Offlinefähige Schließanlagen auf Blockchain-Basis

Robert Manthey, Richard Vogel, Matthias Vodel
Fakultät für Computer- & Biowissenschaften, Hochschule Mittweida, Deutschland

Abstract
Permission management for access of rooms, laboratories etc. is a cost and time-consuming task with common systems in large facilities. Especially, frequent changes and staff turnover need proper and efficient workflows and extensive logistics. The interconnection of common electronic locking systems with blockchain based permission data management and smartphones makes it possible to reduce the needed resources as well as entry point for tampering permissions.

Kurzfassung
Das Berechtigungsmanagement für den Zugang zu Räumen, Laboren etc. ist mit üblichen Systemen eine kosten- und zeitintensive Aufgabe in großen Einrichtungen. Insbesondere häufige Wechsel und Fluktuationen des Personals erfordern gut strukturierte und effiziente Arbeitsabläufe und eine umfangreiche Logistik. Die Verknüpfung gängiger elektronischer Schließsysteme mit Blockchain-basiertem Berechtigungsdatenmanagement und Smartphones ermöglicht es, die benötigten Ressourcen sowie die Einstiegspunkte für Manipulationen zu reduzieren.

1. Einleitung

Große Unternehmen und Institutionen verteilen sich typischerweise über eine Vielzahl an Gelände mit verschiedenen Bereichen mit jeweils spezifischen Zugangsberechtigungen für Labore, Gebäude oder Zweigstellen. In einem Gebäude kann beispielsweise der Zugang zu Raum 213 auf die Mitarbeiter einer Abteilung beschränkt werden, während das Reinigungspersonal Zugang zu allen Räumen im dritten Stock des Hauptgebäudes freitags von 17:00 bis 19:00 Uhr erhält, wie in Abbildung 1 dargestellt. Darüber hinaus können das Sicherheitspersonal sowie Personen mit besonderen Qualifikationen, alle Räume in diesem Gebäude betreten. Reguläres Personal sollten hingegen nur Zugang zu den Räumlichkeiten haben, die zur Erfüllung ihrer Aufgaben benötigen. Diese Zugangsberechtigungen werden oft mittels Schließsystemen realisiert, welche von einer Vielzahl von Herstellern mit einer Vielzahl von Systemen und Schlüsselausstattungen angeboten werden. Sie decken einen breiten Bereich an Anwendungsbereich ab und bieten bewährte Lösungen an.

Allerdings führen häufige Änderungen beim Personal oder den Berechtigungen zu einem beträchtlichen Verwaltungsaufwand und erhebliche Kosten[1] [2]. Ebenso wie bei Verlusten oder Diebstahl[3] müssen dann größere Mengen an Schlüsseln und Schlössern der betroffenen Organisationsbereiche, Abbildung 2, erneuert bzw. reprogrammiert werden. In dieser Hinsicht bieten elektronische Schließsysteme zwar erhebliche Zeit- und Kosteneinsparungen. Sie erfordern jedoch in der Regel eine Datenverbindung zwischen der Verwaltungszentrale und den betroffenen Schlössern, wodurch erhebliche Investitionen in die eingesetzte Infrastruktur notwendig sind.

Die im Rahmen dieser Arbeit erstellte Lösung kombiniert bestehende Schlösser und der damit einhergehenden Sicherheit, Leistungsfähigkeit, Flexibilität und einfachen Aktualisierbarkeit der Berechtigungsdaten mit den dezentralen, manipulationsresistenten Eigenschaften der Blockchaintechnologie, sowie den weitverbreiteten, mit beträchtlichen Speicher- und Rechenressourcen ausgestatteten Smartphones der Schließanlagennutzer.

Abbildung 1: Beispielhafte Verteilung von Schließberechtigungen (rot, grün, blau, hellblau, violett) an vier Standorten mit Gebäude, Türen und Fenster. Bestimmte Berechtigungen außerdem unterliegen zeitlichen Einschränkungen. [1]

[1] https://www.forbes.com/home-improvement/home-security/cost-to-hire-a-locksmith/
[2] https://vizpin.com/blog/access-control-pricing/
[3] https://www.verbraucherzentrale.de/wissen/geld-versicherungen/weitere-versicherungen/generalschluessel-verloren-drohende-kosten-bis-zum-preis-eines-kleinwagens-10679

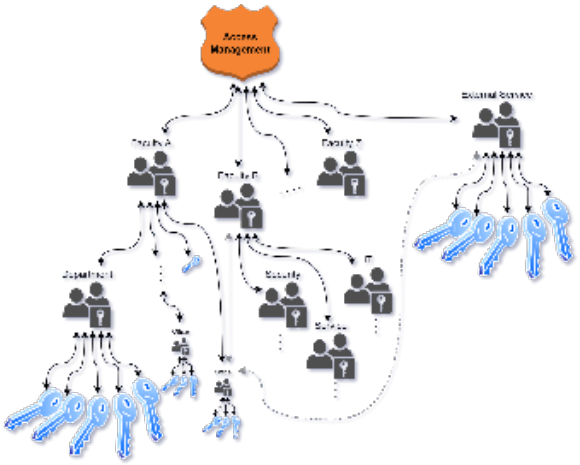

Abbildung 2: Hierarchie der Organisationsbereiche mit der Gruppierung der Zugangsberechtigungen und mehrfachen Zugehörigkeiten. Unterschiedliche Schlüssel repräsentieren die jeweiligen Berechtigungen. [7]

2. Grundlagen

Für die Steuerung des Zugangs zu Gebäuden und Räumen werden häufig klassische mechanische Schließanlagen auf Basis des berechtigten Besitzes von administrativ eingestellten Schlüsseln verwendet. Diese sind zwar vergleichsweise kostengünstig[4], aber unflexibel. Die physischen Schlüssel können unbemerkt kopiert und Kreis der Zugangsberechtigten unerlaubt erweitert werden, was nur durch den aufwändigen Austausch aller möglicherweise betroffenen Schlösser vermieden werden kann.

Elektronische Schließanlagen wie blueSmart von WINKHAUS[5] oder blueSmart von WINKHAUS[6] stellen zwar mehr Flexibilität zur Verfügung, erfordern aber entweder ein individuelles Reprogrammieren bei Änderungen und somit vertrauenswürdiges Personal und Zeit, oder permanent verfügbare Infrastruktur in Form von Kommunikation mit der Verwaltungszentrale, was beträchtliche Kosten verursacht. Lokkit[7] stellt behebt etliche dieser Nachteile zwar, nutzen aber das Smartphone des Nutzers für Verifikationsaufgaben, sodass Dritten vertraut werden muss.

Die von [4] vorgestellte Technologie der Blockchain behebt diese Nachteile und erlaubt eine gesicherte Übertragung der Berechtigungsdaten über ungesicherte Zwischenstellen und in sehr hohem Maße abgesichert gegen unentdeckte Manipulation. Daten werden hierbei in Transaktionen strukturiert und in Blöcken zusammengefasst an eine Menge von Knoten gesandt, welche daraus

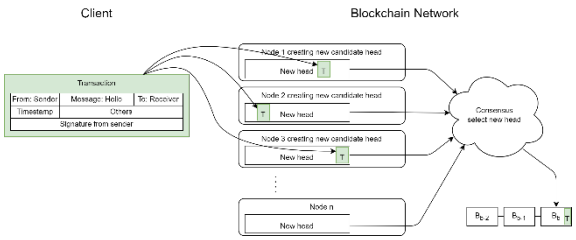

Abbildung 3: Nutz- und Metadaten als Transaktion zusammengefasst werden als Bestandteil in neue Blockkopfkandidaten kombiniert. Durch den Konsensus wird der neue Kopf gewählt und die Blockchain verlängert. [8]

einen neuen Kopf der Blockchain erzeugen. Durch die Verkettung der Blöcke wird eine Absicherung gegen Manipulation erzeugt, wie in Abbildung 3 dargestellt. Erweiterungen der Funktionalität der Blockchain-Technologie ermöglichen außerdem bedingte Transaktionsausführungen, Smart Contracts oder auch verteilte Identitätsprüfung. [2,3,5,6]

3. Realisierung

Für die Verwaltung der Schließberechtigungen, als auch für die Anforderung einer Schließaktion wurde eine auf dem Flutter-Framework[8] basierende Smartphone-App erstellt. Die Nutzer können gruppiert und so mit den notwendigen Eigenschaften des gewährten Zutritts ausgestattet werden, wie in Abbildung 4 dargestellt.

Diese Daten werden an den von der Verwaltung festgelegten Speicherplatz für die Off-Chain-Daten übermittelt, entsprechend des Workflows in Abbildung 5. Zusätzlich erfolgt die Erstellung der Sicherheitsinformationen mittels Hashes und deren Übermittlung als Transaktion an die Ethereum-Blockchain[9].

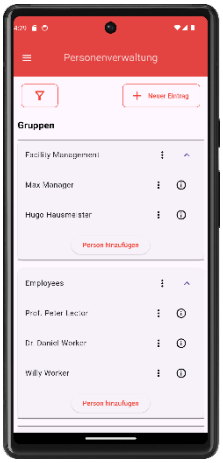

Abbildung 4: Beispiel der Gruppierung von Nutzern in Gruppen denen gleiche Schließberechtigungen zugewiesen wurden.

[4] https://kiwi.ki/schliessanlage/kosten
[5] https://www.winkhaus.com/de-de/zutrittsorganisation/elektronische-zutrittsorganisation/elektronische-schliesssysteme/bluesmart
[6] https://www.winkhaus.com/de-de/zutrittsorganisation/elektronische-zutrittsorganisation/elektronische-schliesssysteme/bluesmart
[7] https://news.hslu.ch/siemens-zeichnet-projekt-von-informatik-absolventen-aus/
[8] https://www.flutter.dev/
[9] https://www.ethereum.org/en/

Der Nutzer lädt regelmäßig die aktuellen Daten vom Off-Chain-Speicherplatz und den aktuellen Stand der Blockchain auf sein Smartphone, wenn eine Verbindung zum Netzwerk verfügbar ist. Sobald das Smartphone in Reichweite eines Schlosses ist, erfolgt eine Übermittlung der Daten des Smartphones mittels Bluetooth LE[10]. Das Schloss, welches über keine weiter Verbindungen verfügt, verifiziert die Korrektheit der empfangenen Daten und aktualisiert seine internen Daten der Zugangsberechtigten und den Stand der Blockchain. Die Eigenschaften der Blockchain und die Hashes der Daten der Zugangsberechtigten verhindern eine unerkannte Manipulation.

Mittels der App fordert der Nutzer eine Schließaktion beim Schloss an und liefert dabei die notwendigen Beweise seiner Identität, welche vom Schloss geprüft werden. Verbindungen zum Netzwerk, der Zugriffsverwaltung oder Datenspeichern ist nicht notwendig. Liegen ebenfalls die entsprechenden Berechtigungen vor, so führt das Schloss die angefragte Aktion aus.

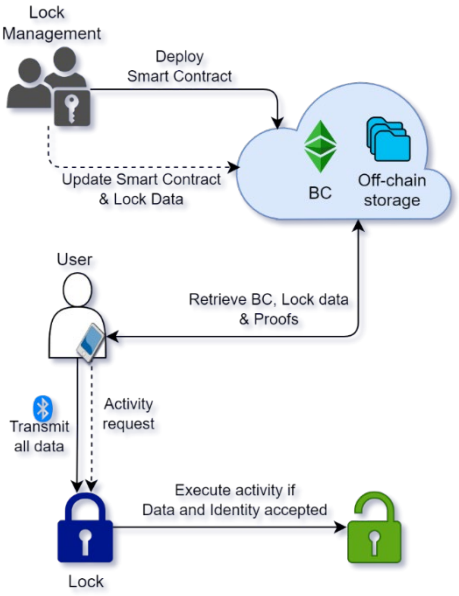

Abbildung 5: Schematischer Ablauf der Verteilung der Schließberechtigungen von der Erstellung durch das Management, über die Speicherung der Daten sowie ihrer Verifikationsinformationen in der gewählten Blockchain bis hin zum Download der notwendigen Informationen durch den Nutzer mit dem späteren Transfer zum Schloss. Hier erfolgt die Prüfung der Daten und gegebenenfalls die Aktionsausführung. [9]

4. Zusammenfassung und Ausblick

Bisherige Schließanlagen waren schwer zu aktualisieren oder benötigten zusätzliche Infrastruktur, was durch die hier vorgestellte blockchainbasierte Weiterentwicklung effizient gelöst wird. Durch die Verwendung des Smartphones des Nutzers, u.a. als Transportmedium, sind keine weiteren Komponenten erforderlich und das Schloss damit offline. Gleichzeitig ist die Aktualität der Schließberechtigungen gewährleistet. Aufgrund der Anforderungen an die Hardware sind zukünftig Optimierungen und Beschleunigungen der Datenübertragungen und des Energieverbrauchs vorgesehen.

Danksagung

Diese Arbeit wurde teilweise im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts *Chainlock - Blockchain-gestützte, smarte Schließanlagen* (Projektnr. 8233216) durchgeführt.

Literaturverzeichnis

[1] R. Manthey, R. Vogel, and M. Vodel, “Chainlock – Blockchain-gestützte, smarte Schließanlagen,” in Konferenzband zum Scientific Track der Blockchain Autumn School 2023, vol. 2. Hochschule Mittweida, p. 4.
[2] Christian Cachin and Marko Vukolić. 2017. Blockchain Consensus Protocols in the Wild. arXiv:1707.01873
[3] Md Sadek Ferdous, Farida Chowdhury, and Madini O. Alassafi. 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 7 (2019), 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
[4] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. (03 2009), 9 pages. https://bitcoin.org/bitcoin.pdf
[5] Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, and Markus Sabadello. 2021. Decentralized Identifiers (DIDs) v1.0. W3C. https://www.w3.org/TR/2021/CRD-did-core-20210529/
[6] N. Szabo. 1994. Smart Contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html
[7] R. Manthey, R. Vogel, M. Baumgart, C. Roschke, M. Ritter, M. Vodel. 2023. Decentralized Resilient Smart Lock System with Offline Capabilities – ChainLock. In Proceedings of the 16th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA) 5-7 July 2023, Corfu Island, Greece
[8] R. Manthey, R. Vogel, F. Schmidsberger, M. Baumgart, C. Roschke, M. Ritter, and M. Vodel, “Blockchain based social commitment-secure & reliable web services,” in International Workshop on Metrology for Living Environment (MetroLivEn). New York, NY, USA: IEEE, 07 2022, pp. 101–104.
[9] R. Vogel, R. Manthey, M. Baumgart, C. Roschke, M. Ritter, and M. Vodel, “Tamperproof data transmission to offline IoT devices in a zero-trust environment,” in 2024 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2024, pp. 817–822. [Online]. Available: http://www.conf-icnc.org/2024/papers/p817-vogel.pdf

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3478807/