idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

CISPA Helmholtz Center for Information Security
Annabelle Theobald

30.06.2023
http://idw-online.de/de/news817059

Forschungsergebnisse, Wissenschaftliche Publikationen
Informationstechnik
überregional

Key-Management wird bei Krypto-Fonds zur Herausforderung

Investierten bis vor einigen Jahren nur tech-affine und risikofreudige Spekulanten in Bitcoin und Co., mausern sich Kryptowährungen zu einer neuen Anlageklasse an den regulären Finanzmärkten. Um damit sicher handeln zu können, brauchen Besitzer:innen kryptografische Schlüssel die geheim bleiben müssen. Schlüssel-Management-Systeme sind bislang auf Einzelnutzer:innen, nicht auf größere Gruppen in Finanzinstitutionen ausgelegt. CISPA-Forscherin Carolyn Guthoff hat in einer qualitativen Interviewstudie aufgezeigt, wie solche Systeme für neue Anwendungen im Finanzsektor fit gemacht werden müssen. Das dazugehörige Paper hat sie auf dem IEEE Symposium on Security and Privacy (S&P;) präsentiert.

Eine dezentral verwaltete Währung, auf die keine Bank, kein Staat und keine Behörde Zugriff hat – das ist die Idee hinter Bitcoin. 2008 erstmals in einem Dokument beschrieben, ist Bitcoin auch heute noch der bekannteste, aber längst nicht mehr der einzige Anwendungsfall der ihm zugrundeliegenden sogenannten Distributed-Ledger-Technologie (DLT). Distributed Ledger bedeutet soviel wie „verteiltes Geschäftsbuch“ und genau das steckt dahinter: eine Datenbank für Transaktionen, die auf vielen Rechnern liegt und so nicht zentral von einer Stelle aus, sondern von vielen Nutzenden dezentral verwaltet wird. „Distributed-Ledger-Technologien sind seit 2014 ein absolutes Hype-Thema in den verschiedensten Branchen“, erklärt Guthoff.

Weitaus geläufiger als DLT ist vielen Menschen der Begriff der Blockchain. Blockchain ist eine der bekanntesten Distributed-Ledger-Technologien und Grundlage für Kryptowährungen. „Der Name kommt daher, dass in der Blockchain Datenblöcke hintereinander abgespeichert werden. Blockchain-Anwendungen wie Bitcoin oder Ethereum basieren auf derselben Technologie, folgen aber unterschiedlichen Regeln“, erklärt Guthoff. Ziel sei aber immer, eine Währung zu haben, die Onlinezahlungen ganz ohne Beteiligung von Finanzinstitutionen möglich machen.

Einzelnutzer-Szenario bei Kryptowährung ist veraltet

Diesen Ursprungsgedanken vor Augen wundert es wenig, dass sich um die Kryptowährungen herum ein Service- und Verwaltungssystem gebildet hat, das auf einzelne Nutzende ausgerichtet ist. So auch im Bereich des Managements der kryptografischen Schlüssel, das für die Abwicklung der Transaktionen in einer Blockchain elementar ist. Jede Finanztransaktion zwischen zwei Handelspartner:innen auf der Blockchain muss genauestens dokumentiert werden und ist für alle Nutzenden sicht- und nachvollziehbar. Nur so bleibt das System insgesamt vertrauenswürdig und zuverlässig. Dabei besitzen Kryptocoin-Besitzer:innen neben einem öffentlichen auch einen sogenannten Private Key, mit dem sie auf ihre digitale Geldbörse zugreifen können und Transaktionen digital signieren können. Diese Private Keys sind 52 Zeichen lang und werden den Nutzer:innen zufällig zugewiesen. Geht ein solcher Key verloren, ist auch die mit dem Schlüssel verbundene Kryptowährung endgültig verloren. Daher ist die sichere Speicherung der privaten Schlüssel essenziell.

Studie liefert Designideen für Key-Management in Multi-User-Szenarien

Die Anforderungen an die sichere Verwaltung und Speicherung von kryptografischen Schlüsseln wachsen, wenn mehrere Nutzende Zugriff darauf brauchen. „Das ist zum Beispiel bei Kryptofonds standardmäßig der Fall. Seit einer Gesetzesänderung 2022 sind solche Fonds in Deutschland ein größeres Thema in Finanzinstitutionen geworden und wie bei anderen Fonds auch, werden sie meist von mehreren Mitarbeitenden gemanagt. Zudem müssen sich Mitarbeitende ja auch im Falle von Urlaub oder Krankheit vertreten können“, erklärt Guthoff. Sie hat 13 Mitarbeitende in Finanzinstituten dazu befragt, welche Sicherheits- und Geheimhaltungsanforderungen die Institute für die Schlüsselverwaltung haben und wie sich die Mitarbeitenden ein optimales Schlüsselmanagement vorstellen. „Die Ergebnisse dieser Studie können dabei helfen, Key-Managementlösungen für Finanzinstitutionen entsprechend ihrer Bedürfnisse, sicher und zugleich praktikabel zu designen.“

Eine der größten Herausforderung für das Schlüsselmanagement bei mehreren Nutzenden ist in der Praxis die Fluktuation von Mitarbeitenden. „Hatte ein Mitarbeiter einmal Zugang zu einem Schlüssel, besteht das Risiko, dass er ihn kopiert hat. Auch wenn er zwischenzeitig gekündigt hat oder auf einer anderen Stelle sitzt, kann er dann noch auf die Vermögenswerte zugreifen“, sagt Guthoff. Eine gute Lösung für dieses Problem könnte nach Ansicht einiger Studienteilnehmer:innen die Nutzung eines Programmes sein, das den Einsatz von Schlüsseln für Transaktionen ermöglicht, aber keinen direkten Zugriff auf den Schlüssel selbst zulässt. „Überhaupt wünschten sich die Teilnehmenden für die Speicherung der Schlüssel überwiegend technische Lösungen, die durch mehrere Faktoren wie TANS und Passwörter abgesichert werden können.“

Eine andere wichtige Frage ist, wie mit Haftungs- und Verantwortungsfragen umgegangen wird. Viele der Befragten stellen sich für ein optimales Schlüsselmanagement und die Verteilung entsprechender Zugriffsrechte auf Vermögenswerte Modelle vor, die der Organisationsstruktur ihres Unternehmens entsprechen. „Das heißt, dass zum Beispiel CEOs über höhere Vermögenswerte verfügen können als einfache Angestellte und erweiterte Zugriffrechte bekommen sollen“, erklärt Guthoff. Die meisten Befragten wünschten sich zudem ein Key-Management, das nicht zu viel Hintergrundwissen zu digitalen Signaturen erfordert und möglichst einfach zu bedienen ist. Einen Intermediär zwischen dem Finanzinstitut und der Handelsplattform einzuschalten, der das Key-Management und dessen Absicherung übernehmen könnte, fanden einige Teilnehmende nützlich, sofern ein entsprechendes Vertrauensverhältnis herrscht.

Viele spannende Forschungsfragen

Für CISPA-Forscherin und PhD-Studentin Guthoff ist es das erste Paper, das sie auf einer Konferenz einreicht. „Dass meine Arbeit auf der renommierten S&P; angenommen wurde, ist toll. Das bestärkt mich.“ Trotz der tiefen Einarbeitung in das Thema Kryptowährung will sich Guthoff in ihrer Forschung künftig nicht auf Finanzthemen fokussieren. „Die Arbeit an diesem Thema war super spannend, aber jetzt werde ich mich erstmal anderen Forschungsfragen zuwenden. Mich interessieren vor allem Themen, bei denen die Vorstellungen und Ansprüche von Sicherheitsforschenden und die Lebensrealitäten der Anwender:innen nicht so richtig zusammenpassen.“ Davon gibt es vermutlich noch einige.

Originalpublikation:

Guthoff, Carolyn and Anell, Simon and Hainzinger, Johann and Dabrowski, Adrian and Krombholz, Katharina (2023) Perceptions of Distributed Ledger Technology Key Management - An Interview Study with Finance Professionals. In: 44th IEEE Symposium on Security and Privacy.
Conference: SP IEEE Symposium on Security and Privacy
DOI: https://publications.cispa.saarland/3948/

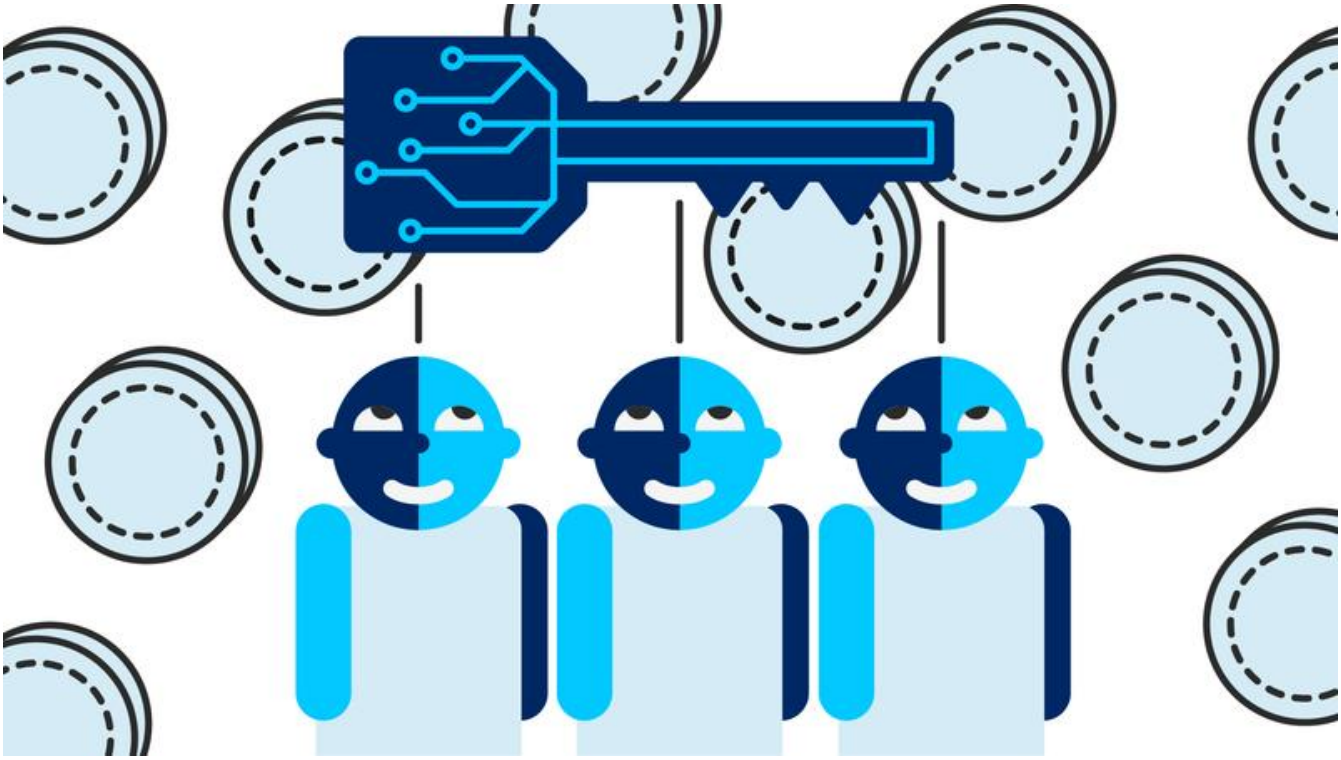

Illustration Studie Key-Management-Systeme Guthoff
CISPA