy risks

Targeted Threats for Distributed Ledger Technologies

- Sybil Attack
- Eclipse Attack
- Alternative history attack
- Race Attacks
- **Loss of private keys**
- Finney & Vector76 Attack
- Block Withholding Attack
- Bribery Attack
- **Data Privacy**

Targeted Threats for Distributed Ledger Technologies

- Sybil Attack
- Eclipse Attack
- Alternative history attack
- Race Attacks
- **Loss of private keys**

⇩

- When using cryptocurrencies, wallets store a public and private key pair
- Around **30%** of all Bitcoin are lost due to the loss of private keys

- Finney & Vector76 Attack
- Block Withholding Attack
- Bribery Attack
- **Data Privacy**

Targeted Threats for Distributed Ledger Technologies

- Sybil Attack
- Eclipse Attack
- Alternative history attack
- Race Attacks
- **Loss of private keys**
- Finney & Vector76 Attack
- Block Withholding Attack
- Bribery Attack
- **Data Privacy**

- Cryptocurrencies are usually hyped as being privacy preserving, but still…
- Decentralization and transparency allows adversaries to trace public keys and addresses of specific users
- AML laws often require wallet providers to still check the identities of their customers

Countermeasures

- It is crucial to apply the principal of **defence in depth**
  - add **multiple layers of security defences** around an IT system to add **redundancy** if a particular countermeasure fails
- A mixture of **physical**, **technical** and **administrative** defences

Firewalls	Multi-factor Authentication	Anomaly Detection	Virtual Private Networks
Blacklisting vs Whitelisting	Monitoring	Input Sanitization and Output Encoding	Sandboxing
Air Gap	Know Your Customer	Antivirus Software	Design-embedded legislation and standardization compliance
Intrusion Prevention Systems	Physical Defences	Biometrics	Validation Techniques
Intrusion Detection Systems	Encryption	Demilitarized Zones	Controlling Connections
Honeypots	Role-based Access Control	Data-centric Security	Dedicated Rules
Awareness Trainings	Penetration Testing	Password Hashing	Password Managers & External Wallets
Strong Password Policies	Threat Modelling	Logging and Auditing	

(In)Famous Cyber attacks in Fintech

- **EasyJet (2020)**
  - Affected: approximately nine million customers
  - Stolen data: email addresses, travel details
  - 2,208 customers also had credit and debit card details “accessed”
- **Capital One (2019)**
  - Capital One: 10th largest bank in the USA,
  - Affected: 10 million individuals (USA), 5 million individuals (Canada)
  - Stolen data: all personal information, credit score, credit limit, self-reported income, payment history, balance
  - Hypothesis: stolen data of users that applied for credit cards between 2005 and 2019
- **Equifax (2017)**
  - Equifax: one of the largest credit reporting companies
  - Affected: 145.5 million users (identity theft risk)
  - Stolen data: user’s personal information (including Social Security Numbers and Driver’s license numbers)

Cybersecurity data for 2020

- 85% of people posting puppy photos are trying to scam you
- 67% of data breaches resulted from credential theft, human error or social attacks
- Organized crime gangs account for 55% of attacks
- 37% of credential theft breaches used stolen or weak credentials, 25% involved phishing
- Human error accounts for 22%
- 18% of organizations reported a ransomware attack
- 41% of customers would stop buying from a business victim of a ransomware attack
- There is a cyberattack every 39 seconds
- 75% of cyberattacks start with an email
- 21% of online users are victims of hacking
- 11% of online users have been victims of data theft
- 72% of breaches target large firms

Data source: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/

Coronavirus cyberattack stats

- Coronavirus blamed for 238% rise in attacks on banks
- 80% of firms have seen an increase in cyberattacks
- 27% of attacks target banks or healthcare
- Cloud based attacks rose 630% between January and April 2020
- Phishing attempts rose 600% since the end of February
- Ransomware attacks rose 148% in March
- Attacks targeting home workers rose five-fold in six weeks since lockdown

- 5% of coronavirus-related domains deemed suspicious
- Visits to hacker websites and forums rose 66% in March
- Average ransomware payment rose 33% to $111,605, compared to Q4 2019
- EventBot, identified in March, has targeted 200 banking and money transfer apps

Data source: https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know/
Image source: https://defensity.co.uk/coronavirus-scams-you-need-to-know-about-may-2020/

Contact us!

Critical Chains Website: https://research.reading.ac.uk/critical-chains/

Twitter: https://twitter.com/ChainsH2020

Austrian contact:

JOANNEUM RESEARCH - DIGITAL, Cyber Security and Defence Group

THE INNOVATION COMPANY

JOANNEUM RESEARCH DIGITAL

www.joanneum.at/digital