SoK: Cyber-Attack Taxonomy of Distributed Ledger- and Legacy Systems-based Financial Infrastructures

Ralph Ankele^{1[0000-0001-8751-9099]}, Kai Nahrgang², Branka Stojanovic^{2[0000-0003-4694-6187]}, and Atta Badii^{3[0000-0002-5130-152X]}

¹ Independent Researcher
 ² JOANNEUM RESEARCH Forschungsgesellschaft mbH, Graz, Austria
 ³ University of Reading, Reading, UK
 firstname.lastname@joanneum.at

Abstract. Nowadays, virtually all products and services offered by financial institutions are backed by technology. While the frontend banking services seem to be simple, the core-banking backend systems and architecture are complex and often based on legacy technologies. Customer-facing applications and services are evolving rapidly, yet they have data dependencies on core banking systems running on ancient technology standards.

While those legacy systems are preferred for their stability, reliability, availability, and security properties, in adapting the frontends and services many security and privacy issues can occur. Clearly, this issues are arising as those systems have been designed decades ago, without considering the enormous amounts of data that they are required to handle and also considering different threat scenarios. Moreover, the trend towards using new technologies such as Distributed Ledger Technologies (DLT) has also emerged in the financial sector. As the nodes in DLT systems are decentralized, additional security threats come to light.

The focus of this work is the security of financial technologies in the FinTech domain. We provide relevant categorization and taxonomies for a better understanding of the main cyber-attack types, and suitable countermeasures. Our findings are supported by using security-by-design principles for some selected critical financial use-cases, and include a detailed discussion of the resulting threats, attack vectors and security recommendations.

Keywords: DLT \cdot blockchain \cdot cyber-attack taxonomy \cdot FinTech \cdot threat modelling \cdot cyber-attack countermeasure

1 Introduction

Financial technologies (FinTech) and innovations that optimize the delivery of financial services are a quickly emerging industry. Simple examples are financial services such as mobile banking apps, services for borrowing and investing,

cryptocurrencies, data driven analytics, artificial intelligence, blockchain and robotic process automation. The main goal of FinTech is to make financial services more accessible to the general public, open new business opportunities, while also reducing the costs of manual labour. However, while financial technologies enable a broader access to financial services also additional challenges arise. Data security is a big issue, as clearly many hackers are interested in the sensitive financial data of customers and corporates. In the common legacy core-banking technologies often security is not considered a big issue, as the mainframes and servers are usually not connected with the outside world, and protected in secure data centres that are heavily guarded. However, new technologies such as distributed ledger technologies move the usually well protected systems out in the open by considering a decentralized approach.

This paper focuses on understanding and categorizing the different attack vectors for both legacy financial infrastructure, and distributed ledger financial infrastructures. Additionally, suitable countermeasures are proposed by considering relevant taxonomies. Moreover we use *security-by-design* principles, such as threat modelling and provide security recommendations according to the emerging threats. Although the literature contains several papers focusing on security in DLT [55] [62] [51] [59] [36] [56] [46], as well as many general distributed ledger and blockchain technology reviews[16] [68] [30] [65] [31], this paper, to the best of our knowledge, is the first one presenting both attack and countermeasures taxonomies, and supports its findings using threat modelling.

This remainder of the paper is structured as follows. Section 1 gives security focused introduction of DLT- and legacy systems-based financial infrastructures, with literature review. Section 2 presents legacy based financial infrastructures and their vulnerabilities. Section 3 describes most common DLT use-cases, and the advantages of this technology. Section 4 proposes a comprehensive taxonomy of specific cyber-attacks within this domain, while Section 5 proposes a list of potential countermeasures. Section 6 presents results of threat modelling for described use cases. Section 7 contains conclusions and future work directions.

2 Legacy Financial Infrastructures

Virtually all products and services offered by financial institutions are backed by technology. Even simple bank transactions or ATM withdrawals require the interplay of various different components, as financial infrastructures are complex systems that have often been built on monolithic architectures [67]. Legacy core banking systems at the hearth of financial infrastructures are still the main issues that hold back innovation efforts and cripple the agility of financial institutions. Many financial institutions are museums of technology dating back to the 1960's, where the complexity of those systems make it impossible to manage risks [33]. Typically the main challenges with these monolithic architectures is that customer-facing applications and services must evolve rapidly, yet they have data dependencies on core banking systems running on ancient technology standards. Indeed, the banking frontends are evolving quickly, however the backend systems of current banks heavily rely on legacy systems such as mainframes from the 1980's, COBOL based software systems from the 1960's, excel, batch systems and ATMs with Windows XP. The main reasons for using legacy systems are stability, reliability, availability, functional resiliency, security and an attitude of many banks to not fix a running system unless it is broken. Those systems have performed reliable over many years, but as they have become increasingly complex and are not designed to cope with rapidly changing technologies they cannot keep up the pace with new technologies such as distributed ledger technologies, cloud-based open digital ecosystems, artificial intelligence and micro service architectures.

2.1 Legacy Systems in Financial Infrastructures

In this section, we will give an overview of the main components used for in the backend of financial institutions as core banking components. These systems include *mainframes*, *software systems based on COBOL* and *Excel Sheets*. Moreover, we also mention customer-facing components such as *ATM's running outdated operating systems*.

Mainframes. Mainframes are computer systems that are usually used by large organizations for critical applications. They are compared to supercomputers, which are optimized for high performance computing, designed to ensure high reliability, security, high throughput and the ability for hot-swapping of hardware and offloading to separate computer systems. Mainframes are used in financial institutions as they are reliable, they offer availability around the clock, they are built with security in mind and they have huge analytical speed and allow high throughput. While mainframes have been also evolved with time, the often do not fit the nowadays needs of bank customers any more. The banks of today are processing huge amounts of data, and with initiatives as open banking they also provide APIs to core banking functions. These needs are currently better solved with cloud-based solutions that work as Software-as-a-Service and micro services [38]. Mainframes in this context are inflexible, expensive and simply out of date to cope with these quickly changing requirements.

COBOL Software Systems. Common business-oriented language (COBOL) is a computer programming language designed for business use that originated in the 1960's. In the finance sector, COBOL is widely used as in legacy applications that are deployed on mainframes, most often for batch and transaction processing. A recent study by Reuters in 2017 showed that for technology of major US banking systems still 43% of banking systems were built in COBOL, 80% of all in-person transactions used COBOL, and 95% of all ATM swipe transactions rely on COBOL. Until today there are still more than 220 billion lines of COBOL in use during the use of every day financial services [54]. While it seems that COBOL is still widely used in financial infrastructure, the problem is that the programming language is not taught at universities any more and it is hard to find developers as most of them already retired. COBOL programs are infamous for being monolithic and lack modularization. Moreover, it was impossible in older versions to restrict access to data so any procedure could modify any

data item. Furthermore, there were also compatibility issues, leading to many dialects that have been created. Current technologies are rapidly growing and the required software stack is constantly adapting and evolving with it. Often the programming languages are designed directly for these new technologies and architectures. COBOL simply cannot cope with this rapid growth and changing of technologies. Moreover, as of today most programming in COBOL is purely done to maintain existing applications [53].

Excel Sheets. Another tool that is widely used in the finance industry are huge Excel sheets. Those Excel sheets are used for accounting and financial services. Moreover, Excel is used as an analytical tool in the finance sector. However, Excel is prone to manipulation and also error-prone due to manual data entry, manual copy-and-paste, and formula errors that provide scope for perpetrators with criminal intent. A further huge issue is the inability to trace the user identity who deals with data and the lack of audit trails that make Excel a risky and manipulative tool.

ATM's running outdated operating systems. Automated Teller Machines (ATM) are widely used to dispense cash all over the world. An ATM consists of two main parts, a cabinet that contains the ATM computer, and a safe that contains the money. The computer usually runs an embedded version of Windows, and up until 2014 the vast majority of 95% was running Windows XP [29]. While Microsoft stopped support for Windows XP in 2014, still in 2020 there are plenty of ATM's still running on this legacy operating systems. However, as there is no continuous support also vulnerabilities are not patched any more, opening up plenty of security hole within ATMs [52]. The reason why ATM's haven't updated their operating systems vary from huge operational costs, as there are plenty of ATM's out there, but also a lack of alternatives as newer versions of Windows also do not offer long-term support.

3 Distributed Ledger-based Financial Infrastructures

A distributed ledger is a consensus of distributed, shared, and synchronized data that is spread across multiple different geographical locations, that is not maintained by a central party. The general idea of distributed ledgers traces back to a proposal by Haber and Stornetta [26] about how to practically validate the generation and modification of digital documents. In 2002, Mazieres and Shasha [39] extended the concept to protocols and data structures in a multi-user network. The groundwork for today's blockchain technologies was laid by Satoshi Nakamoto [44], when introducing Bitcoin in 2008. However, the concept of distributed ledger technologies further extends blockchain technologies that are primarily used for cryptocurrencies, such as bitcoin. While distributed ledger technologies are a disruptive technology, with many different use-cases and plenty of developers that try to create new solutions based on distributed ledger technologies and certain use-cases where different technologies are better. In the context of financial infrastructures, use-cases that can radically improve current technologies

and transform the current financial industry include global payments, insurance claim processing, trade finance, automated compliance and clearing and settlement.

3.1 Use-cases for Distributed Ledger Technologies in Financial Infrastructures

Global Payments. Settling payments between banks within a single country are already complicated and a time-consuming process. Banks usually have accounts for many other banks for interbank transactions. However, if there is no direct relationship between two banks, a central bank or several intermediary banks need to be involved. When considering cross-border payments, additional complications arise. These include reaching consensus in routing payments, performing currency conversions and operations under different regulatory compliance. Recent developments in using Distributed Ledger Technologies for global payments include Central Bank Digital Currencies (CBDC) [66]. These currencies share many similarities with current cryptocurrencies (e.g. Bitcoin, Ethereum), but they are issued by central banks. CBDC's can be denominated in an established currency and together with a monetary policy framework they would permit stability over time. Cross-border payments based on distributed ledger technologies, had been successfully been deployed by the Bank of Canada and the Monetary Authority of Singapore in May 2019 [1]. They demonstrated a Payment vs Payment settlement without the use of any intermediaries. The technical platform used were the DTL platforms Corda⁴ and Quorum⁵, and Hashed Time Lock Contracts (HTLC), a smart contract that returns funds if certain conditions are not met within a time frame.

Insurance Claim Processing. Insurance Claim processing is a slow and cumbersome process, as it includes many manual and laborious claim processing, fragmented data sources, intermediaries, it is also fraud-prone and often includes a complex liability assessment for reinsurance. Using Distributed Ledger Technologies in insurance claim processing can automated the claim processing, add transparency, and improve the efficiency. Basically, by using smart contracts, all associated parties in an insurance claim can initially access the policies and claim conditions. The policyholders will have active policies and different smart contracts with pre-determined claim conditions stored on them. When a customer then wants to raise a claim, he can upload additional documents supporting the claim. After an auditor verified the claim, the smart contract is automatically executed and the customer gets paid.

Trade Finance. Trade finance describes the gap between exporters that want to have a guarantee of payment before shipping any product, and importers that want to have a confirmation of shipment before any payment. Financial institutions currently support that process by offering letter of credits to importers that guarantees payment, while they also review financial agreements that allows exporters to ship their products. However, this process is very

⁴ https://www.corda.net/

⁵ https://www.goquorum.com/

ineffective, and causes many risks, as banks must do anti-money laundering checks (AML) for financials. Furthermore, fraud and non-transparency is a huge risk factor from importers that require several bank loans for financing. Using DLT's, the purchase agreement can be depicted in a smart contract that is automatically executed according to the terms of the agreement. Companies no longer need intermediary banks in that process, and auditors from financial authorities can easily do AML checks and due diligence. Finally, shipment times can be reduced, as payment can be reviewed and approved in real-time.

Automated Compliance. The financial sector is highly regulated, and compliance is important for financial institutions. These regulations include internal and external audits, reporting to appropriate financial regulatory authorities, tax reporting and customer due diligence. While this is often a manual process, spending on compliance reached a total of US\$32.1 billion globally, with a majority of US 23.4 billion spent on operational costs [3]. Using Distributed Ledger Technologies for audits, examiners can use DLT to access information for the audit, so bank personal doesn't need to collect data or deal with errors that results from failure in manual processes. After completing the audit process, auditors can store their report on the distributed ledger, making it available to the financial institution and other financial authorities. Another compliance process that financial institutions continuously have to take is customer due diligence, which includes know your customer (KYC) and Anti Money Laundering (AML). In current systems, this is often a manual process that each financial institution has to do. Using Distributed Ledger Technologies, a KYC and AML registry can be made and shared between various financial institutions [47]. This would accelerate the on-boarding process and reduce operational costs.

3.2 Advantages of Distributed Ledger Technologies over Legacy Financial Infrastructures

When reviewing the different use-cases of Distributed Ledger Technologies as outlined above, the following advantages over legacy financial infrastructures have become eminent. The advantages of distributed ledger technologies in the financial sector include among others, simplicity and efficiency, disruptive technology, transparency, trust in an untrusted setting, reduction of operational costs, less bureaucracy, and faster clearing and settlement enabling real-time money transfers. A more detailed study of advantages of distributed ledger technologies can be found at [25].

4 Cyber-Attack Taxonomy of Financial Infrastructures

This section gives an overview of threats for financial infrastructures. While we provide a detailed list of possible threats and attacks here, we want to stress that this list if by far not exhaustive, and adversaries often exploit several vulnerabilities in a combination during an attack. For a more comprehensive study, we have classified the threats into seven categories, *active cyber-attacks*, *physical attacks*, *unintentional damage*, *scam/fraud/spoofing*, *failure/malfunction/outage*, *legal*, and *targeted threats for distributed ledger technologies*.

4.1 Active Cyber-Attacks (AA)

Distributed Denial of Service (AA1). Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks on financial institutions are a major threat, as they target the availability of financial infrastructures and disrupt the service for other customers. In a Denial of Service attack, an adversary aims to make a computer or service unavailable to its intended users by interrupting the devices normal functioning. This is normally achieved by flooding the system with requests in an attempt to overload the system. In a Distributed Denial of Service attack, the incoming traffic originates from many distributed sources, such as a botnet, making it harder to stop the attack simply by blocking single sources. These attacks make banking websites and services unavailable resulting in revenue losses, reputation damage and a loss in customer confidence. While some attacks just result in slow response times and some customers not being able to access their online banking, targeted attacks might also serve as a diversion tactic from adversaries that compromise data or are committing more serious attacks.

Ransomware (AA2). Ransomware is a type of malware that adversaries use to either publish compromising data, or block access to data unless a ransom is paid. The attack normally works in two stages, where initially an user, or bank employee is tricked into executing or downloading a trojan that is disguised as a legitimate file. Next, parts of a system or data are encrypted making a user/bank employee unable to access the data/service. Often, attackers remain silent, letting the ransomware do its part, and wait until the victims pay the ransom via anonymous cryptocurrencies such as bitcoin. The effects of a ransomware attack complicate matters greatly for financial institutions without a proper protection, leading in chaotic and intense situations. Notable examples for large-scale ransomware attacks are *CryptoLocker* [37], *WannaCry* [10] and *Petya* [2].

Backdoors/Supply-Chain Attacks (AA3). Most of the financial institutions use a complex network of third-party vendors that support their financial infrastructures. This reaches from technology service providers (i.e. payment networks), utility providers (i.e. energy suppliers, internet service providers), hardware vendors (i.e. IT services) to organisations for data processing (i.e. advertising companies). All this endpoints can originate cyber-attacks or can be affected by cyber-attacks, and therefore require an efficient cybersecurity policy. Moreover, also possible backdoors in the software/services provided by any of the vendors originated by malicious parties or disgruntled employees can cause severe risks in the defence of a financial institution.

Insider Threats (AA4). Often cyber-attacks against financial infrastructures are regarded as third-party attacks. However, studies [28,57] have shown that in the finance sector the level of insider threats is as high as 58%, with 53%

inadvertent and 5% malicious attacks. These attacks does not necessarily have to originate from employees, but could as well be third-party vendors, contractors and freelancers, trusted business partners, or former employees. The consequences of insider threats can lead to disclosure of confidential customer data, fraud, monetary loss, loss of intellectual property, disruption of critical infrastructures and the undermining of customers trust. This makes it crucial to protect the financial infrastructures not only against outsider attacks, but also against attacks from inside a financial institution.

Web Application Attacks (AA5). Most banks are providing online services to the customers as it is more convenient, accessible 24/7, and reduces personal costs. However, most online banking applications contain critical vulnerabilities, and all financial institutions are at risk. Finance and banking web applications are at high risk due to the complexity and high amount of transactions every day. This can be between bank servers, mainframes, and different devices that a customer uses to access the banking services. The most common web application attacks against financial infrastructures include Cross-site scripting (XSS), SQL injections, malware, bots and web scraping, two-factor authentication flaws, sensitive data disclosure and information disclosure through error messages. The most common vulnerability, cross-site scripting, allows attacker to infect the devices of customers with malware. SQL injection attacks are critical vulnerabilities that allow attackers to obtain sensitive confidential data from a database. These vulnerabilities underline that every input from an user interface has to be carefully be sanitized and outlines that hackers use any information to attack a vulnerable system.

Zero-Day Exploits/Vulnerabilities/Attacks (AA6). A zero-day exploit is a vulnerability in a software that is either unknown or unaddressed by the vendor of the software. As long as the vulnerability is unaddressed or otherwise mitigated, hackers can exploit it to gain access to computer systems, or can affect and alter data of those systems. Hackers often trade zero-day exploits among themselves, or try to sell them to vendors or other interested parties for large amounts of money [41].

Watering-hole Attacks (AA7). Watering-hole attacks are a specific tactic of adversaries that carefully study the habits and systems that certain users use very often, and specifically target those systems with malware. In a financial infrastructure context, watering-hole attacks can target specifically bank employees, and plant malware on the most frequently used websites and web services that those employees are using [42]. An example for a watering-hole attack on several Polish banks happened in 2016, where malware was planted on the web servers of the Polish Financial Supervision Authority [4].

Advanced Persistent Attacks (AA8). Advanced Persistent Threats (APT) are targeted attacks on critical infrastructures, big companies, financial infrastructures, or other large institutions. In contrast to normal attacks from hackers, APT groups are often large organized groups that are often funded by states. These groups often use advanced attack techniques, and combine multiple methods, tools and techniques to compromise the target. Normally, they

give priority to a specific target, and do not randomly seek for financial gain. Moreover, a study by FireEye [23] shows that the number of days APT groups are undetected in a victims network varies between regions, with an average of 60 days in Americas, and 54 days in APAC and EMEA in 2019.

Carding (AA9). Carding is a form of credit card fraud, where an adversary uses stolen credit card information to charge prepaid cards or gift cards. The attack typically works by hackers gaining access to credit card information, either by installing skimming devices on ATM's, hacking an online store or payment provider, or even buying it in the dark web. The hackers then either buy prepaid cards or gift cards and sell them online. Another option, called *cloning*, is to add the credit card information onto a new credit cards. A specific target for carding are the United States, as it has a large market with credit cards, and compared to most of Europe just checks the magnetic stripe or employs chip and signature technology, rather than chip and PIN.

Hacking (AA10). Hacking originally refers to malicious adversaries that are able to subvert the security measurements that are in place for computer systems. Nowadays, however the focus of hackers has changed from hacking personal computers to cyber attacks on critical infrastructures [43]. In the context of financial infrastructures, often legacy systems are targeted that mostly are running for decades and are not designed in a secure way. This threat category includes all kind of security violations by malicious adversaries that either hack a financial institution or their customers, using malware, viruses, trojans, spyware, rootkits, bootkits, or any other common cyber attack vectors.

4.2 Physical Attacks (PA)

Attacks against ATM's (PA1). There are several attacks targeting both, the ATM's and the customers, respectively. Physical attacks against ATM's include *ram-raiding* [49] (i.e. driving with a truck against the ATM, or trying to rip the ATM from its fixture), using explosives (i.e. sealing the openings of an ATM and filling the vault with explosive gas) and drilling/cutting holes into the ATM. Another specific attack against ATM's is *jackpotting* [21], where criminals drill a small hole into the ATM and then disconnect the existing hard drive and connect a external hard drive using industrial endoscopes. Next, they force reboot the ATM with the external hard drive, and are then under control of the ATM, allowing them to dispense all the cash. Attacks targeting customers of ATM's are often carried out by installing skimming devices [34], that read out the magnetic stripe of debit/credit cards. These are often combined with small cameras, that observes the PIN code of the customers.

Bank Robbery (PA2). Bank robbery is a crime where money or other assets are stolen from a financial institution. This is often subject to a threat of violence against bank employees, and their customers. This threat basically includes robbery of bank branches, ATM's, and armoured vehicles. While today bank robberies are mainly happening digital with an estimated loss of \$US1.5 trillion in revenue in 2018 [40], there were 3033 reported bank robberies in the US [63]. Sabotage (PA3). Sabotage is a deliberate action with the aim to disrupt,

obstruct, subvert or destruct a system or effort. In the case of financial infrastructures, this can originate from disgruntled employees, rival business partners or online trolls. Sabotage of financial infrastructures may include badmouthing the financial institution online, tampering with the system or theft of intellectual property, and results in monetary loss, loss of intellectual property, slowdowns, and higher risks for other cyber-attacks.

Vandalism (PA4). Vandalism is a deliberate action with the aim to destruct or damage a physical property. In the case of financial infrastructures, this includes deliberate damages to ATM's or property of bank branches (e.g. buildings, cars). However, from a cyber aspect, this also includes propagating fake news to damage the reputation of a financial institution, malware, spyware and ransomware.

Theft (PA5). Theft can be defined as taking the property of another entity, without prior consent or permission of the rightful owner. In the context of financial infrastructures, this includes theft of devices, data, storage media, documents and intellectual property. Moreover, in the case of cyber-theft this also includes theft of passwords and credentials, personal identifiable information, and complete identities of customers.

4.3 Unintentional Damage (UD)

Unencrypted Data (UD1). The financial industry is among the most regulated in the world, with many strong data security requirements for banking and in financial infrastructures. Asides from personal identifiable information such as names, addresses, social security numbers, financial institutions are also dealing with transaction data, income, credit scores and other sensitive data. Unencrypted data at database level, or at application level is a huge threat.

Insecure Third Party Services (UD2). Organizations often depend heavily on third-party products and services as an integral part of business operation. However, if no preventive measures are taken insecure third-party services can pose a huge threat to a trusted system. For example allowing content in a trusted application from an untrusted third party server can affect the whole environment. If these risks are not mitigated, the consequences can be reputational damage, loss of data, intellectual property, sensitive information, and unauthorized access to systems/data.

Insecure Systems/Policies (UD3). Financial institutions use many different hardware components and software for their everyday use. Insecure systems and weak cyber security policies can be a major threat and facilitate cyber attacks on their systems. This category of threats includes weak password policies, no or insufficient employee awareness training, no access control restrictions (i.e. one employee has access to all customers), no incident response plans, no risk analysis, no detailed regularly security audits and insufficient logging and monitoring of both systems and employees.

Human Error (UD4). According to recent studies on successful security attacks, human error is represented as one of the major impact factors with

43% in cyber security incidents [58]. Many of the attacks are based on hackers that exploit human weaknesses in order to get access to sensitive information. This includes among other factors, lack of motivation, lack of awareness, risky behaviour of employees and inadequate use of technology.

Bad Security Audits (UD5). Regularly security audits are often required in financial institutions to maintain compliance with regulations and to protect the financial infrastructures from data breech. However, bad executed security audits and ignored findings can be a huge threat [6]. Often security auditors are seen as enemies and not granted access to all systems. Moreover, just relying on security audits can be not enough as attacks develop over time and often occur in several stages.

Cascading Effects due to subordinate Threats (UD6). Attacks on financial infrastructures are often part of a detailed attack strategy that follows several stages. Cyber Attacks often have cascading effects that can cause additional vulnerabilities and lead to even more attacks. For example DDoS attacks often stress a system until it overloads causing reboots and uncontrolled states of the system. Moreover, network or power outages often cause parts of a system to shut down or failures that can then be exploited in attacks.

4.4 Scam/Fraud/Spoofing (SF)

Bank fraud (SF1). There are several different types of bank fraud, including accounting fraud (i.e. companies that make up profits to cover actual losses and debt), forgery and alteration of cheques, cheque kiting (i.e. withdrawing money from cheques with insufficient funds), fraudulent loan applications (i.e. by providing wrong informations to obtain a loan), money laundering, or wire transfer frauds (i.e. forgery of transfers by insiders, or transfer of money from accounts with insufficient funds). A recent study [20] showed that bank fraud in the UK totalled to a financial loss of £844 million in 2018.

Scam (SF2). In a financial context, often advance-fee scam is used by promising a victim a large amount of money, gift, contract in return for a small up-front payment. Scam is often combined with social engineering, or other confidence tricks and typically targets online users by email or phone. Scammers often use irreversible money transfer services, such as Western Union, MoneyGram or Bitcoin which are untraceable and irreversible, so that when the victim becomes aware of the scam cannot reverse the transaction.

Spoofing (SF3). In information security, an adversary pretends to be someone else or identifies as another entity to gain an illegitimate advantage. Adversaries can use spoofing to obtain access credentials from customers or employees of banks or other service providers to illegitimate gain access to banking services, online banking, computer systems or networks. Possible strategies that adversaries exploit can be IP address spoofing (i.e. to gain network access), referrer spoofing (i.e. to redirect the victims to illegitimate websites), email address spoofing (i.e. for phishing attacks), caller id spoofing (i.e. to further scam) and geolocation spoofing (i.e. to circumvent systems that check locations).

Synthetic Fraud (SF4). Synthetic identity fraud is a new form of fraud, where criminals combine personal data obtained with identity theft or social engineering, with fake data to generate an entire new identity that is nearly impossible to trace. This normally works by obtaining a single piece of legitimate personal data, such as social security numbers or passport numbers, and then building a fake identity around it using random addresses, phone numbers, and other contact details. A study in the US estimates that in 2020 the loss of credit card fraud based on synthetic identity fraud reaches up to US\$ 1.2bn [12].

Social Engineering (SF5). In an information security context, social engineering is a deliberate psychological manipulation of a person to perform actions or release confidential information and can be used as an initial attempt to get access to a system. An adversary often relies on the following six principles of influence established by Cialdini [11]: reciprocity (i.e. exchanges of goods, with the expectation to return a favour), commitment and consistency (i.e. forcing people to commit to an idea), social proof (i.e. people do what they see other people doing), authority (i.e. posing as an entity with authority, e.g. CEO, police), liking (i.e. using what people are liking) and scarcity (i.e. limiting the time for an offer).

Identity Theft (SF6). In the context of financial infrastructures, an adversary aims to get an economic advantage by applying for credit cards and loans using another persons' identity, or by acquiring goods and services that have to be paid by the person with the stolen identity. There are many different ways that adversaries exploit to gain personal identifiable information and credentials from other persons. This includes buying information in the dark net, hacking computer networks and databases, exploiting public records in databases, social media, dumpster diving for letters and documents, skimming devices at ATM's, shoulder-surfing for credentials, pickpocketing/theft of passports or phishing and obtaining somebodies trust until private information is given.

4.5 Legal (L)

Regulations/Violation of Laws (L1). The finance sector is one of the highest regulated sectors, as it is also one of the quickest growing sector. There are many risks within the financial sector either to customers (i.e. lack of customer understanding, miss-selling of products, data privacy), companies (business model viability, governance, data handling) and risks to financial stability (system-wide vulnerabilities, crypto assets). While these regulations mainly focus on improving the security, safety and privacy of customers, it can be difficult to keep up with all regulations. Non-compliance and violation of regulations in the financial sector added up to penalties of US\$ 36 billion globally in 2019 [19]. These fines include violations of regulations, Markets in Financial Instruments Directive (MiFID) as well as data privacy regulations such as the Global Data Protection Regulations (GDPR).

Payment services directive (L2). The payment services directive 2

(PSD2) [13], also known as Directive (EU) 2015/2366 is a regulation with the purpose of improving the security, privacy of customers and to integrate a better connected European payments market. One of the key points of the PSD2 however, is also an initiative to promote the development of innovative online and mobile payments through open banking. However, with opening up API's for third-party developers to build applications and services around financial institutions also adds additional security and privacy risks.

4.6 Targeted Threats for Distributed Ledger Technologies (TD)

Sybil Attack (TD1). In a Sybil attack [15] an adversary can subvert the repudiation in a distributed ledger technology, by creating or controlling a large number of pseudonymous identities of a network/distributed ledger. This allows an adversary to disconnect a host node from the network, by just connecting it to nodes the attacker controls. Furthermore, an adversary then can refuse transactions of a host, that disconnects the host from the network, and enables double-spending attacks. Depending on the underlying distributed ledger technology, the consensus algorithm and the number of participants can increase the difficulty of the attack. For example, in a distributed ledger technology with Proof-of-Work or Proof-of-Stake as consensus algorithm an attacker needs to control 51% of the network for an successful Sybil attack.

Eclipse Attack (TD2). Eclipse Attacks [61] are closely related to Sybil Attacks. Compared to a Sybil attack, where an adversary creates a large number of different identities from a single node, in Eclipse attacks, a number of malicious nodes conspire to fool correct nodes into connecting with malicious nodes. While the overall goal in a Sybil attack is to control the whole network, the goal of a Eclipse Attack is to isolate and attack a specific user or node. A decentralized network does not let all nodes simultaneously connect to all other nodes in the network for efficiency reasons. Instead, a node can connect in i.e. Bitcoin networks to eight outgoing connections, and i.e. in Ethereum networks to 13 outgoing connections, respectively. If an adversary manages to isolate a node, by controlling all the outgoing connections of a node, the adversary can carry out a race attack [32].

Alternative history attack (TD3). Alternative history attacks, also called long-range attacks [24,14] in the literature, are an scenario where an adversary reverts the blockchain until the genesis block and creates a fork of the blockchain. The adversary then populates the new branch with a different history then the main chain and aims to overtake the main chain, forcing all participants to continue verifying transactions at the alternated branch.

Race Attacks (TD4). In a race attack [32], and adversary exploits traders and merchants that accept payments immediately by seeing an 0/unconfirmed status. However, the adversary executes a double-spending attack in the meantime. The attack works when the adversary is able to create two conflicting transactions. The first transaction is sent to the victim, who accepts the payment and sends the goods without waiting for confirmation. Additionally, the adversary sends a second transaction to the network, basically paying himself the same amount of

cryptocurrency. Eventually, the second conflicting transaction is mined into a block and accepted as genuine payment, making the first transaction invalid.

Finney & Vector76 Attack (TD5). In a Finney Attack [22], that is similar to a race attack, an adversary collaborates with an malicious miner. The attacker exploits, similar to a race attack, the fact that a trader or merchant accepts 0/unconfirmed transactions. While this time, the merchant waits some time to check if a double-spend attack happens and then transfers the goods, the collaborating malicious miner pre-mines an identical transaction in a block and invalidates the now second transaction. The combination of race attacks and the finney attack, is called *Vector76 attack* [64].

Block Withholding Attack (TD6). In a Block Withholding Attack [5,18], also called selfish mining in the literature, an adversary mines blocks in its own fork of the blockchain without releasing them for a certain time to the network. The adversary then publishes the blocks to the network, with the aim to revert the main chain and either disrupts the network by wasting resources while mining, or to gain the rewards for mining the blocks. A variation of the block withholding attack is the fork-after-withhold attack [35], where a malicious miner hides a winning block until another miner propagates a valid block. The malicious miner then releases the block to create an intentional fork, that yields equal or higher rewards then block withholding attacks.

Bribery Attack (TD7). Bribery Attacks [7], also often referred to as Short-Range Attacks in the literature, exploit the possibility of an adversary to rent mining capacity by bribing miners to work on its blocks or forks of the blockchain. This allows an adversary to add arbitrary transactions as valid, that are verified by dishonest nodes. Bribing the miners with an reward equal, or higher than the block reward gives the miners a high incentive to join. A special case of bribery attacks are $P + \epsilon$ attacks [8], where assuming that miners are perfectly rational the bribe of the attacker should go towards zero as accepting any bribe would be more profitable for miners than mining directly. This would then also make the malicious branch the main chain.

Loss of private keys (TD8). When using cryptocurrencies, wallets store a public and private key pair. While the public key is used as an address to send and receive currency from other participants, the private keys are used to sign on the public ledger, effectively to spend the associated cryptocurrency. Loosing access to the private key, or forgetting the passphrase that was used to derive the private key, basically declines an user to access the funds associated with the wallet. According to an analysis [9] around 30% of all Bitcoin are lost due to the loss of private keys.

Data Privacy (TD9). While cryptocurrencies are often hyped as being privacy preserving, there are several concerns regarding the data privacy in blockchains. Because blockchains for cryptocurrencies are often decentralized and public all transactions can be verified by any node, increasing the transparency. However, this also allows adversaries to trace public keys and addresses of specific users. Moreover, due to the decentralized nature there is often no party checking for attacks or malicious users. Furthermore, anti-money laundering laws

and regulations often require wallet providers to still check the identities of their customers, which when being hacked can leak the identity of a person.

5 Countermeasures

In this section, we list countermeasures that are applicable to the threats listed in Section 4. While a specific countermeasure might harden various other attacks, most of the countermeasures are a specify measure to counteract a single threat. These measures are derived often particularly in a setting, where no cross effects are taken into account. Therefore, we want to stress, that it is crucial to apply the principal of defence in depth[45,60,27], which has the aim to add multiple layers of security defences around a IT system to add redundancy if a particular countermeasure fails. Our proposed countermeasures are a mixture of physical, technical and administrative defences.

5.1 List of Countermeasures

In the following, we give a detailed list of common countermeasures implemented to protect critical infrastructures. Financial infrastructures are complex systems that are based on many different technologies throughout the whole software/hardware stack. While some of those systems are quite similar to infrastructures in other domains, there are some parts that need higher security levels and more detailed defence mechanisms. The following provides an non exhaustive list of measures to improve the security of financial infrastructures.

Firewalls (CM1). Firewalls are network security systems that monitors incoming and outgoing network traffic in a computer network based on security rules. Normally, firewalls are established as a barrier between a trusted internal system and an untrusted external system. The network filtering rules need to be updated regularly to adapt to changes in systems. The filtering can happen on several layers, the application layer, network layer or by filtering each network packet separately. Moreover, firewalls can either be placed at network barriers, or also directly on host computers that control all network traffic on each machine. Blacklisting vs Whitelisting (CM2). Blacklisting and whitelisting are approaches to help keeping infrastructures, networks and applications secure. Blacklisting means to accept most entities, but exclude particular ones that pose a threat to your system. Whitelisting means to block all entities, apart from a few explicitly allowed ones. Blacklisting makes the most sense in a public network, where we want all entities to access a system, but want to exclude malicious entities. Whitelisting makes sense in a private network, where we want to limit the access to certain parties. Often, also the possibility exists to use a hybrid approach of whitelisting and blacklisting.

Air Gap (CM3). An air gap is a network security measure with the goal to physically isolate computer systems from each other. Data can therefore only be exchanged by using a removable storage medium, such as external hard drives or use flash drives. Financial institutions often have air gapped systems for backups

and critical systems.

Intrusion Prevention Systems (CM4). Intrusion Prevention Systems (IPS) are systems used in network security, which continuously monitors network traffic in order to detect and, in the following, to prevent security incidents by taking actions. These actions include to notify the administrator, dropping malicious packets, blocking traffic from the source and to reset the malicious connection.

Intrusion Detection Systems (CM5). An Intrusion Detection System (IDS) is a network security detection technology, similar to the IPS. The system also continuously monitors network traffic, but only tries to detect security incidents. Any intrusion is then reported to the administrator or to a security information and event management (SIEM) system.

Honeypots (CM6). Honeypots are a computer security systems to detect and counteract attempts of adversaries to unauthorized access data. In this context, the aim of the honeypot is to redirect adversaries to attack a part of the system that seems legitimate, but is actually isolated, monitored and doesn't consist any real data.

Awareness Trainings (CM7). Awareness trainings aims to train employees with regards to IT security in order to prevent phishing and ransomware attacks. These trainings are an important concept in IT security, since the human factor in IT systems are considered to be the weakest link and therefore a common starting point for hackers.

Strong Password Policies (CM8). Strong password policies can be part of awareness trainings, as employees tend to use remember-able passwords, which mostly are to be considered as weak passwords. Strong password policies should therefore be enforced and follow expert recommendations like [48].

Multi-factor Authentication (CM9). Multi-factor authentication is an authentication method which grants an user only access, if the user can present at least two pieces of evidence to an authentication request. These pieces can be (1) knowledge - something the user knows, like a password; (2) possession - something the user has, like a hardware token; (3) inherence - something the user is, like a biometric fingerprint.

Monitoring (CM10). Monitoring can be referred to system monitoring as well as to network monitoring. It does not aim to detect attackers but moreover detects status of servers, their availability, uptime and response time. If a benchmark of a monitored host drops to a certain point, an administrator usually gets notified.

Know Your Customer (CM11). Know your customer, also referred to know your client (KYC) in financial services requires that professionals make an effort to verify the identity, suitability, and risks involved with maintaining a business relationship. The purpose of KYC is to ensure, that customers or entities involved in a business relationship, are anti-bribery compliant, and are actually who they claim to be. Banks, insurers, export creditors and other financial institutions are increasingly demanding that customers provide detailed due diligence information.

Physical Defences (CM12). Physical defence are countermeasures against

physical intruders. These defences can include fences, walls, doors, secure door locks, security guards, cameras and other surveillance equipment.

Encryption (CM13). Encryption is a cryptographically process to convert information into ciphertext using a secret key, so that only authorised people can decrypt and process the information again. Encryption should be in place for any sensitive data.

Role-based Access Control (CM14). Role-based Access Control (RBAC) restricts resources based on the role of a user. Hence, RBAC enforces that employees are only allowed to access necessary information they need to fulfil there work. As a result users with low privileges should not be able to access any sensitive information.

Penetration Testing (CM15). Penetration testing is a simulated and authorised cyber attack against company networks or systems. These tests are a realistic way to test implemented security measures and monitoring systems and can be performed in black box, white box and grey box tests. As penetration tester, in contrast to cyber criminals, are usually limited by their resources (e.g. time, money) a grey or white box approach is usually done when performing a penetration test.

Threat Modelling (CM16). Threat modelling is a theoretical modelling approach, which has the goal to identify potential threats based on the architecture of the given system. Conceptually different methodologies are used ranging from secure and agile application development to operative and business driven concepts. Threat modelling is especially useful when applied during the design phase, as it delivers a semiformal security assessment which identifies security issues and the most likely attack vectors.

Anomaly Detection (CM17). Anomaly detection is the process of identifying unexpected events or items in a data set. In network monitoring, an anomaly could be an unusual data stream that might occur during a cyber attack.

Input Sanitization and Output Encoding (CM18). Input sanitization and output encoding are best practices in software development, where each input is cleared from illegal characters (e.g. injection attempts) and the presented data is encoded probably. A faulty or missing implementation of those could lead to an unexpected behaviour of the system, or even to common attacks like SQL injections or Cross Site Scripting.

Antivirus Software (CM19). Antivirus software (AV software) solutions are used to detect, prevent and to remove malware. Most of modern solution also offers Browser extensions that detect malware when accessing malicious websites. This is especially useful for sensitive work like online banking.

Biometrics (CM20). Biometrics like fingerprints or iris detection can be used as an authentication method. As biometric scans are not fully secure, they are usually used as a part of a multi-factor authentication processes.

Demilitarized Zones (CM21). In network security, a demilitarized zone (DMZ) is a logical subnetwork that exposes an institutions services to an untrusted external network. The purpose of the DMZ is to add an additional layer of security, as any external host can only access hosts and services within

the DMZ. The rest of the private network of the institution is isolated behind a firewall.

Data-centric Security (CM22). Data-centric security focuses on the security of data, rather than the security of networks, servers or applications. While this approach does not make a lot of sense for financial institutions that provide a whole infrastructure themselves, it is especially interesting for all customer focused internet banks and challenger banks, that often rely on infrastructure from large service providers such as Amazon Web Services or Microsoft Azure.

Password Hashing (CM23). Cryptographic hash functions are one-way transformations into a hash. Such process should be irreversible and is thus used for sensitive information like passwords, before storing them into databases. It is however necessary to use state of the art algorithms, to be save from hash-collision and brute force attacks.

Logging and Auditing (CM24). Logging and auditing the logged information is another essential best practice in IT security. When it comes to logging, it is necessary to log any data that is needed when reconstructing incidents, but to not log sensitive data like user passwords or similar.

Virtual Private Networks (CM25). Virtual Private Networks (VPN) are used to extend a private network across an insecure public network, such as the Internet. This enables users to access computers, send and receive data and access applications that are running in the private network. To ensure security, the connection is established by an encrypted layered tunnelling protocol. In a financial setting, a VPN can be used to connect different branches with a centralized backend, or to connect ATM's with the private network of a bank.

Sandboxing (CM26). Sandboxing is the process of running software processes in containers separated from other software. This sandbox includes its own part of memory space and storage and is further limited to access other resources such as networking or reading/writing at other devices. The overall aim of sandboxing is to prevent that software vulnerabilities are spreading or that one process can affect another process. This means for example that a banking app on a mobile phone cannot be affected by any other malicious app on the same mobile phone.

Design-embedded legislation and standardisation compliance (CM27). Newly built systems should include compliance with relevant standardisation and legislation from the design phase. This includes (but is not limited to) regulations for Anti-Money Laundering (AML), Know Your Customer (KYC), global sanctions, Markets in Financial Instruments Directive (MiFID), data privacy regulations such as the Global Data Protection Regulations (GDPR) and the payment services directive 2 (PSD2), also known as Directive (EU) 2015/2366.

Validation Techniques (CM28). Validation techniques with either a centralized entity or a repudiation based scheme were entities can vouch for other entities can be used to efficiently counter Sybil attacks. Additionally, switching to Proof-of-Work schemes make Sybil attacks more expensive.

Controlling Connections (CM29). Nodes in a DLT can block incoming connections and just allow outgoing connections that are whitelisted by

19

other peers to counter Eclipse attacks, Race attacks and Finney/Vector76 attacks. Moreover, it is possible to allow only trusted miners when considering countermeasures for block withholding attacks. When using Proof-of-Stake (PoS) as consensus mechanism, also punishment by reducing the stake of miners can be used to counter bribery attacks.

Dedicated Rules (CM30). To counteract attacks such as alternative history attacks dedicated rules and policies must be taken into account. One example is to make use of the longest chain rule (i.e. the main chain is the one with the greatest number of blocks). Other countermeasures include using moving checkpoints [17].

Password Managers & External Wallets (CM31) The use of password managers or external providers for wallets can efficiently prevent the loss of private keys.

6 Threats & Threat Models for Financial Infrastructures

In this section, some examples of basic threat models in the banking industry are given. First, a threat model for an ATM transfer and a model for online banking including the SWIFT protocol for a bank-to-bank transaction are shown, then a model for data flows in DLT is given. In each section, a comparison between the standard STRIDE template and the extended template, which includes the domain specific threats presented in chapter 4 is shown.

6.1 ATM Threat Model

Fig. 1 illustrates an example threat model for an ATM. The user entity ordinary interacts with the ATM by inserting the banking card, entering the pin code as well as the desired options. Then, the ATM connects to the host computer, validating the request. The host computer then sends the request to the user's bank, which either accepts or declines the request. More details on the internal workings of an ATM can be found at [50]. Using the standard STRIDE template for modelling the DFD, the results contain a total of 48 cyber threats. However, adding the extended threat model results in a total of 127 cyber threats. This is an increase of 79 new and domain specific threats.

6.2 Online Banking Threat Model

Fig. 3 illustrates an example threat model for the online banking process. In the model, an user accesses his Bank A using online banking, starting a cash transfer to Bank B. Once bank has verified the user input, a connection to the central bank is established. The request is verified and sent to Bank B. The result can then be seen from both users. Using the standard template for the DFD results in 84 cyber threats within the STRIDE categories. When applying the extended template, the threats increasing to a total of 252 cyber threats.

6.3 Distributed Ledger Technologies Threat Model

Figure 2 illustrates an example threat model for typical data flows between system components of a Distributed Ledger System. In this scenario, an user (or node) communicates with the Distributed Ledger through one of three channels. The first one is a third-party organisations or exchange as in the case for cryptocurrencies. The second channel is the use of online web-based wallets with Multi-Signature authentication. The third channel is via distributed applications (dApps). Also for this threat model we applied the extended threat template to the threat model. The extension results in 262 threats, in comparison to the standard 74 STRIDE threats.

6.4 Security threats-countermeasures mapping

Table 4 presents mapping between threats and potential countermeasures that at least partially can answer specific threats, with stated threat category per STRIDE model, and risk factor. The presented threat models served as a basis for estimating category and risk factor of previously described threats (Table 4), within FinTech / distributed ledger domain.

7 Conclusions

This work outlines a detailed taxonomy of cyber-attacks for financial infrastructures. We aim to provide a better understanding of the main cyber-attack types, including a categorization according to the attack origin and give a prospect of what impact these threats have to relevant critical use-cases of financial services. Our hopes are that decision makers in financial institutions become more aware of the different threats by providing a detailed analysis of threats that we categorized in seven categories – active cyber-attacks, physical-attacks, unintentional damage, scam/fraud/spoofing, legal and targeted threats. In addition to cyber-attack taxonomy, a comprehensive list of suitable countermeasures is provided as well. Our analysis of cyber-attacks and threats for financial infrastructures is divided into two parts, legacy-based financial infrastructures and modern distributed ledger-based technologies that are targeted for FinTech applications. It is clearly evident that those legacy systems are not designed to be secure when the frontends are adapted to handle enormous amounts of data. Yet, we can also show that even with new technologies based on distributed ledger technologies some of the threats still remain, including new types of threats, and potentially significant consequences. The findings of our work are supported by using security-by-design principles for defined use-cases. Consequently, we provide detailed threat models of critical use-cases including ATM usage, online banking, and data flows in Distributed Ledger Technologies. Based on those findings, security recommendation of suitable countermeasures' types for specific attacks are provided, with a risk factor indicating the probability of attacks occurrence based on the direct output of

threat modelling process. Future research directions within project consortium include extending this taxonomy and threat models to privacy related threats and an extensive threat severity ranking methodology taking into account possible countermeasures. Moreover, it would be interesting to validate the detailed cyber-attack taxonomy using additional use-cases considering financial infrastructures and core-banking services.

7.1 Acknowledgements

This work was funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 833326, project CRITICAL-CHAINS. We gratefully thank all Critical-Chains partners engaged in collaborative research, and especially ERARGE and NETAS for their support and valuable advices. The security countermeasures that address the privacy and security concerns among transaction between two end nodes via a central authority (e.g. Bank A, Bank B and the Central bank) is derived from the Triangular Accountability Model proposed in Critical-Chains, a H2020 project with contract nr. 833326). In addition, the threat severity ranking methodology that addresses the privacy and security concerns, a part of a joint study within Critical-Chains consortium, is not included in this publication.

References

- Accenture: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies (2019), https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf
- Aidan, J.S., Verma, H.K., Awasthi, L.K.: Comprehensive survey on petya ransomware attack. In: 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS). pp. 122–125 (Dec 2017). https://doi.org/10.1109/ICNGCIS.2017.30
- 3. Arin Ray and Neil Katkov: IT and Operational Spending in AML-KYC: A Global Perspective (2019), https://www.celent.com/insights/900750380
- badcyber: Several polish banks hacked, information stolen by unknown attackers (2017), https://badcyber.com/several-polish-banks-hacked-informationstolen-by-unknown-attackers/
- Bag, S., Ruj, S., Sakurai, K.: Bitcoin block withholding attack: Analysis and mitigation. IEEE Transactions on Information Forensics and Security 12(8), 1967– 1978 (Aug 2017). https://doi.org/10.1109/TIFS.2016.2623588
- Böhme, R.: Security audits revisited. In: Keromytis, A.D. (ed.) Financial Cryptography and Data Security. pp. 129–147. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
- Bonneau, J.: Why buy when you can rent? In: Clark, J., Meiklejohn, S., Ryan, P.Y., Wallach, D., Brenner, M., Rohloff, K. (eds.) Financial Cryptography and Data Security. pp. 19–26. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
- Buterin, V.: The P + epsilon Attack (2015), https://blog.ethereum.org/2015/ 01/28/p-epsilon-attack/
- Chainanalysis Team: Bitcoin's \$30 billion sell-off (2018), https://blog. chainalysis.com/reports/money-supply

- 22 Ankele et al.
- Chen, Q., Bridges, R.A.: Automated behavioral analysis of malware: A case study of wannacry ransomware. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA). pp. 454–460 (Dec 2017). https://doi.org/10.1109/ICMLA.2017.0-119
- 11. Cialdini, R.: Influence : the psychology of persuasion (2007)
- 12. Conroy, J.: Synthetic identity fraud: The elephant in the room (2018), https: //www.aitegroup.com/report/synthetic-identity-fraud-elephant-room
- Council of European Union: DIRECTIVE (EU) 2015/2366 (2015), https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366
- Deirmentzoglou, E., Papakyriakopoulos, G., Patsakis, C.: A survey on longrange attacks for proof of stake protocols. IEEE Access 7, 28712–28725 (2019). https://doi.org/10.1109/ACCESS.2019.2901858
- Douceur, J.R.: The sybil attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds.) Peer-to-Peer Systems. pp. 251–260. Springer Berlin Heidelberg, Berlin, Heidelberg (2002)
- El Ioini, N., Pahl, C.: A review of distributed ledger technologies. In: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems". pp. 277–288. Springer (2018)
- Evangelos Deirmentzoglou: Rewriting History: A Brief Introduction to Long Range Attacks (2018), https://blog.positive.com/rewriting-historya-brief-introduction-to-long-range-attacks-54e473acdba9
- Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Commun. ACM 61(7), 95–102 (Jun 2018). https://doi.org/10.1145/3212998, https://doi. org/10.1145/3212998
- Fenergo: Aml, kyc & sanctions fines for global financial institutions top \$36 billion since financial crisis (2020), https://www.fenergo.com/news/aml-kyc-andsanctions-fines-for-global-financial-institutions-top-\$36-billionsince-financial-crisis.html
- 20. Finance, U.: Fraud the facts 2019 (2020), https://www.ukfinance.org.uk/system/ files/FraudTheFacts2019-FINALONLINE.pdf
- Finkle, J.: Atm makers warn of 'jackpotting' hacks on u.s. machines (2018), https://www.reuters.com/article/us-cyber-atms-usa/atm-makers-warn-ofjackpotting-hacks-on-u-s-machines-idUSKBN1FG0WU
- 22. Finney, H.: The finney attack (2011), https://bitcointalk.org/index.php? topic=3441.msg48384#msg48384
- FireEye: M-trends 2020 (2019), https://content.fireeye.com/m-trends/rpt-mtrends-2020
- 24. Gaži, P., Kiayias, A., Russell, A.: Stake-bleeding attacks on proof-of-stake blockchains. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 85–92 (June 2018). https://doi.org/10.1109/CVCBT.2018.00015
- Golosova, J., Romanovs, A.: The advantages and disadvantages of the blockchain technology. In: 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). pp. 1–6 (Nov 2018). https://doi.org/10.1109/AIEEE.2018.8592253
- 26. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. Journal of Cryptology **3**, 99–111 (1991)
- 27. Homeland Security: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies (2016), https: //www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

- 28. Insiders, C.: Insider threat 2018 report. Tech. rep., Cybersecurity Insiders (2018)
- 29. Jett Goldsmith: 95% of ATM machines still use Windows XP, and will be exposed to vulnerabilities after April 8 (2014), https://www.neowin.net/news/95-of-atmmachines-still-use-windows-xp-and-will-be-exposed-to-vulnerabilitiesafter-april-8/
- 30. Kadam, S.: Review of distributed ledgers: The technological advances behind cryptocurrency. In: International Conference Advances in Computer Technology and Management (ICACTM) (2018)
- Kannengießer, N., Lins, S., Dehling, T., Sunyaev, A.: Trade-offs between distributed ledger technology characteristics. ACM Computing Surveys (CSUR) 53(2), 1–37 (2020)
- Karame, G.O.: Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. In: In Proc. of Conference on Computer and Communication Security (2012)
- 33. Keith Pogson: Why banks can't delay upgrading core legacy banking platforms (2019), https://www.ey.com/en_gl/banking-capital-markets/why-banks-cant-delay-upgrading-core-legacy-banking-platforms
- 34. Krebs, B.: A dramatic rise in atm skimming attacks (2016), https:// krebsonsecurity.com/2016/04/a-dramatic-rise-in-atm-skimming-attacks/
- 35. Kwon, Y., Kim, D., Son, Y., Vasserman, E., Kim, Y.: Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p. 195–209. CCS '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3133956.3134019, https://doi.org/10.1145/3133956.3134019
- 36. Lamba, A., Singh, S., Balvinder, S., Dutta, N., Rela, S.: Mitigating iot security and privacy challenges using distributed ledger based blockchain (dl-bc) technology. International Journal For Technological Research In Engineering 4(8) (2017)
- 37. Liao, K., Zhao, Z., Doupe, A., Ahn, G.: Behind closed doors: measurement and analysis of cryptolocker ransoms in bitcoin. In: 2016 APWG Symposium on Electronic Crime Research (eCrime). pp. 1–13 (June 2016). https://doi.org/10.1109/ECRIME.2016.7487938
- 38. Manoj Kashyap and John Shipman and Haskell Garfinkel and Steve Davies and Dean Nicolacakis: Redrawing the lines:FinTech's growing influence on Financial Services (2017), https://www.pwc.com/jg/en/publications/pwcglobal-fintech-report-17.3.17-final.pdf
- Mazières, D., Shasha, D.: Building secure file systems out of byzantine storage. In: Proceedings of the Twenty-First Annual Symposium on Principles of Distributed Computing. p. 108–117. PODC '02, Association for Computing Machinery, New York, NY, USA (2002). https://doi.org/10.1145/571825.571840, https://doi.org/ 10.1145/571825.571840
- McGuire, M.: Into the web of profit (2018), https://www.bromium.com/wpcontent/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf
- Miller, C.: The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. In: In Sixth Workshop on the Economics of Information Security (2007)
- Mohammadi, A.K.: How watering hole attacks target the financial sector and government agencies (2019), https://securityboulevard.com/2019/03/howwatering-hole-attacks-target-the-financial-sector-and-governmentagencies/

- 24 Ankele et al.
- 43. Murphy, H.: Companies urged to bolster infrastructure cyber defences (2019), https://www.ft.com/content/797e1e5e-ca53-11e9-af46-b09e8bfe60c0
- 44. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf (2008)
- 45. National Security Agency: Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments. (2010), https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-indepth.cfm
- 46. Pandl, K.D., Thiebes, S., Schmidt-Kraepelin, M., Sunyaev, A.: On the convergence of artificial intelligence and distributed ledger technology: A scoping review and future research agenda. IEEE Access 8, 57075–57095 (2020)
- Parra-Moyano, J., Ross, O.: Kyc optimization using distributed ledger technology. SSRN Electronic Journal (01 2017). https://doi.org/10.2139/ssrn.2897788
- 48. Paul A. Grassi and James L. Fenton and Elaine M. Newton and Ray A. Perlner and Andrew R. Regenscheid and William E. Burr and Justin P. Richer and Naomi B. Lefkovitz and Jamie M. Danker and Yee-Yin Choong and Kristen K. Greene and Mary F. Theofanos: Digital Identity Guidelines: Authentication and Lifecycle Management (2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
- Peachey, K.: Surge in gas and ram-raid atm attacks (2018), https://www.bbc.com/ news/business-46468279
- Positive Technologies: ATM logic attacks: scenarios, 2018 (2018), https://www. ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/
- Putz, B., Pernul, G.: Trust factors and insider threats in permissioned distributed ledgers. In: Transactions on Large-Scale Data-and Knowledge-Centered Systems XLII, pp. 25–50. Springer (2019)
- 52. Rewterz Information Security: Outdated OS gets ATMs Hacked within minutes (2019), http://www.rewterz.com/uncategorized/outdated-os-getsatms-hacked-within-minutes
- Robert L. Mitchell: Cobol: Not Dead Yet (2006), https://www.computerworld. com/article/2554103/cobol--not-dead-yet.html
- 54. Robert L. Mitchell: Cobol: Not Dead Yet (2017), https://www.reuters.com/ article/us-usa-banks-cobol/banks-scramble-to-fix-old-systems-as-itcowboys-ride-into-sunset-idUSKBN17C0D8
- Salman, T., Zolanvari, M., Erbad, A., Jain, R., Samaka, M.: Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials 21(1), 858–880 (2018)
- 56. Sambana, B., Ramesh, Y., Rao, M.S.: Blockchain approach to cyber security vulnerabilities attacks and potential countermeasures. International Journal of Security and Its Applications 14(1), 1–14 (2020)
- 57. Security, I.: Ibm x-force threat intelligence index 2017. Tech. rep., IBM (2017)
- 58. Security, I.: Ibm x-force threat intelligence index 2019. Tech. rep., IBM (2019)
- Siddiqui, S.T., Ahmad, R., Shuaib, M., Alam, S.: Blockchain security threats, attacks and countermeasures. In: Ambient Communications and Computer Systems, pp. 51–62. Springer (2020)
- 60. Simon Woodside: Defence in Depth: The medieval castle approach to internet security (2016), https://medium.com/@sbwoodside/defence-in-depththe-medieval-castle-approach-to-internet-security-6c8225dec294
- Singh, A., Ngan, T., Druschel, P., Wallach, D.S.: Eclipse attacks on overlay networks: Threats and defenses. In: Proceedings IEEE INFOCOM 2006. 25TH

25

IEEE International Conference on Computer Communications. pp. 1–12 (April 2006). https://doi.org/10.1109/INFOCOM.2006.231

- Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.K.R.: A systematic literature review of blockchain cyber security. Digital Communications and Networks 6(2), 147–156 (2020)
- U.S. Department of Justice: Bank crime statistics 2018 (2018), https://www.fbi. gov/file-repository/bank-crime-statistics-2018.pdf
- 64. vector76: The Vector76 Attack (2011), https://bitcointalk.org/index.php? topic=36788.msg463391#msg463391
- 65. Westerlund, M., Kratzke, N.: Towards distributed clouds: A review about the evolution of centralized cloud computing, distributed ledger technologies, and a foresight on unifying opportunities and security implications. In: 2018 International Conference on High Performance Computing & Simulation (HPCS). pp. 655–663. IEEE (2018)
- 66. World Economic Forum: Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today? (2019), http://www3.weforum. org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf
- 67. Xavier Lhuer and Phil Tuddenham and Sandhosh Kumar and Brian Ledbetter: Next-generation core banking platforms: A golden ticket? (2019), https: //www.mckinsey.com/industries/financial-services/our-insights/bankingmatters/next-generation-core-banking-platforms-a-golden-ticket
- Zhu, Q., Loke, S.W., Trujillo-Rasua, R., Jiang, F., Xiang, Y.: Applications of distributed ledger technologies to the internet of things: A survey. ACM Computing Surveys (CSUR) 52(6), 1–34 (2019)

A Threat Models

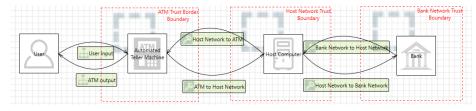


Fig. 1: ATM Threat Model

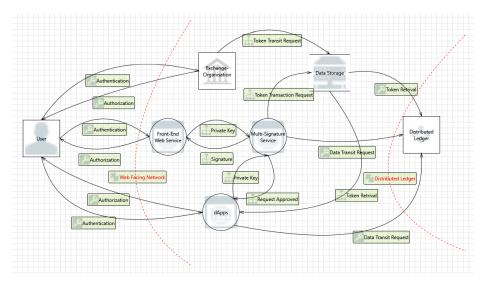


Fig. 2: Distributed Ledger Technologies Threat Model

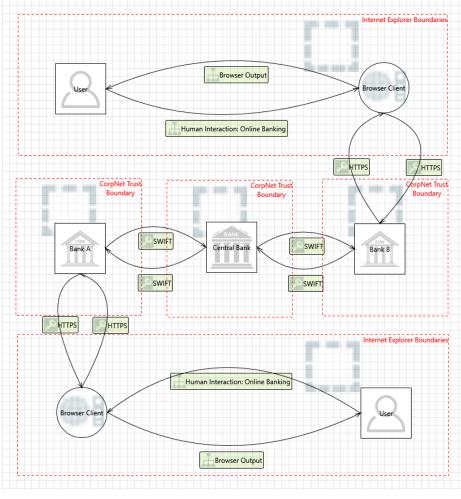


Fig. 3: Online Banking Threat Model

B Mapping of Threats and Countermeasures

Threat id	id (STRIDE) ^{Rusk Factor} CM1 [CM2 [CM3]CM4 [CM5]CM6 [CM7]CM8 [CM9]CM10 [CM11]CM12 [CM13]CM14 [CM15]CM16 [CM17]CM18 [CM19]CM20 [CM21]CM22 [CM23]CM24 [CM25]CM26 [CM27]CM28 [CM29]CM30 [CM31]															CM31																	
														Acta	ive Cyl	er Atta	icks (A.	A)					-			-							
AA5 AA6 AA7 AA8 AA9	$\begin{matrix} D \\ E \\ S, T, R, I, D, E \\ S, T, R, I, D, E \\ S, T, R, I, D, E \\ S \\ S, T, R, I, E \\ S, T, R, I \\ S, T, R, I \\ S, T, R, I, E \end{matrix}$	High Medium High High High High Medium High High High			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	× × × × × × ×	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	\$ \$	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	\$ \$ \$ \$	~ ~ ~ ~	$\begin{array}{c} \checkmark \\ \checkmark $		√ ✓ ✓	\$ \$ \$ \$		\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	\checkmark \checkmark \checkmark		V	√ ↓ ↓	√ √ √	√ √	~	√ √			✓ ✓ ✓					
	Physical Attacks (PA)																																
PA1 PA2 PA3 PA4 PA5	D T T, R, I, D D S, I, D	High Medium High Low Medium							۲ ۲	↓	✓	V		~ ~ ~ ~ ~			× × ×					✓											
	Unintentional Damage (UD)																																
UD1 UD2 UD3 UD4 UD5 UD6	$\begin{array}{c} {\rm S, T, I, E} \\ {\rm T, R, I, D, E} \\ {\rm S, T, I, E} \\ {\rm S, T, R, I, D, E} \\ {\rm R, I} \\ {\rm R, D} \end{array}$	Medium Medium High High Medium Low	\$ \$ \$	\$ \$ \$	\$ \$	× × × ×	~ ~ ~ ~ ~		~ ~ ~	× × × × ×	~ ~ ~ ~	\$ \$ \$		~	~	\$ \$ \$	\$ \$ \$	√ √ √	× × × × ×	\$ \$ \$	۲ ۲	\$ \$ \$ \$		√ √	\$ \$ \$		1	\$ \$ \$					
	Scam/Fraud/Spoofing (SF)																																
SF1 SF2 SF3 SF4 SF5 SF6	T, I S, T, R, I S S, T, I S S, R, I	Medium Medium High High Medium Low				~					~ ~ ~ ~ ~	\$ \$ \$ \$ \$ \$			~	۲ ۲	< < < < <<	\$ \$ \$	~			 		\$ \$ \$	\$ \$								
L1	R	High	1	1	1		1	1		1	1 1		1	1		egal (L	,		1		1	1		1	1	1	1	1		1	1		
L1 L2	R I	High High							 ✓ 																				↓ ✓				
												Targe	ted Thi	eats for	r Distr	ibuted .	Ledger	Techno	ologies ((TD)													
TD1 TD2 TD3 TD4 TD5 TD6 TD7 TD8 TD9	R T, R S, T T, R T, R T R D I	Low Low Medium Medium Medium High Medium							~	✓	~				V			√				V			V		~		~		~ ~ ~ ~	~	✓

Fig. 4: Security threats-countermeasures mapping

 $\mathbf{28}$

Ankele et al.