Perceptions of Distributed Ledger Technology Key Management – An Interview Study with Finance Professionals

Carolyn Guthoff*†, Simon Anell*†, Johann Hainzinger‡, Adrian Dabrowski*, Katharina Krombholz*
*CISPA Helmholtz Center for Information Security, Germany
{carolyn.guthoff, simon.anell, adrian.dabrowski, krombholz}@cispa.de
†Saarland University, Germany
‡Plutoneo Consulting GmbH, Germany, j.hainzinger@plutoneo.com

***Abstract*—Key management is an integral part of using distributed ledger technology (DLT). Previous work has primarily focused on key management for single-user scenarios on Bitcoin. Over the last decade, DLT has evolved to commercial and financial sectors; for example, a new German law allows the trading of a variety of financial securities via DLT. Instead of a single-user paradigm, financial institutions follow a multi-user paradigm. Combining multi-user key management with single-user key management solutions leads to unique challenges with usability and security.**

We extend current research through a two-stage qualitative interview study with 13 finance professionals. We investigate how the technical reality contrasts with perceptions of key management practices in corporate financial organizations. Our interdisciplinary study shows, among other things, that DLT does not meet real-world requirements in this particular domain. Moreover, it introduces additional challenges in terms of authentication and auditing.

Our findings suggest that corporate financial institutions strongly support the adoption of blockchain solutions. However, to comply with regulatory and operational requirements, they face additional usability and security challenges, e.g., authentication and access control. Better mechanisms or novel design approaches are required to cover professional environments. This includes how multiple users can access the same assets and approve joint transactions.

1. Introduction

Bitcoin's original goal was to provide *"electronic cash [that] would allow online payments [...] without going through a financial institution"* [37]. Consequently, the user model of Bitcoin and many other implementations of the distributed ledger technology (DLT) is based on a single self-managing user. This is reflected in the transaction design and key management (e.g., BIP32 [44]). Self-custodial wallets dominate the market and almost exclusively focus on the key storage aspect of key management (KM).

Unimpressed by the original goals, the financial sector discovered cryptocurrencies as an operational field, as well as the distributed ledger technology that these currencies are based on — including the blockchain. In 2021, German lawmakers allowed the electronic issuance of bearer bonds on central registers and DLT [6], [26]. And they changed the German Investment Code [4] to include the electronic issuance of investment funds on central registers [5]. Since 2022, investment funds may be issued on distributed ledgers [7]. This will change the way investment funds are traded. As a result we expect KM to become a fundamental part of investment funds trading.

Previous research has focused on different aspects of single-user usage. Mai et al. [36] looked at mental models of cryptocurrency systems, while Krombholz et al. [34] investigated user experiences focusing on security and privacy. Furthermore, Abramova et al. [8] looked into crypto-asset users' risk perceptions and security behaviors. Despite this and more research, there is no one-fits-all solution for KM in the single-user case. The amplified interest of the financial sector in DLT shifts KM challenges from a single user to multiple users with a higher trading volume. This challenges current KM solutions which are focused on single users. Overall, the challenges and requirements of professionally trading investment funds regarding KM are unknown.

This paper analyzes adoption obstacles for DLT key management within the financial sector, specifically investment funds trading and fintechs with a cryptocurrency context. We focus on this sector because it is highly regulated; hence, even stricter regulations apply here than in other sectors. Furthermore, it is non-trivial to embed new and adequate technologies within this context.

We recruited a total of 13 long-time professionals to explore the challenges of KM within the financial sector. Our participants all speak German. Most work in Germany, with a few in non-German jurisdictions. We focus on employees working at investment funds, fintechs, or crypto start-ups, as they have cryptocurrency experience. This way, we include the unique views and perspectives of employees working for more established and newer financial institutions.

Our methodology follows an iterative inductive approach, split into two stages. The first stage (A) focused on key storage in a hypothetical context of DLT-traded investment funds. It broadened our understanding of the problem space and lead to the following research questions.

RQ1 Within the financial sector, what DLT key manage-

2023 IEEE Symposium on Security and Privacy (SP) | 978-1-6654-9336-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/SP46215.2023.10335652

DOI 10.1109/SP46215.2023.00150

ment requirements do finance professionals have?

RQ2 Which security and secrecy requirements for DLT key management in financial applications do financial institutions have?

RQ3 Which attacker and threat types have an impact on DLT key management in financial institutions?

RQ4 What are the areas of tension between the requirements of finance professionals, security requirements, and the technical abilities of state-of-the-art DLT?

In the second stage (B), we took a more holistic view of KM for distributed ledgers within the financial sector, with a focus on Bitcoin. We chose Bitcoin since it is the best-known and most commonly used implementation of a cryptocurrency on a blockchain.

Our results show that participants concentrate on the use cases of several people (1) needing access to the same assets and (2) agreeing to transactions. Access management of distributed ledgers is a big issue in finance environments. Its implementation is non-trivial due to differing requirements across domains, such as usability and security and the established procedures and infrastructure.

The rest of this paper is organized as follows. Section 2 provides background knowledge on the financial sector and key management. Section 3 gives an overview of related work. Section 4 introduces our methodology while differentiating between stage A and stage B. In Section 5, we describe the results of our studies and answer the research questions. Section 6 puts our results into perspective and discusses possible future work

2. Background

2.1. Financial Sector

In order to have a common understanding of the goals of this paper, we describe some key terms related to the financial sector. Further background on current legislation around investment funds trading based on DLT is available in Appendix A.

- The **finance sector** is a big part of the global economy encompassing banking institutions, investment firms, insurance companies, fintechs, and several others [11], [32]. In this paper, we will focus on banking and investment firms as well as fintechs.
- A **finance professional/expert** has professional and/or technical expertise in a field related to the financial sector. For this paper, this includes both economics as well as computer science backgrounds.
- An **investment fund** invests the funds of its investors in a predefined way and gives out share certificates.
- A **financial application** is an application that enables the user to perform financial transactions within their specific work context.
- **Know-your-customer (KYC)** regulations require screening of new customers, possibly aided by technology-based background checks [22]. The goal is the prevention of money laundering and terrorism funding.
- The **four-eyes principle** is an internal control mechanism. It requires two persons to approve an action. This is a common practice to minimize risk and misuse [16].

Four actors are relevant to the immediate environment of KM in the financial sector:

- For the scope of this paper, the **financial institution** is the owner of any assets owned in cryptocurrencies. It is the legal entity that may commission an employee to perform tasks or enter and maintain a contractual relationship with an intermediary.
- An **employee** is a finance professional employed by the financial institution and is commissioned to perform tasks on its behalf. These tasks may include trading cryptocurrencies and thus using asset keys related to cryptocurrencies owned by the financial institution.
- An **intermediary** is a legal entity that can enter and maintain a contractual relationship with a financial institution. The financial institution may delegate or outsource certain tasks like KM to the intermediary.
- A **regulatory and oversight authority**, like BaFin in Germany (see Section 4.5) is responsible for the regulation of financial service providers, custodians, and other companies working within the financial sector. It can provide licenses for different areas of responsibility.

2.2. Key Management

An often neglected problem in the context of cryptography is key management (KM). It is the primary enabler of encryption in real-world applications. In cases such as secure transmission for web browsing with HTTPS, the industry found ways to make KM opaque to the user [23]. In other cases – like cryptocurrency trading – the end-user typically has more obligation regarding key handling – such as generation or custody. This section briefly covers the basic building blocks of KM and digital signatures that are needed for the rest of the paper.

A **digital signature** is a type of public-key cryptographic algorithm. It is used in Bitcoin to irrevocably tie transactions to a key pair. We will focus on KM for digital signatures. KM, as defined by Baker [12], describes "the activities involving the handling of cryptographic keys and other related key information during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, use, and destruction." It is important to stress that KM is a combination of different key-related aspects, including *key usage* and *storage*. The goal of KM is to generate, store, distribute, use, and revoke cryptographic keys (integrated into enterprise processes) while keeping the private key secret. KM is not necessarily equal to a (cryptocurrency) wallet, but a wallet may be used as a simple tool for KM.

2.2.1. Key Usage. For digitally signing a transaction, one or more private keys are required. This can be realized by using either a single key pair or multiple key pairs. In the case of multiple key pairs on Bitcoin, an m-of-n multisignature [9] is set up. All n public keys are tied to the asset, but only m private keys are needed to sign a transaction.

2.2.2. Key Storage. Key storage is a component of KM. We distinguish between hot and cold key storage [18] and non-custodial and custodial [8] options.

Cold key storage describes any kind of storage that is usually disconnected from the network. Examples include hardware wallets like a hardware security module (HSM) or keys printed on paper and stored in a secure location.

In contrast, **hot key storage** describes a key stored on a network-connected device, e.g., a file or software running on a desktop or server.

Abramova et al. [8] describe *custodial wallets* as "third-party services that take care of KM" [8]. For the purpose of this paper, a more thorough distinction between KM and key storage is necessary. Thus, we describe **custodial key storage** as the storage of keys by a separate party, which can be either in-house or a third entity that does not use the key. This party can, but does not have to, take care of all other aspects of KM. For self-managed assets, this could be a cryptocurrency exchange. For financial institutions, custodial key storage can be implemented in-house or externally by an intermediary.

Abromava et al. [8] write that "*non-custodial wallets* allow users to manage and control the key pairs directly" [8]. For **non-custodial key storage**, this translates to the user of the key being responsible for the storage location and medium. A storage location can be at home, at work, in a safe, or at any other physical location. A storage medium can be a file on a computer or server, a sheet of paper, or an HSM.

3. Related Work

This paper bridges the gap between financial corporate environments with their interest in cryptocurrencies, distributed ledger technology (DLT) and KM.

3.1. Key Management

The National Institute of Standards and Technology (NIST) published a comprehensive guide about different aspects of KM that is continuously updated [12]. The guide covers the entire life cycle of a key as well as different types of keys, explains how to best handle them in which scenario and gives extensive definitions.

KM with Coin Management Tools. A lot of research in the previous years has looked at different aspects of KM with coin management tools. Some of this research relates to usable security [8], [19], [24], [34], [36], [40], [41], while others look into vulnerabilities [14], [17], [31] or how to make existing wallets more secure [18].

Concerning usable security research, Krombholz et al. [34] first used the term Coin Management Tools (CMTs) to more adequately describe wallets. Eskandari et al. [19] looked at different wallet options for cryptographic keys used for cryptocurrencies with a focus on usability. Mai et al. [36] describe user mental models of cryptocurrencies with the example of Bitcoin. Fröhlich et al. [24] explore how users deal with KM challenges and how they choose aiding tools. Voskobojnikov et al. [40] look into risk perception of both cryptocurrency users and non-users. Voskobojnikov et al. [41] compare the user experience (UX) of five mobile currency wallets. They show that "users struggle with general and domain-specific UX issues that [...] might lead to dangerous errors and irreversible monetary loss" [41]

KM outside Cryptocurrencies. KM apart from CMTs is often hidden from end users in everyday life. Examples are secure web mail communication and secure web-browsing and end-to-end messenger encryption.

In 1999, Whitten and Tygar [42] published the first usability study with non-expert users on PGP 5.0, an encryption tool used for email security. They found numerous flaws in the user interface design related to security, and most participants could not successfully sign and encrypt emails. Six years later, Garfinkel et al. [25] analyzed different mail encryption standards. They proposed "simple modifications to web mail systems that would significantly increase integrity, privacy, and authorship guarantees [of these] systems" [25]. In 2016, Ruoti et al. [38] showed that newer PGP tools still had major adaption and usability flaws and discussed mitigation strategies. Herzberg and Leibowitz [30] also found usability issues with the end-to-end encryption features in instant messaging applications.

Moving from secure email and messaging to HTTPS, Krombholz et al. [35] found major usability challenges in the adaption and deployment of HTTPS. Their results "highlight that even educated users prefer solutions that are easy to use" [35] Two years later, Krombholz et al. [33] presented results that suggest that end users "underestimate the security benefits of HTTPS" because they do not understand integral parts of encryption and "ignore and distrust security indicators". Tiefenau et. al [39] found instances of well implemented applications for HTTPS deployment. In a comparative study between traditional configuration and the use of Let's Encrypt in combination with Certbot, they found that the later option is significantly more usable and effective. The authors attribute the positive results to the user-centered-design approach.

All these papers show that even decades after the first usability study on a KM tool for secure email, we still face major problems in areas where numerous technicalities are hidden from the end user. This is due to misunderstanding, underestimation and lack of education.

Furthermore, these papers focus on a one-to-one or one-to-many relationship between the individual user and a key. However, our results suggest that this use case does not find application in the financial sector for asset management with corporate users. Studying DLT users in both personal and business contexts will deepen our knowledge of DLT KM users, their attitudes and behaviors, which will also be applicable to other domains like digital notaries.

3.2. Distributed Ledger Technology (DLT)

Distributed Ledger Technologies (DLTs) describe geographically spread data storage methods that replicate their data through the use of a consensus mechanism.

Bellaj et al. [13] propose a "taxonomy-oriented framework for conceptualizing and examining DLTs". The most well-known class of DLTs is the blockchain. Wüst and Gervais [45] distinguish between *permissionless* and *permissioned blockchains*. *Permissionless blockchains* describe open and decentralized systems, where anyone can join and leave the network at any time. Bitcoin [37] and Ethereum [43] are the best-known implementations of this kind. In contrast, *permissioned blockchains* regulate access through a central entity. Hyperledger Fabric [10] and Corda [28] are two well-known implementations.

4. Methodology

This study was realized following an iterative inductive two-step approach. We conducted semi-structured interviews that were analyzed with different coding techniques. Our exploratory study is split into two stages, A and B. Stage A focuses specifically on key storage, whereas stage B aims to look at KM from a more holistic perspective. We use this labeling throughout the next sections to show how each stage influenced further data collection and analysis. After completing stage A we refined our general research topic into RQs and revised our interview guideline.

4.1. Study Design

We conducted a qualitative study with semi-structured interviews. The context of stage A centered around a hypothetical scenario of investment funds trading on DLT. This involves high-volume assets, both cryptocurrencies and other assets, traded within a highly volatile and strictly regulated environment. Investment funds trading on DLT is not yet widespread, since the legal basis in Germany was only introduced in June 2022 [7]. However, there is a strong interest to deploy working solutions of investment funds regulated on DLT. We were interested in exploring key storage options that would be feasible within these constraints from the perspective of a financial expert..

Thus, the interview guideline for stage A focused on key storage options within this context and was structured into five parts. The interview guideline is presented in Appendix B.1, Table 2. The first part included general questions on demographics like age, education, and current job title. Additionally, it introduced the context described above. Parts two to five dealt with different storage options. We looked at hot and cold storage (group 1) and custodial and non-custodial storage (group 2). We asked the same questions for each storage option and additional comparison questions for each group. The questions covered benefits and drawbacks, a relation to the work environment and security considerations. Finally, we asked for a general preference.

After careful consideration of the collected data in stage A, we changed our interview guideline for stage B. We shifted the focus from using distributed ledgers for trading investment funds to high-volume cryptocurrency trading within the financial sector. This change allowed us to maintain the focus within the environment from stage A while being able to ask more tangible questions. We also broadened the exploration space from key storage options to KM at large. This was necessary because a holistic approach to KM in financial institutions will need to link requirements between all parts.

The complete interview guideline for stage B is available in Appendix B.2 in Table 3. This interview guideline is split into five parts.

Part one aimed to establish a connection with the participant. We included two questions about experience with cryptocurrencies and the cryptographic part of cryptocurrencies from Mai et al. [36]. We specifically picked these questions to better understand our participants' knowledge on cryptography.

Part two sought to assess mental models of blockchains. This part followed the methodological approach from Mai et al. [36] who incorporated a drawing task for buying Bitcoin in a private environment in their interview guideline. We adapted this context to a business environment to fit our study and asked follow-up questions about security risks and digital signatures. Consequently, we also chose to use Bitcoin as an example since it is the most widespread and best-known cryptocurrency. We added this part to gain a deeper knowledge of the participants' cryptographic understanding.

The third part focused on key storage. We asked about the perfect storage method within the context of a business environment as well as security risks and personal preferences with a focus on key usage. This was followed by a shortened version of parts two to five of the interview guideline of stage A with questions about different storage options and their comparison. This part was added because key storage is an elementary part of KM.

Part four looked at requirements for a platform that would handle both KM and cryptocurrency transactions. Questions in this part covered preferences for KM and requirements for the platform. We added this part because of an inclination towards custodial key storage during stage A.

The interview guideline ends with part five that gave room for questions, further comments, and a thank you.

4.2. Recruitment and Participants

For both stages A and B, we recruited 13 participants from different parts of the financial sector. Some have experience in investment banking, traditional banking, or consulting, while others gained their experience working for fintech or crypto startups. All of them either work with investment funds or cryptocurrencies. Most of our participants work in Germany with a few under other jurisdictions. Nonetheless, all interviewees were German native speakers and were interviewed in German. For recruitment, we used personal contacts for stage A as a starting point to gain first insights on the topic. For stage B, we utilized these business contacts for snowballing to gain a more holistic view of the topic. Our recruitment criteria was that participants either work with investment funds or cryptocurrencies.

The recruitment included basic information about the study. For stage A, we asked for oral consent and basic

TABLE 1. DEMOGRAPHICS FOR STUDY A AND STUDY B

Label	Age	Gender	Highest level of completed education	Current job title	Employment Jurisdiction
A1	25-29	f	Master (or similar)	Consultant	Germany
A2	35-39	m	Bachelor (or similar)	Head of Digital Hub	Germany
A3	40-44	m	Apprenticeship	CEO	Germany
A4	50-54	m	Master (or similar)	CEO	Germany
B1	25-29	m	Ph.D.	Lecturer, Researcher	Germany, UK
B2	44-49	m	Ph.D.	Co-founder, Investor	Costa Rica
B3	35-39	f	Master (or similar)	Senior Director	Germany
B4	40-44	m	Master (or similar)	Head of Fund in Fund Operations	Germany
B5	55-59	m	Bachelor (or similar)	Consultant	Luxembourg
B6	40-44	m	Apprenticeship	Consultant	Germany
B7	45-49	m	Apprenticeship	Business Development Manager Private Equity and Real Estate Funds	Germany
B8	40-44	m	Master (or similar)	Director	Germany
B9	45-49	m	Apprenticeship	Business Expert	Germany

demographics at the start of each interview. For stage B, we sent out one-pagers with general information about the study. We asked participants to fill out a questionnaire containing a consent sheet for the interview and some basic demographic questions. See Table 1 for demographics for all participants.

All participants were either offered a 25 Euro Amazon voucher to appreciate their time commitment, which we estimated to be around 60 min, or the interview was counted as paid work time. Each interview lasted between 45 to 90 min and was conducted in the summer and fall of 2021.

We recruited participants and conducted interviews until saturation was reached. We determined that we reached saturation because we could not find any new themes anymore.

4.3. Data Collection

All interviews were conducted via Zoom, with video and/or audio recordings, depending on the interviewee's preference. During stage B, we collected drawings via the built-in whiteboard feature. In four cases, using the whiteboard feature was not possible for the participants. We reverted to oral descriptions instead. All data was complemented with hand-written notes by the interviewer during and after each interview.

4.4. Data Analysis

All audio data was transcribed and analyzed in its original language German. We applied the following open coding procedure: Two researchers coded one interview and all collected supplementary material independently. They then met to discuss and resolve conflicts and built a first version of the codebook. This process was repeated for all stage B interviews with continuous updates to the codebook if necessary. A few conflicts arose because coders had different perspectives on the same core topic. E.g. for the quotation "*For example, if a person has a separate app or access device to legitimize the transactions, it doesn't matter whether it's a cell phone or another token device.*" [B8], one coded 'B04.01 key usage::access', which described access to the key, and the other one coded 'B05.01 platform::access', which describes access to the platform. From the quotation and the context, it is not clear whether the quote is solely about access to the platform or also includes key usage. In these cases we decided to code both. We also purposefully chose not to combine these two codes, because sometimes 'access' was only mentioned within the context of 'key usage'. Throughout each discussion, we extended and updated the codebook accordingly. This process was repeated for all interviews until all conflicts were resolved. The final codebook is available in the Appendix B.2 in Table 5.

After coding all interviews, we discussed which first-level codes best answered which RQs. We split up all first-level codes according to RQs between the two researchers. They each applied a combination of axial coding and selective coding to the data in order to best answer the RQs. They discussed their results several times with each other. This approach worked best for our first three RQs. The results are described in Sections 5.1, 5.2 and 5.3, respectively. For RQ4, the two researchers discussed areas of tension with a third researcher. These results are reported in Section 5.4. Afterwards, one researcher coded all interviews from stage A independently to check for saturation (see Section B.1 Table 4 for the codebook). We did not find any new themes and thus did not recruit for a third stage.

4.5. Regional Specifics

The main regional focus of our interviews was Germany. However, some of our participants have experience working with or for international financial institutions whose headquaters may be in other countries. This may have influenced their answers.

When talking about current processes within financial institutions and any legal regulations, the German *Federal Financial Supervisory Authority* (BaFin) was mentioned several times. BaFin is responsible for "the supervision of banks and financial services providers, insurance undertakings and securities trading" [21] within Germany.

4.6. Ethical Considerations

We carefully weighed the benefits and risks of interviewing finance professionals about their work environment and made sure to protect their privacy. For this reason, we only report their age group, gender, their highest level of completed education, their current job title, their years of experience in the financial sector and their employment jurisdiction.

Additionally, this study was approved by the Ethical Research Board (ERB) of the computer science and math department at Saarland University.

4.7. Limitations

Our study lays important foundations towards understanding KM considerations of finance professionals. We

specifically recruited people with a background in investment funds or cryptocurrencies in finance, which is a narrow and hard-to-reach population. We therefore chose to recruit via business contacts and snowball sampling. Our qualitative study is of exploratory nature, which implies that we cannot generalize from our sample. Hence, the foundational results of this work can be used to construct a theory. This theory can be used to develop concrete statistical hypotheses that can be evaluated through a quantitative follow-up study.

Furthermore, our participants are not commissioned within their jobs to trade cryptocurrencies for their employers. We thus only report on their thoughts about how this could be done, but not on their experience.

As the participant composition leans towards German jurisdiction, we may have missed some themes otherwise present in a more international mix.

5. Results

The results are structured by our RQs. We start with finance and security requirements before we discuss attacker and threat types. Finally, we examine areas of tension between the mentioned requirements and state-of-the-art DLT. Quotes are translated to English and attributed to a specific participant (Table 1).

5.1. RQ1 - Finance Requirements

RQ1 Within the financial sector, what DLT key management requirements do finance professionals have?

Requirements within the financial sector for DLT KM cover topics on key usage, key storage, usability, trust, and requirements a financial institution and, if present, an intermediary has to fulfill.

Key usage requirements mostly relate to access. Participants wished for a hierarchical access model and the possibility of changes in access rights. Additionally, more than one person should be able to approve a transaction, and keys should be, whenever possible, invisible to the user.

Requirements for key storage highly depend on the size of the financial institution, its preference, and the level of expertise of its employees. All participants mentioned benefits and drawbacks of all types of key storage. Only non-custodial key storage was consistently described as infeasible for regulatory and liability reasons. We also assembled a list of general areas of importance for key storage.

Usability requirements cover handling, knowledge levels of employees, and a balance between security and usability.

Trust itself is a requirement that can be established between different parties. These parties are the financial institution, employees, and, if present, an intermediary.

An intermediary is not a necessity for successful KM. However, in a corporate finance environment, delegation of KM or parts thereof is a feasible option. Both an intermediary and a financial institution need to fulfill some general and legal requirements. Furthermoer, participants mentioned benefits and drawbacks of using an intermediary.

The following subsections cover the requirements separated by topic in more detail.

5.1.1. Key Usage. Participants mentioned that several employees needed access to the same assets. They talked about models of key access rights that are similar to their institutions' organizational structure and how changes in access rights can be executed. They also brought up the need to have more than one person authorize transactions and the possible utilization of multisignatures for this use case. Furthermore, participants discussed the level of invisibility of the key to the user.

Access Rights - Hierarchical Access Models. Several participants described KM models that mirror a hierarchy present in their company. They link familiar structures from their daily professional lives with a potential representation of these structures in key usage: Supervisors or CEOs, depending on the size of the financial institution, have more power and responsibility in a company and thus should be entrusted with more powerful keys. These keys could, in contrast to inferior keys, enable transactions of a higher volume or be used to derive traceable sub-keys. A system that requires several specific people to authorize big transactions can also enhance traceability. "*This private key [would] contain the information, e.g., you may transfer Bitcoin on your own up to the amount of 100. Everything exceeding this is automatically transferred to the supervisor for approval via a second signature.*" [B9]

Changes in Access Rights. Participants comprehended that access to a private key is not revocable. If an employee had access to a key at some point, they might have copied it. The key stays valid for the corresponding asset even if an employee leaves the company. Thus, a change in permission results in complex or costly adjustments. These include key generation, key distribution, and the shift of assets to the new key(s). A shift of assets (i.e., a blockchain transaction) incurs transaction costs, but this was not mentioned by any participant. "*Keys are persistent information. If you have it once [...] the key remains valid forever. When you want to do it correctly, you need to set up a whole new multisignature with the [updated] group of authorized users.*" [B2]

There are many "*trigger events*" [B2] that entail updates of the key(s). These include day-to-day operations such as employees leaving, joining, being on vacation, or shifting responsibilities within the organization. Incidents such as key loss, key compromise, death and illness of employees, or force majeure events also entail updates. "*The employer needs to have the processes prepared, e.g., a leaving employee. [...] in a different system, you would simply remove access [rights], but this does not work on many multisig[natures] that way.*" [B1]

Multisignature - jointly approved transactions. Participants mentioned the concept of executing a transaction only if multiple individuals approve it. This concept can be implemented through multisignatures on the blockchain or with CMTs. Some participants referred to this concept directly. Other participants outlined a model where two or more employees are required to authorize a transaction, sometimes referring to it as "*four-eyes principle.*"

The two main benefits of this technique were resilience against key loss or compromise and added protection against

malicious employees. Depending on the variant of the multisignature setup, loss or compromise of a small number of keys does not result in the loss of assets. The assets can be transferred to a new multisignature, which entails new key generation and key distribution. In order to be safe, this has to be done as soon as a threat has been detected. Some participants also proposed storage of keys at a bank or a notary as a backup option. For protection against malicious employees, the threat of a single fraudulent employee is mitigated since no individual can act on their own.

Invisible Key Usage. Participants preferred a solution where key usage is mostly encapsulated within an application and hidden away from the user. In this case, participants mentioned the risk of losing a key through an attack or intended malicious actions by an employee. Usage of the key can be enabled through access via personal credentials like username and password or multifactor authentication, using a phone or biometric features. According to our participants, a credential-based system can mitigate some but not all threats. Loss or intended malicious actions by an employee might still be possible. However, this risk is also present in traditional trading settings.

5.1.2. Storage. Participants talked about all previously mentioned storage options and voiced their preferences for the use case of several employees needing access to the same assets. They mentioned benefits and drawbacks as well as option-specific requirements. They also pointed out general requirements regardless of the chosen storage option. The final decision on a storage option depends heavily on the use case. The following requirements were collected within the context of trading high sums for one's employer.

Cold Key Storage. Participants had divergent opinions about this storage option and its use in the financial sector. If cold key storage seemed a feasible option, it was usually mentioned in a combination with hot storage. Participants often listed many possible storage mediums and locations. Storage mediums included common ones like HSMs, paper, CDs, and some rather uncommon ones like stones and tattoos. Storage locations consisted of places like a home or an office, and mediums like a safe or a safety deposit at a bank or a notary. Some of these mediums and locations were labeled as more accessible than others, e.g., storing a key with a notary was a very inaccessible option and usually preferred as a backup method.

Benefits of cold key storage included no permanent connection to the internet, making theft more difficult, and that remote access was not possible. It was also labeled as a good key storage choice for backups. Drawbacks are that availability might be a problem, control by the financial institution is complicated, the usability is poor, and – if hardware devices are used – it is necessary to trust the hardware product.

Hot Key Storage. B7 described hot key storage as "*information technology, data-based, and can be addressed externally*" [B7]. Apart from this, participants mentioned that this option needed further security mechanisms. These included access precautions like passwords, multi-factor authentication, and TANs (transaction authentication number) or limitations on external access through VPNs only. Furthermore, if stored hot, the key should be encrypted. Whether hot key storage was an option depended highly on the used storage medium. Publicly accessible clouds were a no-go, whereas integration into already available banking applications was an option. In this case people also preferred invisible key storage. See Section 5.1.1 for a broader discussion on invisible key usage.

Benefits of hot key storage range from easy access and availability for employees to usability and possibly remote access control. B6 associated this option with "*no hardware problems*", while B8 said it mitigated "*risk of loss*". Drawbacks included maintenance complexity and the use of software-only security.

Custodial Key Storage. Custodial key storage has overlapping areas with hot key storage and was often equated with storage through an intermediary. "*I need an intermediary in between [the financial institution and the trading platform], who will handle [key storage].*" [B6]

Participants explicitly mentioned regulation for this storage option and the possibility of user support, if required. B7 said that it would be "*more complicated to steal [the key], if it was centrally stored*". In contrast, B1 pointed out that "*there should be no central component in the system, in the software, that can authorize [transactions].*" Overall, it was suggested that security mechanisms such as decentralized authorization implemented through technological safeguards should be put in place and that users should be legitimized.

Mentioned benefits include availability, easy usability, and the deferral of responsibility. Drawbacks include complex maintenance, risk of threats, and security that was only achieved through software means. If an intermediary is present, they also include cost, loss of speed, and possible mistrust.

Non-custodial Key Storage. Participants referred to this storage method as "*the wild west*" [B6] and said that "*there is no way this would work in practice*" [B3]. Adoption of this storage method heavily depends on the size of the company and the type of institution. For established financial institutions that trade high amounts of money, this is not a feasible option. Reasons range from not enough regulation and clear guidelines to maintenance issues, especially in the case of trigger events, see Section 5.1.1.

Benefits include flexibility and control through the employee. Drawbacks mention that this is not a suitable option for most users. They would need to put more effort into this storage method. Nonetheless, the financial institution would have no control, and the risk of threats would be higher. This could lead to liability issues for the employee. Participants also mentioned that a lot of knowledge was needed for the adequate use of non-custodial storage.

General Requirements. General requirements for key storage cover some of the topics that were already mentioned for specific key storage options.

Participants value usability. They point out that it is not necessary to see key storage or know how user access of the key through a software is handled. B2 mentioned a simple

"*click and sign*" function as a possible solution, while others strive for integration and compatibility with existing finance applications.

Concerning availability, participants stated that access for others in case of trigger events, see Section 5.1.1, is a must. The recoverabilty of keys and accordingly the access to assets was also considered important. Backups were mentioned several times as a requirement, although it was assumed for hot and custodial key storage.

Participants also mentioned compliance, regulation, and risk mitigation efforts. Regulation on what employees were permitted and prohibited to do was important, specifically for liability reasons. Employees have to sign contracts stating that they will follow policies and guidelines in order to gain their employer's trust. For the employer, it is crucial to have audit mechanisms in place to verify compliance with regulations and guidelines.

Two participants mentioned the need for decentralized key storage. Others desired additional security layers, especially when accessing keys. Overall, , no matter which key storage option is used, implementation quality is important.

Preferences.

- Most participants preferred a combination of hot and custodial key storage. This approach shifts responsibility for the secrecy of keys from the employee to the custodian. This is regardless of whether KM is handled by the financial institution itself or a third-party intermediary. Benefits include easier tracking of keys and changing of access rights. One participant identified the economic trade-off for companies of either handling key storage themselves or delegating it. Both have their individual advantages. However, two participants also mentioned that KM should not be handled by one central component but should be done in a decentralized way.. While decentralization and hot and custodial key storage are not necessarily conflicting options, a solution combining both will be complicated to realize.
- Most participants think that in a company setting, employees should not have direct access to private keys. They mention the concept of abstraction of the transaction process. For users, keys should be invisible and incorporated within a dedicated signing process hidden behind an easy to understand user interface (UI). "*The user might only have the task of managing these Bitcoin. But the user doesn't need to know how this works in the background. I don't need to know how a banknote is printed, just because I have it in my wallet.*" [B9]
- Preference also depends on the size of the financial institution. Some participants mentioned that bigger institutions can decide to outsource the storage and management of keys to verified, regulated external providers. However, smaller institutions may adapt faster to process changes and new technologies.

5.1.3. Usability. Participants mentioned several issues regarding the usability of KM solutions. They discussed two approaches for systems that target employees and trade-offs between usability features and security.

Handling. Participants generally found KM systems difficult to use. They wish to have usable, flexible, and easily accessible solutions. End users should not need to know how digital signatures work on a theoretical level to use cryptocurrencies [B2]. Participants complained that both currently available and formerly used KM solutions did not fulfill these requirements. "*[The participant is talking about their own first personal experience with Bitcoin.] The hurdles were pretty high back then [for using cryptocurrencies]. So I can understand that some people gave up completely unnerved. I was also completely unnerved. I think I wasted far too much time [on the setup and execution of the first transaction*" [B3]

Knowledge. Participants advocate that no background knowledge should be necessary to use keys. However, in a company environment, employees should have a certain basic knowledge about KM and the consequences of misuse and incidents. Strategies include education and training as well as specific lessons about security issues on topics like handling keys and basic security.

Employee-Targeted Systems. We found two different ideas on how employee-targeted systems should look like: a password-credential-based application and a system that requires direct use of keys by employees.

- A password-credential-based application is perceived as an easy and fast way of performing transactions without an additional KM tool. The actual key is stored and managed by the provider of the application, either the company or an intermediary, and is not accessible to the users. As users use personalized credentials, necessary information is available to link transactions to authorizing personal.

  The advantages include good accessibility, support, and that DLT keys are not handed out to users. Participants also mentioned this kind of solution to be more similar to traditional banking settings.
- The second approach lets employees directly use DLT keys. However, this solution requires more technical skills and background knowledge. It can be faster and more flexible but also more susceptible to employee fraud and less controllable for the employer. Participants found this method to be less intuitive and mentioned the need for training and regular trial runs through established processes.

Usability vs. Security and Privacy. The trade-off between usability versus security and privacy was an engaging topic among the participants.

- Participants discussed methods that increase key handling *security*. These include the use of multisignatures or other authorization processes that require more than one employee for certain types of transactions. In this case, the compromise of a single key, e.g., through fraudulent employees or loss, does not (necessarily) lead to the loss of all assets. Still, participants were aware of the more complex signing process. A big point of concern is employee fluctuation. Changes to key authorizations and arrangements can trigger cumbersome processes to update all the necessary keys. "*In fact, I have not seen*

truly usable multisignature [...] it is still very manual and very... tedious." [B2]

- For faster and more comfortable access, participants preferred biometric login methods. However, they acknowledged that personal *privacy* is affected by using personal characteristics. "*With regard to comfort, [biometric methods] would definitely be the preference. From a personality and surveillance point of view, it is a nightmare – so in this respect, you have to find a middle ground.*" [B7]

5.1.4. Trust. Trust is established between the financial institution, the employee, and, if present, the intermediary. Trust can be strengthened through different factors that depend on the relationship between the mentioned entities. Most of these themes are already significant for traditional banking and are not specific to KM. Nonetheless, they are vital for KM and thus mentioned.

Financial Institution to Intermediary. If KM is done by a third party, a financial institution needs to trust this intermediary. This trust can be established through numerous factors. One factor is the appropriate implementation of legal requirements, including regular audits. Another source of trust is the name, region of origin, and whether the intermediary is a market leader. The level of knowledge an intermediary can convey, their security concept, and the use of adequate technology also boost trust. "*Before I talk to [intermediaries], they have to prove why I should. Because it's a big company, because they know what they are doing, because they have a security concept, otherwise it's a waste of my time, and at the end of the day I would rely on the biggest player with the highest security on the market anyway.*" [B6]

Financial Institution to Employee. Trust between a financial institution and an employee is built via regulations, control mechanisms, and consequences put in place from the employer's side. The financial institution's goal is to distribute responsibility as much as possible while selecting the best employees to take on the remaining responsibility. "*The employer should make sure that [...] the responsibility is not in the hands of one.*" [B2] Apart from this, the education of employees is an important factor to build trust.

Employee to Intermediary. Trust from the employee to the intermediary is built in a similar way as trust from a financial institution to an intermediary. The intermediary needs to follow legal requirements and show adequate competence. "*I would like to have an institution that tells me: 'Yes, we have your testament, you will get your money and we will help you.' [...] But this is more traditional thinking because it seems more secure.*" [B6]

5.1.5. Financial Institution and Intermediary. Participants talked about legal and non-legal requirements (i.e., the latter add business value but are not legally required) requirements that need to be met by both a financial institution and an intermediary. They also mentioned benefits and drawbacks to mandating an intermediary. Just as for trust, a lot of these themes are present in traditional banking and not solely important for KM. However, we also think that mentioning these requirements is vital for KM in this setting.

Interestingly, the legal and non-legal requirements for an intermediary overlap with the factors that influence and boost trust from a financial institution to an intermediary.

Legal Requirements. Among the legal requirements mentioned were laws that implement KYC procedures and licenses that have to be obtained before any form of custodial business can be established. On the other hand, participants also mentioned the need for regulations that manage certificates and make sure that regular audits are conducted, both for the business practices followed during the past year and to audit established processes in regular intervals.

Non-Legal Requirements. An often mentioned non-legal requirement is the implementation of secure and safe processes and mechanisms. Storage of keys is crucial for both a financial institution and an intermediary with the goal of handling KM. Other important topics are transaction history, 24/7 availability and insurance, the last of which is especially crucial for intermediaries.

Benefits and Drawbacks for Intermediary. Benefits mentioned included outsourcing of responsibility and day-to-day activities as well as insurance. Drawbacks mentioned included a dependency on a third party and the resulting loss of the freedom cryptocurrencies offer, namely actions outside of highly regulated areas, as well as cost factors.

5.2. RQ2 - Security Requirements

RQ2 Which security and secrecy requirements for KM in financial applications do financial institutions have?

Security and secrecy requirements mentioned by participants can be separated into measures and properties. These can be distinguished into being directly, indirectly or not related to KM as well as being of a technical or non-technical nature. We focus on security measures and properties directly related to KM, independent of a technical or non-technical nature, but also briefly mention the others. A visualization of these security measures and properties and their mapping is shown in Figure 1.

5.2.1. Classification. In the following, we define our structure for the security measures and properties mentioned by participants. We differentiate between security measures and properties with a direct, indirect or no impact on KM and between technical and non-technical security measures and properties. We give a specific example for each feature. All other measures and properties are related to these traits in similar ways.

- Relation to KM
  - ***Direct security measures and properties*** are specifically related to KM or (may) have a close impact on the way KM is handled or implemented. An example are regular updates and upgrades of technology. They impact the implementation and handling of KM since both have to be rethought and tested for every update or upgrade of technology.
  - ***Indirect security measures and properties*** are "not directly related to KM but only have an indirect impact on the way KM is handled or implemented. An example are audits since they may impact the way

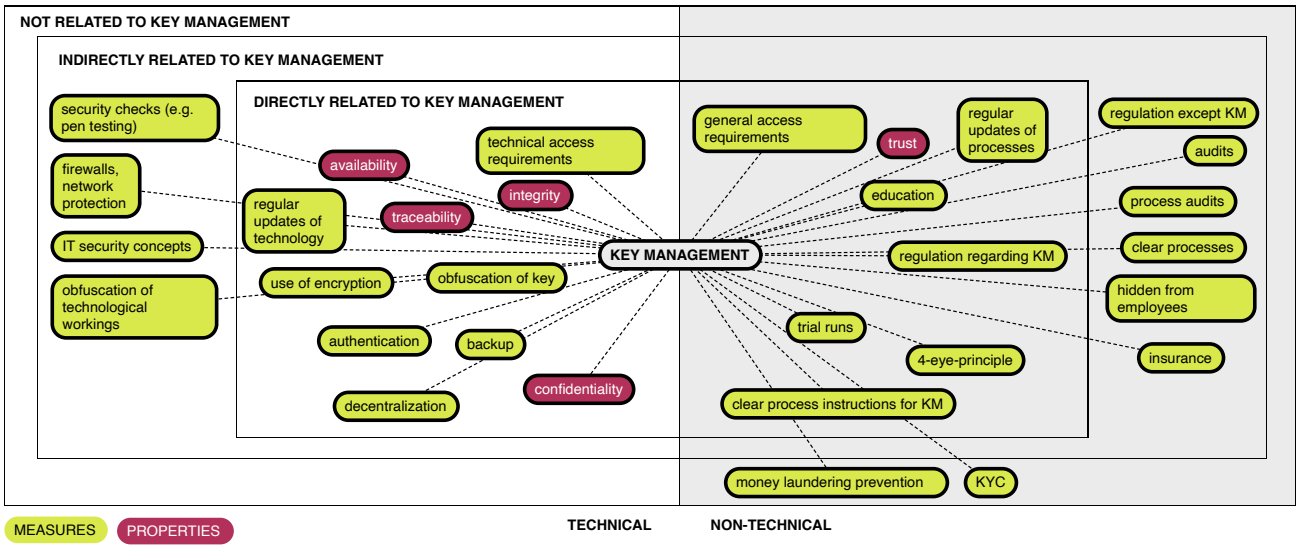

Figure 1. Classification of reported security measures and properties by how they are related to KM and whether they are of a (non-)technical nature.

KM is handled and/or implemented, however this is the consequence of a process change as a result of an audit finding and thus not directly related to KM.

- Any other security measures and properties have ***no impact on KM*** or the way it is implemented or handled. For example, participants mentioned money laundering prevention, which is a big task in the finance world, however it has no connection to KM.

- Technical vs. Non-Technical
  - ***Technical security measures*** are directed at the system or infrastructure. ***Technical security properties*** can primarily be achieved by software-based solutions but may need a regulatory basis for implementation. For example, the availability of systems is a technical security property because the hardware and software have to be available 24/7 and independent of the location, both of which must be defined by rules. Similarly, authentication is a technical security measure since it has to be validated through some software.
  - ***Non-technical security measures*** are primarily of a non-technical nature, and ***non-technical security properties*** can mostly only be fulfilled through the use of non-technical solutions. For example, clear process instructions and regulations for KM are a non-technical security measure. They are of a non-technical nature, although they might lead to technical changes.. Likewise, trust is a non-technical security property because trust in employees is reached through regulations, instructions and other, mostly non-technical factors.

5.2.2. Direct and Technical Security Measures. Security measures that are both direct and technical include topics like the use of encryption, technical access requirements, especially authentication, regular updates of technology, backups, decentralization and the invisibility of the private key to the user.

- The ***use of encryption*** was mentioned as a prevention of hacking attacks.
- Participants described ***technical access requirements*** which mainly focused on security measures that need to be provided by platforms handling transactions including KM. These include the usage of authentication, username and password combinations, two-factor authentication where necessary and the use of biometric factors if possible.
- ***Updates of technology*** were mentioned in the context of knowledge that needs to be available within a financial institution or intermediary to always stay up to date.
- Participants mentioned different options for ***backups***. These included cold storage of backups in a safe, decentralized storage, the distribution of key parts, also known as key sharding, and utilization of multisignatures. Also mentioned was the general expectation that a backup will be available if the key is hosted on bank servers or handled by an intermediary (custodial key storage).
- ***Decentralization*** was mentioned in two ways. First, authorization of key usage through an intermediary should not be possible through a central software component. Second, decentralized key storage without the need for a central component should be used.
- Participants preferred an ***invisible private key***, so users with less background can also properly use the system.

5.2.3. Direct and Technical Security Properties. Security properties that we labeled as direct and technical include confidentiality, integrity, availability, and traceability of actions.

- ***Confidentiality*** in a corporate finance environment is highly important since keys tied to financial assets are especially worth protecting.

- ***Integrity*** prevents redirection of funds.
- Participants mentioned ***availability*** in terms of 24/7 availability, having access from anywhere, and being able to recover keys.
- Participants acknowledged repeatedly that ***traceability*** was crucial, specifically who did what, when, and how.

5.2.4. Direct and Non-Technical Security Measures. We labeled the following security measures as direct and non-technical: general access requirements, education, updates, regulation, including clear process instructions for KM, and the four-eyes principle.

- ***General access requirements*** included different access rights for users depending on their level of responsibility, access recovery mechanisms in case of credential loss and, if present, access restrictions for physical storage.
- Participants mentioned ***educational measures*** as an essential security measure. Users need to have basic knowledge on KM for general use and a technical understanding of the inner workings if they have close contact to KM (see also Section 5.1.3). Topics mentioned included cryptocurrencies and blockchain, associated risks, potential consequences of misuse, and specific education about private keys. Trial runs at regular intervals were also mentioned for two reasons: (i) as a repeated educational measure and (ii) to make sure people practice proper software and hardware usage.
- ***Regular updates of processes*** were mentioned in combination with the previously described updates of technology. Knowledge about the inner workings of KM is necessary to establish these processes and think about fitting security measures. Regular updates of processes are crucial to stay up to date.
- Participants mentioned that ***regulation and clear process instructions for KM*** were a necessity. Financial institutions and intermediaries or custodians need to be licensed and regulated through BaFin. Any regulations need to be translated into policies and clear process instructions through the financial institution.

  > "*[The participant is talking about the benefits of regulation and clear instructions for key storage.] Yes, as I said, there's no room for discussion. The [transaction] history is well comprehensible. Who did and did not do what, when, and how. This gives security to the employee. They will feel more at ease. It is of course also better for the regulatory authority because without this ... I have to be very clear now, this has to be. Without this, BaFin would not allow it. Then we could close down immediately. So, this is ... I don't think about this, because there is no way this [having no regulation] would work in practice. In a bank, everything is regulated.*" [B3]
- Participants mentioned the ***four-eyes principle*** as a measure for the distribution of responsibility among employees and as a control mechanism by the financial institution.

5.2.5. Direct and Non-Technical Security Properties. Trust was the only direct and non-technical security property mentioned. This mostly refers to trust from the financial institution in the employee. For details, see Section 5.1.4.

5.2.6. Indirect Security Measures. Indirect technical security measures include security checks, e.g., pen testing, firewalls and network protection, IT security concepts, and the hiding of technical workings. Indirect non-technical security measures cover regulation and clear processes not focused on KM, audits and insurance.

5.2.7. Other Security Measures and Properties. Other non-technical security measures mentioned are the Know-Your-Customer (KYC) [27] requirement and generally money laundering prevention measures.

5.3. RQ3 - Attacker and Threat Types

RQ3 Which attacker and threat types have an impact on DLT key management in financial institutions?

The following sections summarize different attacker types and threats as reported by the participants. A visual categorization of the attacker types can be found in Figure 2 and of threat types in Figure 3.

5.3.1. Attacker Types. Participants differentiated between internal and external attacker types. Internal attackers are employees who turn to malicious actions, whereas external attackers can be split into hackers and thieves. Hackers are responsible for digital data theft and misuse, whereas thieves engage in physical theft. Another dimension is whether the perpetrator is an individual, an industry competitor or a government.

5.3.2. Threats. Threats can be summarized into four different categories. These categories are internal, external, systems and infrastructure, and force majeure.

Internal threats originate either from the financial institution itself or employees. Misuse through the financial institution includes insufficient regulation, no strategy, and no or not enough education. Misuse by employees can be categorized into unintentional and intentional misuse. Unintentional misuse is not intended to cause harm. It may originate in trivial usability issues sometimes leading to mishaps. For example, overburdening or unusable security features might lead to careless circumvention acts. Intentional misuse negligently accepts harm and includes theft, fraud, or assisting fraud. It also includes people with

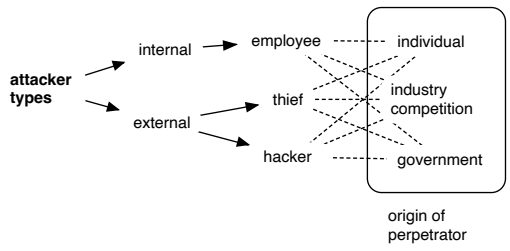

Figure 2. Attacker types linked to threats for KM and their possible origin.

administrative access misusing their power. Loss of keys, credentials, hardware, mishandling of information, and sharing keys can be both unintentional and intentional. "*You don't want to lose [the key] – especially when it is your employer's. (...) From personal experience, I am always more afraid of losing the key than it being stolen.*" [B1]

External threats are either directed towards the financial institution or towards an intermediary. Hacking, theft and social engineering are the threats that overlap for both. Examples of mentioned threats are ransomware, monster-in-the-middle (MITM) attacks and phishing. External threats directed towards the intermediary are also bankruptcy, key loss and misuse.

Threats targeted at systems or infrastructure are threats that somehow involve technology. They can be categorized as threats directed to the blockchain, the financial institution, or an intermediary. Threats for the blockchain are non-reversibility of transactions, vulnerabilities in the blockchain framework, and connection issues on the network. Threats towards the financial institution and the intermediary are identical. These are vulnerabilities in any software used for KM, connectivity issues and any malfunction of hardware.

Force majeure threats include fires, electricity outages, and natural catastrophes in general. They also include strikes and the death of employees.

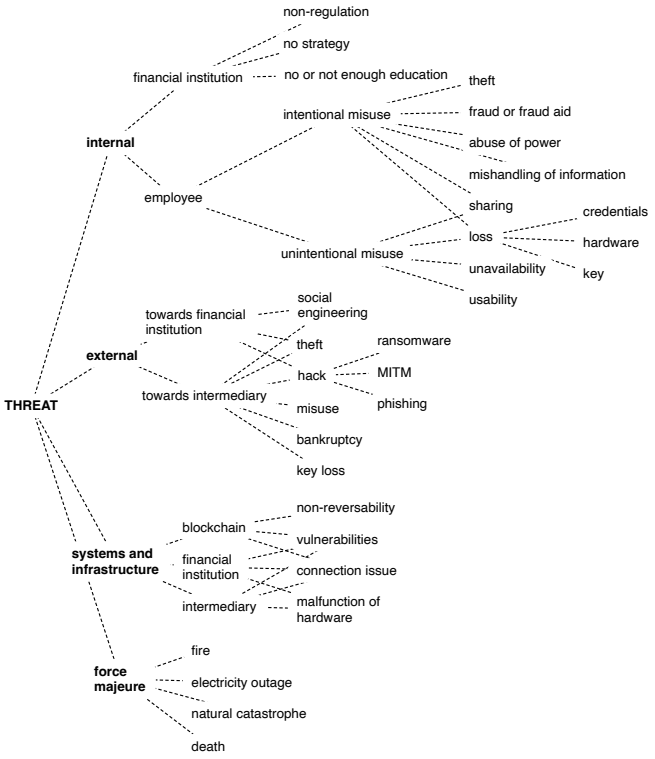

Figure 3. Threats for KM in a corporate finance environment. Threat types include internal, external, systems and infrastructure and force majeure.

5.4. RQ4 - Discrepancies between Requirements and DLT

RQ4 What are areas of tension between the requirements of finance professionals, security requirements, and the technical abilities of state-of-the-art DLT?

Even though there exist a lot of different DLT architectures, we chose to focus on the most widespread implementation, Bitcoin. We identified two major areas of tension, both of which are related to key usage. First, access rights management directly on Bitcoin is very complex since this blockchain was not designed for change. Second, access rights management outside of Bitcoin is highly dependent on its security and trust environments.

The following paragraphs explain these areas of tension in more detail. This is aided by three primary use cases we derived from our interviews which are crucial to KM.

1) signing a transaction $1:1$ (1 transaction, 1 signer)
2) signing a transaction $1:n$ (1 transaction, n signers)
3) change of access rights

All three use cases can be implemented either on Bitcoin or via an external technical solution.

5.4.1. Access Management on Bitcoin. If the use cases are implemented on Bitcoin, assets are either protected through one key pair or through n key pairs. In the case of n key pairs, this is usually realized through m-of-n multisignature where m keys are needed to sign a transaction.

If one key pair is used (use case 1), the private key has to be shared across all end users with access to the assets. This leads to many problems in the case of trigger events (see Sec. 5.1.1) like people leaving the company. Every time a trigger event happens, a new key pair has to be set up, the assets have to be shifted, which incurs transaction costs, and the new key pair needs to be distributed. In this use case, access management is very restricted. It is not traceable who signed a transaction, as every employee has access to all assets linked to the key pair and the financial institution has no control. Since there is only one key pair, every user can sign every transaction by themselves.

On the other hand, when using an m-of-n multisignature (use case 2), every end user can have their own key. This leads to many of the same problems as in the case of a single key. Nonetheless, in this case, it is traceable who signed a transaction if there exists a link between key pairs and natural people. For $m \neq 1$, also more than one person has to sign a transaction. Still, multisignatures on Bitcoin have the drawback that they are very complex to set up and use, and thus expert knowledge is required.

Access management (use case 3) in combination with custodial key storage on Bitcoin is not possible. Furthermore, non-custodial key storage was strongly opposed.

5.4.2. Access Management outside Bitcoin. Instead of managing access on the blockchain, it can also be realized via a gateway application. In the back end this can both be realized via one key pair or n key pairs.

The major drawback of using a separate access management application is the expansion of the attack surface. The security of this application is highly perceptible to the trust

and security issues of the environment it is built within. On the upside, a lot of the requirements of the financial sector can be realized. The four-eyes principle and changes in access management are easily implemented. Furthermore, key storage and key usage can be abstracted away from (i.e., made invisible to) the user.

While this may solve some of the problems the financial sector faces with regard to KM, using access management outside Bitcoin shifts the challenges of KM to other authentication problems. These are also open problems in usable security, for which we do not have holistic answers yet.

6. Discussion

We discuss and interconnect further discrepancies between DLT's KM and the financial sector, as well as future work based on our results.

Legal and Liability Challenges. Responsibility in the event of security breaches is a legal and liability challenge unique to financial institutions. For individual users, key theft, loss, or other mishaps affect only them. The major differences for financial institutions are that (1) they often manage third-party assets and (2) the scale of these assets leads to closer scrutiny and restrictions. On the technical side, this can be mitigated through concise and restrictive processes for users, e.g., their interaction with keys is limited or keys are hidden. On a non-technical side, regulators should publish minimum standards for precautions financial institutions and intermediaries must implement to protect themselves and their employees.

Implementation of the four-eyes principle is a liability challenge. The four-eyes principle translates to multiple users needing to approve a transaction and thus needing joint access to the same assets, see Section 5.4 – a scenario that is irrelevant to individual users. One solution is to combine hot and custodial key storage integrated into a system already used in-house, which also conceals the key from the user. Thus, KM will be as secure or insecure as the application and the authentication mechanisms used. This adds authentication challenges to the KM problem. Authentication is another major unsolved research area in usable security for which novel approaches are needed, irrespective of the application scenario. Moreover, all benefits (e.g., already used and known authentication mechanisms) and all drawbacks (e.g., bugs and loopholes) of already used in-house systems will be transferred to KM.

Organizational Challenges. There are organizational challenges unique to financial institutions that have no impact on individual users. Examples are multi-user use cases, employee absences, and employee turnover. In these cases, KM needs to be well-defined, and control mechanisms need to be put in place. These have to ensure that processes are applied as intended. Solutions also depend on the size of the organization and the speed with which it can adapt to change. Traditional banking institutions highly depend on solutions that are closely modeled after existing infrastructure, e.g., hierarchical access models (see Section 5.1.1), while fintechs may have an easier time adapting to requirements due to their smaller size and higher agility.

All three challenge types are specific to financial institutions and independent of individual users. Future research on the usability of multi-user KM systems with integrated access management and multi-tier transaction approval is needed. Additionally, contrasting younger with more established institutions, or different sectors, might yield valuable insights.

Trust. Trust is not unique to key management. Overall, client trust in financial institutions is independent of their DLT usage. Nonetheless, minimum standards would provide a competitive advantage (e.g., minimum risk requirements provided by BaFin [2]) even when they pose constraints on the implementation. We argue that future standardization efforts should touch on the security requirements for different key storage options. Therefore, further research into the exact standards for multi-user KM is necessary. Our results suggest that there are no specific types of trust related to key management in financial institutions, see Section 5.1.4.

International Differences. Germany is known for its high standards and detail-obsessed bureaucracy. This could complicate the implementation and adoption of investment funds on DLT in Germany, while other countries may have already tested digital solutions that solve similar use cases and can serve as a foundation. Due to the qualitative nature of our work and the focus of our results on Germany, future work will need to explore the differences between different countries and cultures. Qualitative follow-up work can contrast our results with the viewpoints of individuals working in other jurisdictions. Quantitative follow-up work can generalize the hypotheses derived from our work, such as, how to map hierarchical structures onto asset access. However, generalizability will only be given in the specific cultural group these hypotheses were tested in, as shown by Henrich et al. [29].

7. Conclusion

This paper takes a deep dive into the relationship between financial institutions and key management for distributed ledger technology (DLT). Two qualitative interview studies with professionals from the field contrast the actual requirements with the technical reality. Our sample includes participants from fintechs and blockchain start-ups that can easily align their processes around a blockchain, to conventional financial institutions that are more restricted through their size and history.

KM for DLT in general (and Bitcoin specifically, as its most important financial representative) does not meet the real-world legal and organizational requirements of the industry on multiple levels. The effort to maintain on-chain authentication and audit functionality covering day-to-day operations, e.g. employee absence or shifting responsibilities within the organization – as well as – contingencies such as key compromise or force majeure events – is unmanageable, except for the smallest institutions.

Acknowledgments

We would like to thank the reviewers and the anonymous shepherd for their constructive feedback.

This work was partially funded by INTAS.tech and Plutoneo Consulting GmbH.

References

[1] DLT pilot regime: Securities trading on the blockchain. https://www.osborneclarke-fintech.com/2022/10/27/dlt-pilot-regime-securities-trading-on-the-blockchain/, accessed 2023-04-05.

[2] Rundschreiben 09/2017 (BA) - Mindestanforderungen an das Risikomanagement - MaRisk. https://www.bafin.de/dok/10149454, accessed 2023-04-05.

[3] Gesetz über das Kreditwesen (Kreditwesengesetz - KWG). 1961.

[4] Kapitalanlagegesetzbuch (KAGB). 2013.

[5] Gesetz zur Einführung von elektronischen Wertpapieren (eWpG). *Bundesgesetzblatt (Deutschland)*, I(29):1423–1435, 2021.

[6] Gesetz über elektronische Wertpapiere (eWpG). 2021.

[7] Verordnung über Kryptofondsanteile (KryptoFAV). *Bundesgesetzblatt (Deutschland)*, I(19):868–869, 2022.

[8] Svetlana Abramova, Artemij Voskobojnikov, Konstantin Beznosov, and Rainer Böhme. Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–19, New York, NY, USA, 2021. ACM.

[9] Gavin Andresen. M-of-N Standard Transactions. https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki, accessed 2023-04-05, 2011.

[10] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. Hyperledger fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA, 2018. ACM.

[11] Financial Conduct Authority. Financial sector. https://www.handbook.fca.org.uk/handbook/glossary/G1412.html#, accessed 2023-04-05.

[12] Elaine Barker. Recommendation for Key Management: Part 1 – General. Technical Report NIST Special Publication (SP) 800-57 Part 1 Rev. 5, National Institute of Standards and Technology, May 2020.

[13] Badr Bellaj, Aafaf Ouaddah, Emmanuel Bertin, Noel Crespi, and Abdellatif Mezrioui. SOK: A Comprehensive Survey on Distributed Ledger Technologies. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, ICBC '22, pages 1–16, Shanghai, China, May 2022. IEEE.

[14] Michael Brengel and Christian Rossow. Identifying Key Leakage of Bitcoin Users. In Michael Bailey, Thorsten Holz, Manolis Stamatogiannakis, and Sotiris Ioannidis, editors, *Research in Attacks, Intrusions, and Defenses*, RAID '18, pages 623–643, Cham, Switzerland, 2018. Springer International Publishing.

[15] Carsten Heise, BaFin. Now also in electronic form: securities. https://www.bafin.de/dok/16589128, accessed 2023-04-05.

[16] CROS - Collaboration in Research and Methodology for Official Statistics. Four eyes principle. https://ec.europa.eu/eurostat/cros/content/four-eyes-principle_en, accessed 2023-04-05.

[17] Adrian Dabrowski, Katharina Pfeffer, Markus Reichel, Alexandra Mai, Edgar R. Weippl, and Michael Franz. Better Keep Cash in Your Boots - Hardware Wallets are the New Single Point of Failure. In *Proceedings of the 2021 ACM CCS Workshop on Decentralized Finance and Security*, CCS '21, pages 1–8, Virtual Event Republic of Korea, November 2021. ACM.

[18] Poulami Das, Sebastian Faust, and Julian Loss. A Formal Treatment of Deterministic Wallets. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 651–668, New York, NY, USA, November 2019. ACM.

[19] Shayan Eskandari, Jeremy Clark, David Barrera, and Elizabeth Stobert. A First Look at the Usability of Bitcoin Key Management. In *NDSS Workshop on Usable Security (USEC) 2015*, USEC '15, San Diego, CA, USA, 2015.

[20] European Commision. Digital finance package. https://finance.ec.europa.eu/publications/digital-finance-package_en, accessed 2023-04-05.

[21] Federal Financial Supervisory Authority. About BaFin. https://www.bafin.de/EN/DieBaFin/diebafin_node_en.html, accessed 2023-04-05.

[22] Federal Financial Supervisory Authority. Know-Your-Customer (KYC). https://www.bafin.de/SharedDocs/FAQs/EN/Fintech/Geschaeftsmodelle/Regtechs/Anwendungen/3_en.html?id=18490484, accessed 2023-04-05.

[23] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, SOUPS '16, pages 1–14, Denver, CO, USA, 2016. USENIX Association.

[24] Michael Fröhlich, Felix Gutjahr, and Florian Alt. Don't lose your coin! Investigating Security Practices of Cryptocurrency Users. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, DIS '20, pages 1751–1763, Eindhoven, Netherlands, July 2020. ACM.

[25] Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, and Robert C. Miller. How to Make Secure Email Easier to Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, pages 701–710, New York, NY, USA, April 2005. ACM.

[26] Gesley, Jenny. Germany: Electronic Securities Act Enters into Force, 2021. Library of Congress, https://www.loc.gov/item/global-legal-monitor/2021-06-29/germany-electronic-securities-act-enters-into-force/, accessed 2023-04-05.

[27] Martin Gill and Geoff Taylor. Preventing Money Laundering or Obstructing Business?: Financial Companies' Perspectives on 'Know Your Customer' Procedures. *The British Journal of Criminology*, 44(4):582–594, April 2004.

[28] Mike Hearn. Corda: A distributed ledger. page 56.

[29] Joseph Henrich, Steven J. Heine, and Ara Norenzayan. The Weirdest People in the World? *Behavioral and Brain Sciences*, 33(2-3):61–83, June 2010.

[30] Amir Herzberg and Hemi Leibowitz. Can Johnny Finally Encrypt? Evaluating E2E-Encryption in Popular IM Applications. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*, STAST '16, page 17–28, New York, NY, USA, 2016. ACM.

[31] Yiwen Hu, Sihan Wang, Guan-Hua Tu, Li Xiao, Tian Xie, Xinyu Lei, and Chi-Yu Li. Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, CODASPY '21, pages 89–100, New York, NY, USA, April 2021. ACM.

[32] Germany Trade & Invest. Financial services. https://www.gtai.de/en/invest/industries/services/financial-services#863580, accessed 2023-04-05.

[33] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "If HTTPS Were Secure, I Wouldn't Need 2FA" - End User and Administrator Mental Models of HTTPS. In *2019 IEEE Symposium on Security and Privacy (SP)*, SP '19, pages 246–263, San Francisco, CA, USA, May 2019. IEEE.

[34] Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security*, FC '16, pages 555–580, Berlin, Heidelberg, Germany, 2016. Springer Berlin Heidelberg.

[35] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. "I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS. In *26th USENIX Security Symposium*, USENIX Security '17, pages 1339–1356, Vancouver, BC, Canada, August 2017. USENIX Association.

[36] Alexandra Mai, Katharina Pfeffer, Matthias Gusenbauer, Edgar Weippl, and Katharina Krombholz. User Mental Models of Cryptocurrency Systems - A Grounded Theory Approach. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, SOUPS '20, pages 341–358, Virtual Event, 2020. USENIX Association.

[37] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009.

[38] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent Seamons. "We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4298–4308, New York, NY, USA, 2016. ACM.

[39] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. A Usability Evaluation of Let's Encrypt and Certbot: Usable Security Done Right. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 1971–1988, New York, NY, USA, November 2019. ACM.

[40] Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users. In Joseph Bonneau and Nadia Heninger, editors, *Financial Cryptography and Data Security*, FC '20, pages 595–614, Cham, Switzerland, 2020. Springer International Publishing.

[41] Artemij Voskobojnikov, Oliver Wiese, Masoud Mehrabi Koushki, Volker Roth, and Konstantin (Kosta) Beznosov. The U in Crypto Stands for Usable: An Empirical Study of User Experience with Mobile Cryptocurrency Wallets. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–14, New York, NY, USA, 2021. ACM.

[42] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th conference on USENIX Security Symposium*, SSYM '99, pages 1–14, USA, August 1999. USENIX Association.

[43] Dr Gavin Wood. Ethereum: A Secure Decentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*, pages 1–32, 2014.

[44] Pieter Wuille. Hierarchical deterministic wallets. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki, accessed 2023-04-05, 2012.

[45] K. Wüst and A. Gervais. Do you Need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, CVCBT '18, pages 45–54, Zug, Switzerland, June 2018. IEEE.

Appendix A. Background on DLT Regulation

Germany. In January 2020, financial services on the subject of cryptographic assets and cryptographic keys were included in German legislation for the first time (KWG § 1, para. 1a, no. 6.) [3].

This was extended with the introduction of the "Gesetz über elektronische Wertpapiere (eWpG)" (engl. Electronic Securities Act) [5], [6] in June 2021, which "enables the issuance of bearer bonds using innovative technologies such as distributed ledger technology (DLT)" [26]. This law allows the electronic issuance of "bearer bonds, mortgage bonds (Pfandbriefe) and certain fund units" [15], which means that an issuer no longer issues a physical securities certificate, but makes an entry in an electronic securities register. An electronic securities register is either a *central register* or a *crypto securities register*. A central register is maintained by either a central securities depository or a custodian authorized by an issuer. A crypto securities register is maintained on a tamper-proof decentralized recording system, e.g., a blockchain, which logs entries in chronological order and protects against deletion and subsequent modification. The eWpG only allowed the issuance of bearer bonds on crypto securities registers.

Along with the introduction of the eWpG, § 95 of the "Kapitalanlagegesetzbuch (KAGB)" (engl. German Investment Code) [4], [5] was changed to allow the electronic issuance of investment funds on central registers through custodians. The "Verordnung über Krypofondsanteile (Krypto-FAV)" (engl. Regulation on Crypto Fund Shares) introduced the electronic issuance of investment funds on crypto securities registers through custodians.

European Union. The European Commission proposed its digital finance package with a digital finance strategy in 2020 [20]. The goal is room for innovation in financial products while protecting consumers and financial stability. One part of this strategy is the DLT pilot regime, which is valid for 3 years and allows securities trading based on DLT to be tested within a regulated framework. There are limits to the volume of the traded assets. The goal is to built a "reliable and secure secondary market for crypto assets" [1].

Appendix B. Interview Guidelines and Codebooks

All tables are structured top to bottom, left to right.

B.1. Stage A

Table 2 provides the interview guideline for stage A. All interviews were held in German, thus this interview guideline was translated to English. Our codebook for stage A is available in Table 4.

B.2. Stage B

Table 3 presents the interview guideline for stage B. The interview guideline was translated to English. Our codebook for stage B is available in Table 5.

TABLE 2. INTERVIEW GUIDELINE FOR STAGE A

Part	**Explanations, Questions**	***Comments*, Further Explanations**
Intro	Hello, thank you for your participation in this interview.	*Greet participant and thank for participation.*
	The goal of this interview is to learn more about credential management possibilities and which of these may be suitable options in the financial sector. I will introduce a context and ask some questions to specific topics. There are no right or wrong answers. Feel free to say anything that comes to mind. You are the expert in this interview.	*Explain the topic and purpose of the study.*
	First I would like to get your consent for this interview and the recording of it. I will send you the consent text in the chat. Please read it carefully and then give your consent verbally.	*Get consent from the interviewee for taking part in the interview.*
	Can you please repeat your consent?	*Start audio recording and ask the participant to repeat consent.*
Part 1 Demograpics	To start, I would like to ask some general demographic data. • How old are you? • What is your highest completed level of education? • What is your current job title? • How long have you been working in the financial sector?	Inquiry of general demographic data.
Different storage options	In the following we want to look at four different types of storage options. All will be introduced within the fictional context of digital investment funds and then the same questions will be asked for each.	
Context	Let's assume that digital investment funds will be traded in the future. We are talking about trading of investment funds with appropriately high sums (e.g. $>$ 500.000$). In order to buy these, employees in the financial sector need access data. This access data is very long, longer than what you know from normal username and password combinations. This access data has the following properties: • The access data is very long (several hundreds characters). For the average user it is impossible to memorize this access data. • Access data is non-recoverable. • Access data is not modifiable in case of loss.	
Group 1: Hot vs. Cold	We will start with the first topic block.	
Part 2 Cold	We will start with the cold storage of access data. This combines everything that can be used outside of a technical device or anything, that is not always connected to the internet. Examples are writing access credentials on paper and storing this securely or using a hardware security module (HSM). [For questions see below]	*If the difference between electronic and non-electronic is not mentioned, mention this:* Specifically for the cold storage option, one can also differentiate between electronic and non-electronic. A non-electronic storage option, e.g., is writing on a sheet of paper and storing it securely.
Part 3 Hot	Next we will talk about hot storage. This includes anything that uses a technical device that is connected to the internet most of the time. For example a program or file on your computer or cell phone. [For questions see below]	
	[For questions after Hot vs. Cold part see below.]	
Group 2: Custodial vs. Non-Custodial	That was the first topic block. Let's continue to the second topic block.	
Part 4 Non-Custodial	We will start with the non-custodial storage of access credentials. The user has full control and responsibility over their access data. Examples are technical devices or devices supplied by the employer specifically for storing access data.	
Part 5 Custodial	The last storage option we are talking about is custodial storage. In this scenario, the data is not exclusively stored by the user but also or exclusively by another entity. An example would be that an employee needs to log into a website to obtain access to the access data.	
	[For questions after Non-Custodial vs. Custodial part see below.]	
Questions	[Questions after each part or storage option.]	
Questions for each storage option	• What are your thoughts about this storage option? • What benefits do you see? • What drawbacks do you see? • In your opinion, is this a storage option you could see in this work environment (referring to context)? Why? Why not? • Is this storage option integrable in current infrastructure? Or would it be a modern novelty? • How could this storage option look like at the place of work? How could it be integrated? Could problems arise? What are your thoughts? • In your opinion, is this a realistically usable option? Why? Why not? • What are your thoughts about the security of this option?	Ask the following questions after each storage option.
Questions after Hot vs. Cold and Non-custodial vs. Custodial parts.	• Comparing these two options, what are your thoughts? • Which of the options could you see in this work environment in the future? • Do you have anything to add to these options?	Ask the following questions after each group ("Hot vs. Cold" and "Custodial vs. Non-Custodial").
Final questions before debriefing	If digital investment funds with these types of access credentials are introduced, which type of storage option would you prefer? Why?	Ask the following questions after both groups.
Debriefing	• Do you have any questions? • Would you like to add anything?	
	To recap, this interview was about potential storage options and how private and public keys that are used in cryptographic algorithms can be stored.	Recap of the purpose of the interview.
	Please contact me if any questions arise in the future or if you want to revoke your consent to the interview and its recording.	Contact data for further questions or revocation of consent.
	Thank you for your participation and your knowledge. We have reached the end of the interview. Have a great day!	Thank the interviewee for their time and input.

TABLE 3. INTERVIEW GUIDELINE FOR STAGE B

Part	Explanations, Questions	*Should be covered*, Backup Questions, Explanations
Intro	Thank you for your participation in this interview. Today, we will talk about the usage of wallets in the financial industry. This interview is structured as follows. In the first part, I will ask a few generic questions. Then we will talk about cryptocurrencies and storage methods. Finally, we will briefly talk about security requirements and privacy.	
	You can talk frankly about anything that comes into your mind. There are no right or wrong answers or opinions here. You are the expert in this interview.	
Consent	Do you still consent to participating in this interview and the recording of it?	
	[start recording and ask to repeat consent]	
Part 1 **General questions**	First, I like to start with the general part.	Experience with cryptocurrencies
	What are your experiences with cryptocurrencies?	
	In your opinion, what is the cryptographic part in cryptocurrencies?	
Part 2 **Key Management and Authentication**	We will start with a drawing task.	
	[share the whiteboard]	
	First, let us test the whiteboard. On the top edge, you should see the menu named 'view options'. If you select 'annotate', you should be presented with a toolbar. Can you draw anything for testing, please?	
	Context: Let's assume you and your work colleagues are responsible for trading and managing Bitcoin worth several hundred millions of Euros for your Employer.	*participants, trancation, process, signature, access, access rights, regulation, direct trade*
	Task: Please draw a diagram on how you understand a transaction between you as a seller and a buyer works. Assume those are your employer's 200 bitcoins. Please draw all relevant entities and components. Talk while drawing and explain your diagram.	How to make sure that you are allowed to trade Bitcoin? (supervisor, four-eyes principle) How do you have access to the Bitcoins? (technical)
	Do you see any security risks? If yes, what are they? From what origin?	*security risks, attacker* Do you see options for attacks?
	How do you visualize a digital signature? When and where is it present in your picture?	*digital signature*
	This concludes the first big part.	
Part 3 **Key Management and Key Storage**	We will now talk about storage of access data for Bitcoin. I will first ask some general questions and then I will ask some questions to specific key storage options.	*perfect storage option, access, threats, opinion of different storage options*
	What does this access data look like?	*combination of numbers and letters, length: depends on format, opinion*
	What are traits of the perfect key storage method?	*Who is responsible?, What happens in case of loss?, user input, user interaction, hot or cold, custodial or non-custodial* similar to wallet: HSM, software wallet, paper wallet
	Do you see any security risks? If yes, what are they?	*risk, attacker, physical, electronically* Do you see risks? What do they look like? Who is the perpetrator?
	Is there something that your employer has to pay special attention to?	*special security measures, regulations, processes* special security measures that have to be met or regulations that have to be followed?
	What is the responsibility that you carry for this key?	
	How would your collegues access those Bitcoins?	
	How do changes in access rights look like? How are they implemented?	
	Now I will ask some questions about key storage. There are four different types of storage options. I will introduce all of them briefly and then ask some questions.	
	Questions for each key storage method: • What benefits for this option do you see from an employer/employee perspective? • Which drawbacks do you see from an employer/employee perspective? • What are your responsibilities? • What are the consequences in case of loss? • Do you see problems or security risks? If yes, what are they? • What could be improved with this option?	*protection, security, attacker, attacker potential, responsibility*
	Cold Key Storage: Cold key storage combines everything that can be used outside of a technical device, or anything that is not always connected to the internet. Examples are writing keys on a sheet of paper and storing it securely or using hardware security modules (HSMs).	
	Hot Key Storage: Hot key storage includes anything that uses a technical device that is connected to the internet most of the time. For example a program or file on your computer or cell phone.	
	Non-Custodial Key Storage: In non-custodial key storage, the user has full control over and responsibility for their access data. Examples are technical devices or devices supplied by the employer specifically for storing access data.	
	Custodial Key Storage: In custodial key storage, the data is not exclusively stored by the user but also or exclusively by another entity. An example would be that an employee needs to log into a website to obtain the access data.	
Part 4 **Requirements for Security and Privacy**	Let's assume that a platform exists that handles buying, selling and custody of Bitcoins for you and your colleagues and you are supposed to work with this platform.	*Requirements of user, requirements regarding security: personal security, personal protection, system; access, tracking, data storage, regulation, legal requirements* Does data exist that needs to be stored? If yes, which? Do processes exist that have to be followed? If yes, which?
	• Which type of key storage do you prefer? • What requirements do you have for such a platform? • Which requirements do you see from a legal point of view? • Which regulations need to be followed? • Which requirements, specifically from a security point of view, have to be met by this platform? • How could access to this platform look like?	
Part 5 **Outro**	Do you have further questions or comments? Do you have anything to add?	
	Thank you for your participation. If you have any questions afterwards or want to withdraw your consent to the use of your data, please contact me.	
	One last question: Do you know anyone with a similar profile that would be interested to participate in this study?	

TABLE 4. CODEBOOK FOR STAGE A

A01 financial institution	A02.06 education	A04.02 adaptability	A06.07 option
A01.01 acceptance	A02.07 experience	A04.03 benefits	A06.08 risk
A01.02 comparison	A02.08 key sharding	A04.04 cost	A07 threat
A01.03 consequences	A02.09 KYC	A04.05 drawbacks	A07.01 attackers
A01.04 control	A02.10 limitations	A04.06 intermediary	A07.02 external
A01.05 cost benefit-calculation	A02.11 password	A04.07 option	A07.03 fraud
A01.06 customer	A02.12 physical layer	A04.08 risk	A07.04 internal
A01.07 delegation	A02.13 PIN	A05 storage hot	A08 usability
A01.08 digitalization	A02.14 prevention	A05.01 accessability	A08.01 access
A01.09 education	A02.15 regulation	A05.02 adaptability	A08.02 ease of access
A01.10 future oriented	A02.16 responsibility	A05.03 benefits	A08.03 ease of use
A01.11 insurance	A02.17 secure system	A05.04 drawbacks	A08.04 easy
A01.12 process assessment	A02.18 storage	A05.05 future oriented	A08.05 efficiency
A01.13 processes	A02.19 traceability	A05.06 habit	A08.06 knowledge
A01.14 regulation	A02.20 user	A05.07 MPC	A08.07 lean
A01.15 responsibility	A03 storage cold	A05.08 option	A08.08 obscurity
A01.16 risk assessment	A03.01 accessability	A05.09 requirement	A09 user
A01.17 safety precautions	A03.02 adaptability	A05.10 safety measure	A09.01 ability
A01.18 standardization	A03.03 benefits	A05.11 sharing	A09.02 effort
A01.19 strategy	A03.04 cost	A05.12 traceability	A09.03 fear
A01.20 system	A03.05 drawbacks	A05.13 transparency	A09.04 help
A01.21 trust	A03.06 maintanance	A06 storage non-custodial	A09.05 knowledge
A02 security	A03.07 option	A06.01 adaptability	A09.05 mentoring
A02.01 4-eye-principle	A03.08 security measures	A06.02 autonomy	A09.06 misuse
A02.02 access	A03.09 sharing	A06.03 benefits	A09.07 responsibility
A02.03 audit	A03.10 trust	A06.04 cost	A09.08 time
A02.04 backups	A04 storage custodial	A06.05 drawbacks	
A02.05 bureaucracy	A04.01 accessability	A06.06 no standard	

TABLE 5. CODEBOOK FOR STAGE B

B01 cryptographic understanding	B04.04 preference	B07.05 decentralization	B08.05 non-custodial
B01.01 blockchain	B04.05 process	B07.06 education	B08.06 preference
B01.02 experience	B04.06 trigger event	B07.07 financial institution	B09 threat
B01.03 key	B05 platform	B07.08 four-eyes principle	B09.01 attacker
B01.04 metaphor	B05.01 access	B07.09 integrity	B09.02 external
B01.05 signature	B05.02 access rights	B07.10 know your customer	B09.03 force majeure
B01.06 transaction	B05.03 data	B07.11 obfuscation	B09.04 internal
B01.07 wallet	B05.04 help	B07.12 prevention	B09.05 technical
B02 financial institution	B05.05 key	B07.13 reaction	B10 trust
B02.01 comparison	B05.06 release process	B07.14 regulation	B10.01 in employee from employer
B02.02 employee	B05.07 security requirements	B07.15 secure network	B10.02 in intermediary from employer
B02.03 employer	B05.08 threat	B07.16 technical layers	B10.03 in intermediary from user
B03 intermediary	B05.09 transaction	B07.17 traceability	B10.04 factors
B03.01 benefit for employer	B05.10 requirements	B07.18 transparency	B11 usability
B03.02 drawback for employer	B05.11 private customers	B07.19 trial runs	B11.01 comfort
B03.03 legal requirements	B06 responsibility	B07.15 trustworthiness	B11.02 ease of use
B03.04 requirements	B06.01 care	B07.16 updates	B11.03 efficient
B03.05 duties	B07 security	B08 storage	B11.04 knowledge
B04 key usage	B07.01 access	B08.01 cold	B11.05 handling
B04.01 access	B07.02 availability	B08.02 custodial	B12 user
B04.02 access rights	B07.03 backup	B08.03 access	B12.01 understanding
B04.03 multisignature	B07.04 confidentiality	B08.04 hot	B12.02 can see risks