Fakultät Angewandte
Computer- & Biowissenschaften

Prof. Dr.-Ing. habil. Matthias Vodel

**Professur Softwareentwicklung
für Medien & Anwendungssysteme**

Technikumplatz 17
09648 Mittweida

Tel.: +49 (0) 3727 / 58 – 1010
Fax: +49 (0) 3727 / 58 - 2 1010

E-Mail: vodel@hs-mittweida.de
Web: www.cb.hs-mittweida.de

Hochschule Mittweida | University of Applied Sciences
Postfach 1457 | 09644 Mittweida

Projektträger Jülich
Forschungszentrum Jülich GmbH
Postfach 61 02 47
10923 Berlin

Vorhabenbezeichnung „Chainlock - Blockchain-gestützte, smarte Schließanlagen“ Mittweida, 12.11.2025
Förderkennzeichen: 03WIR1321A
Abschlussbericht

Sehr geehrter Herr Dr. Engelhard,
sehr geehrte Frau Adelberger,

nachfolgend übersenden wir Ihnen den Projektabschlussbericht für das Förderprojekt 03WIR1321A.

1. Aufzählung der wichtigsten wissenschaftlich-technischen Ergebnisse und anderer wesentlicher Ereignisse.

Projektmanagement / Organisation

Für die Verwaltung des Projektes und zur Speicherung von Dokumenten, Konzeptunterlagen, Zuarbeiten, Ideen und generiertem Wissen wurde die Projektmanagementplattform *Confluence*[1] verwendet. Mit dem darin enthaltenen Ticketsystem können der Projektverlauf, also bisherige Arbeitsschritte, aktueller Stand und kommende Aufgaben, organsiert, Entwicklungsentscheidungen nachvollzogen und dokumentiert sowie die verfügbaren Ressourcen verwaltet werden. Durch die Beschränkung der zugehörigen Zugänge wurde die Nachvollziehbarkeit und Vertraulichkeit gewährleistet. Aufgrund der Speicherung der Tickets ist eine Historie erstellbar welche archivierbar ist. Für den Dateiaustausch mit externen Projektteilnehmern, Kooperationspartnern, interessierten Studenten und anderen Projekten wurde eine auf der Open Source Software *Nextcloud*[2] aufbauenden Lösung verwendet. Die Verwaltung von Programmquellen, Source Code, Assets, Konfigurationen der Buildumgebungen, Testdaten u.ä. wurde durch die Git-basierte Quellenverwaltungen *GitHub*[3] realisiert.
Für die Abstimmung und Koordination wurden regelmäßige Meetings in direkter Form beziehungsweise digital durchgeführt. Je nach Arbeitsschwerpunkt und Aufgabenbereich wurden hierzu sowohl Projektpartner, potenziell interessierte Kooperationspartner als auch externe Mitarbeiter im Rahmen der juristischen und technischen Betreuung eingebunden. Zur Durchführung dieser Kommunikation, speziell bei kurzfristigen Abstimmungen, kam das Videokonferenzsystem *Zoom*[4] zum Einsatz.

[1] http://www.atlassian.com/software/confluence
[2] https://nextcloud.com
[3] https://github.com
[4] https://zoom.us

partnerhochschule des spitzensports

Zertifikat seit 2009
audit familiengerechte hochschule

Use Cases Definitionen

Die Use Cases des Projektes Chainlock ergeben sich aus der Analyse der Nutzung von Schließsystemen, der dabei auftretenden Kombinationen von Schließberechtigungen (Abbildung 1) und der damit einhergehenden Optimierungspotenziale. Für die Verringerung des Verwaltungsaufwands und zur Durchsetzung und Kontrolle der Verwaltungsregeln wurde eine zentrale Konfiguration realisiert, welche die Zuordnung von Personen zu Schließgruppen und Schließgruppen zu Schlössern konfiguriert und autorisiert (Abbildung 17). Die Art des Zugangs, z.B. Normaler Schlüssel, Generalschlüssel des Bereichs, Notfallzugang etc. wird hierbei durch die Zuordnung zu entsprechenden Schließgruppen realisiert, aus deren Kombination sich die effektive Berechtigung einer Person zur Nutzung eines Schlosses ergibt. Da Nutzer meist nur zu bestimmten Zeiten, z.B. Mitarbeiter nur an Arbeitstagen und Reinigungspersonal nur an Arbeitstagen nach den regulären Arbeitszeiten, Zugang benötigen, kann dies Eingeschränkt werden und die Sicherheit verbessern. Diese zeitliche Randbedingungen werden ähnlich Terminen eines Kalenders behandelt und als weiterer Faktor an die Schließberechtigungen angehängt. Durch die Schließgruppen ist eine Abstraktion von einzelnen Nutzern gegeben, wodurch die Durchführung von Änderungen, z.B. das Hinzufügen neuer Nutzer oder das Ändern von Berechtigungen, vereinfacht wird und sich allein auf die Gruppenzuordnung beschränkt. Die Zuordnung von Schließgruppen zu anderen Schließgruppen bildet die logische Struktur der jeweiligen Einrichtung, z.B. Universität, ab und muss nur selten verändert werden. Bei Bedarf ermöglicht diese Struktur aber auch flexible Organisationsstrukturen mit beliebig viele Gruppen zur Verwaltung auch großer Schließsysteme. Die effektiven Berechtigungen zur Aktionsausführung eines Schlosses ermittelt dieses durch die Kombination der in den Schließgruppen definierten Berechtigungen.

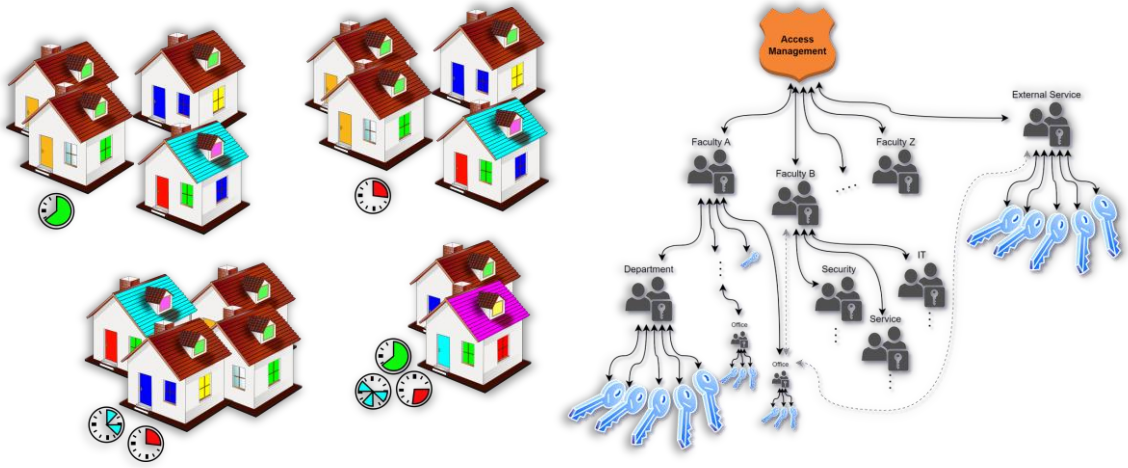


Abbildung 1: Use Cases (Links) Am Beispiel der notwendigen Schließberechtigungen einer Wohnanlage mit unterschiedlichen Kombinationen von Zugängen zu Türen und Fenstern sowie zeitlichen Einschränkungen. (Rechts) Komplexe Hierarchie der Verwaltung von Schlüsseln in größeren Einrichtungen mit Abteilungen und Fakultäten, einzelnen Generalschlüsseln sowie mit sich überschneidenden Berechtigungsbereichen.

Die kosteneffiziente Verwaltung der Schließregeln bei gleichzeitiger Sicherstellung der Anforderungen an die Korrektheit und Authentizität der Daten erfordert deren Aufteilung. Die Speicherung der potenziell umfangeichen Schließregeln erfolgt verschlüsselt und kostengünstig in einem vom Betreiber der Schließanlage festgelegten Cloudspeicher (Off-Chain). Die Informationen Manipulationsabsicherung, zur Verifikation und zur Bestätigung der Authentizität fließen hingegen als Teil von Blöcken in die verwendete öffentliche Blockchain (Ethereum Classic) ein. Diese sind unabhängig vom Umfang der Schließregeln und bleiben somit ebenfalls kostengünstig. Gleichzeitig sind die Auswirkungen von Ausfällen und Angriffen signifikant verringert sowie eine Unabhängigkeit vom Hersteller der Schließanlage realisiert. Nutzer mit eigener Serverinfrastruktur können ihre Daten lokal speichern und so die volle Kontrolle über ihre Informationen sicherstellen. Alternativ besteht die Möglichkeit, externe Speicherdienste wie Google Drive oder Nextcloud zu nutzen.
Autorisierte Nutzer verwalten ihre Identitäten in der Schließapp in Form von Schlüsseln, welche sie nach eigenem Ermessen, z.B. entsprechend ihrer Funktion als Büromitarbeiter oder als Maschinentechniker, anlegen und nutzen können. Gegenüber der Verwaltung der Schließanlage identifizieren sie sich mit einem gewählten Schlüssel und die entsprechenden Schließberechtigungen werden dieser Identität bzw. der Berechtigungsgruppe zugeordnet. Dies Abstrahiert die Person von ihren jeweiligen Funktionen, ermöglicht eine effizientere Verwaltung und einen unterbrechungsfreien Ersatz im Bedarfsfall. Gleichzeitig bleiben die für die Identitätsverifikation notwendigen Informationen lokal auf dem Gerät, damit in der Hoheit des Nutzers. Somit sind, speziell größer angelegte Angriffe signifikant erschwert.
Sobald ein Smartphone eine Internetverbindung herstellen kann, sowie in regelmäßigen Intervallen, aktualisiert die Schließapp des Nutzers den bisher bekannten Datenstand der Schließberechtigungen und der Blockchain (Abbildung 17). Durch anschließende Bewegung des Nutzers gelangt das Smartphone in Reichweite für eine Verbindung zu einem Schloss, welches die Aktualisierungen vom Smartphone übermittelt bekommt und somit selbst über keine Infrastruktur verfügen muss. Das Schloss aktualisiert daraufhin den eigenen Stand der entsprechenden Berechtigungen, die Kenntnisse zum Stand der Blockchain, die aktuelle Zeit sowie weiterer Parameter. Andere Nutzer mit späteren Datenupdates führen zum gleichen Aktualisierungsvorgange, wohingegen veraltete oder fehlerhafte Datenstände ignoriert werden. Auf diese Weise führen auch die Nutzer zu Datenupdates, welche das entsprechende Schloss nicht benutzen wollen. Diese Vielzahl an unterschiedlichen, schwer beeinflussbaren Updatepfaden erhöhen die Sicherheit des Systems weiter.
Ein schließwilliger Nutzer verwenden die entsprechende Funktion der Schließapp seines Smartphones, welches dazu explizit mit dem entsprechenden Schloss kommuniziert und weist die Identität des Nutzers nach. Das Schloss prüft die Schließberechtigungen bezüglich der Nutzeridentität und führt die Schließaktion aus. Ist der Identitätsnachweis des Nutzers fehlerhaft, älter als vorgegeben, keine passende Schließberechtigung des Nutzers für dieses Schloss bekannt oder der aktuell bekannt Datenstand zu alt, so erfolgt keine Schließaktion.

Hieraus ergeben sich die in Abbildung 2 dargestellten Hauptkomponenten des im Projekt realisierten Schließsystems mit den für ihre Umsetzung typischen Eigenschaften und Technologien. Das Zusammenspiel dieser Hauptkomponenten bei der Durchführung eines modernen, digitalgestützten, blockchainbasierten Schließvorgangs erfolgt entsprechend des in Abbildung 3 dargestellten Ablaufs und trägt maßgeblich zur Sicherheit, Nachvollziehbarkeit und Benutzerfreundlichkeit bei.

Abbildung 2: Die vier Hauptkomponenten des Schließsystems mit ihren zentralen Eigenschaften.

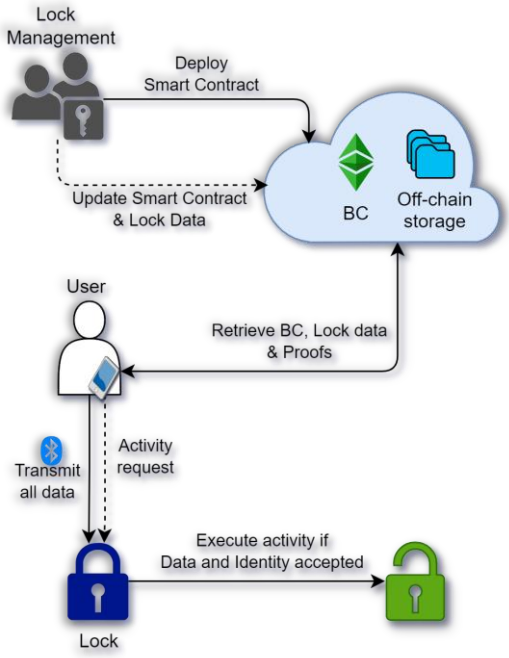


Abbildung 3: Ablauf mit der Verwaltung von Berechtigungen, der Blockchain (BC) und dem Speicher der verschlüsselten und gesicherten Berechtigungsdaten (Off-Chain-Storage). Mittels periodischen Downloads der Regeln auf das Smartphone des Benutzers und deren spätere Übermittlung zum Schloss erhält dieses zuverlässig Aktualisierungen der Regeln. Bei Anforderung einer Schließaktion prüft das Schloss die Identität des Nutzers und die Zulässigkeit der Aktion und führt die gewünschte Aktion gegebenenfalls aus.

Dieser Prozessablauf sowie die Randbedingungen der beteiligten Systeme wurden mit der juristischen Begleitung des Projektes abgestimmt, um rechtlich aufwendige und schwer handhabbare Folgen während des Betriebes zu minimieren.

Technologie & Hardware

Im Berichtszeitraum wurde die Bearbeitung der Kernbereiche durchgeführt, welche die Verwaltung der Schließberechtigungen, die vom Anwender einzusetzende smartphonebasierte Schließapp sowie die im Schloss integrierte Steuerhardware umfasst.

Die Verwaltung umfasst dabei mehrere Teilbereiche. Den ersten Teilbereich stellt die Erstellung neuer Benutzerkonten bzw. deren Registrierung dar, wofür eine zentrale Verwaltungsplattform oder eine Integration der Verwaltungsfunktion in einen gesicherten Bereich der Schließapp zu realisieren ist (Abbildung 17). Jeder Nutzer wird dabei eindeutig identifiziert und fundamentale Daten wie beispielsweise die E-Mail-Adresse, der Name, und die im System eindeutige Nutzer-ID erfasst. Von Seiten des Nutzers erfolgt die Erstellung eines digitalen Schlüsselpaars unter Verwendung des international verbreitetes, quelloffenen und herstellerunabhängigen, auf asymmetrischer Kryptographie basierenden Public-Key-Authentifizierungsverfahrens Ed25519 (RFC 7748). Die Funktionalität hierzu ist in der Schließapp integriert und erlaubt die Erstellung beliebiger Anzahlen an Schlüsselpaaren, entsprechend den unterschiedlichen Funktionen im Unternehmen, für unterschiedliche Bereiche, dem unterbrechungsfreien Ersatz alter Schlüssel oder ähnlicher Anforderungen. Der geheime Schlüsselteil verbleibt dabei gesichert beim Nutzer und der öffentliche Schlüsselteil kann an die Verwaltung übertragen werden. Diese verknüpft den öffentlichen Schlüsselteil als Bestandteil der Daten mit der Nutzer-ID, wodurch dieser Nutzer sich gegenüber dem System authentifizieren kann.

Der zweite Teilbereich definiert die Zuordnung der registrierten Nutzer zu den Schlössern (Abbildung 4), welche benutzt werden dürfen, um Zugang zu bestimmten Standorten, Gebäuden, Abteilungen, Räumen etc. zu erhalten. Um ein effektives und effizientes Management auch größerer Schließanlagen mit vielen Abteilungen und Verantwortungsbereichen realisieren zu können, wurde dieser Verwaltungsbereich an das Prinzip des Gruppen- und Rollenmanagements gemäß *Role Based Access Control* (RBAC, ANSI-Norm 359-2004) angelehnt, welches zur Zugriffskontrolle bereits in vielen Betriebssystemen und international verbreiteten Softwarelösungen seit Jahrzehnten etabliert ist. Dabei erhalten einzelne Nutzer üblicherweise selbst keine Berechtigungen, werden aber bestimmten Gruppen zugeordnet. Diese Gruppen abstrahieren vom einzelnen Nutzer und fassen mehrere Nutzer mit gleichen Anforderungen zusammen, wodurch eine Vereinfachung der Organisation sowie der Verbesserung der Übersichtlichkeit und Durchsetzungsfähigkeit von z.B. den Sicherheitsrichtlinien von Unternehmen erreicht wird. Die Gruppen wiederum werden festgelegten Rollen zugewiesen, z.B. *Mitarbeiter Abteilung A*, *ID-Administrator Abteilung B*, *Heizungstechnik Gebäude M*, *Externer Dienstleister Fenster Gebäude F* oder auch *Inneneinrichter Raum 3/26*. Diese Rollen abstrahieren die Strukturen, Organisationsbereiche etc. von einzelnen Einrichtungen, Gebäude, Räumen, Abteilungen usw. und fassen mehrere Teile mit gleichen Zugangsregelungen zusammen. Die konkreten Schließberechtigungen der einzelnen Schlösser werden dann den Rollen zugewiesen. Zusätzlich werden die zeitlichen Einschränkungen definiert, etwa die Gültigkeit an *Werktagen zwischen 8 und 18 Uhr für die Mitarbeiter der Abteilung A* oder für die *Inneneinrichter des Raums 3/26 vom 1.3.2025 bis zum 26.4.2025 jeweils von 6 bis 22 Uhr* wie in Abbildung 17 gezeigt. Um

diese zeitliche Randbedingungen umzusetzen, werden diese ähnlich Terminen eines Kalenders behandelt, wobei ein an *xCal* (RFC 6321) angelehntes Format zum Einsatz kommt.

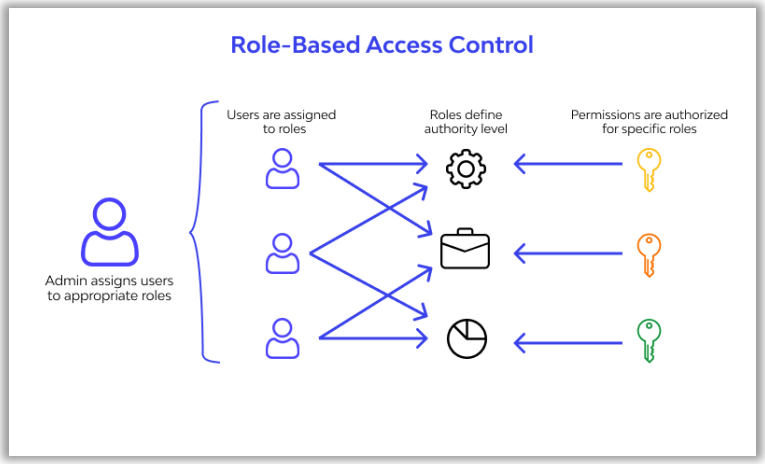


Abbildung 4: Beispiel einer Zuordnungsstruktur von Nutzern zu Rollen, um Zugriff zu bestimmten Objekte zu ermöglichen.

In ähnlicher Weise erfolgt im Teilbereich Drei das Hinzufügen neuer Schlösser zum Schließsystem. Die grundlegenden Daten zum neuen Schloss wie ID, Bezeichner und Standort werden von der Schlossverwaltung angelegt. Das uninitialisierte Schloss wird durch direkte Verbindung mit grundlegenden Daten zum Schließsystem, der verwendeten Blockchain, den zugehörigen Identifikationsdaten, seiner ID, der aktuellen Uhrzeit und weiteren Einstellungen bespielt. Anschließend kann der Einbau des Schlosses am vorgesehenen Standort und dessen Nutzung erfolgen. Aktualisierungen können nur noch mit Autorisierung durch die Schließanlagenverwaltung durchgeführt werden.

Der Teilbereich Vier deckt die Änderung bzw. Löschung von Schließberechtigungen ab. Durch die Anlehnung an die rollenbasierte Zugriffskontrolle (RBAC), erfolgen Änderungen der Zugangsberechtigungen nicht auf der Ebene einzelner Nutzer, sondern über die Zuweisung und Anpassung von Gruppen bzw. Rollen. Wird ein Nutzer z.B. aus der Gruppe *Eingänge Gebäude L* entfernt und diese Gruppe wurde entsprechend RBAC-Empfehlungen definiert, so ist ein Zugang nicht länger möglich, da alle Schlösser an Eingängen zum Gebäude L die entsprechenden Schließanfragen ablehnen. Ändert der Betreffende seine Funktion, z. B. durch Abteilungswechsel, wird die alte Rolle entfernt und eine neue zugewiesen. Dadurch erhält der Benutzer automatisch den passenden Satz an Zutrittsrechten für seine neue Position. Der manuelle Abgleich einzelner Türen oder Zeiten entfällt, was Fehlerquellen reduziert und die Sicherheit erhöht. Durch diese Strukturierung wird die Übersichtlichkeit der Regelungen verbessert und die Durchführung von Änderungen meist beträchtlich vereinfacht.
Die Informationen bezüglich dieser Änderungen der Schließregeln werden in einem aktualisierten xCal-artigen Eintrag, ein digitaler Fingerabdruck davon erzeugt und gesichert an das Schloss übermittelt. Dieses verifiziert die Korrektheit, wertet die Informationen aus und aktualisiert seine internen Speicher. Werden einem Nutzer alle Gruppenzugehörigkeiten entzogen, so ist auch eine weitere Nutzung der Schließanlage nicht mehr möglich und der Nutzer praktisch gelöscht. Erfolgen Veränderungen im

Bereich der Organisationsstruktur, einer Menge an Schlössern, an den Sicherheitslichtlinien o.ä., so können die der zugehörigen Rolle zugewiesenen Rechte zentral angepasst werden. Beispielsweise kann für die Rolle *Reinigungspersonal* der Zugang zu bestimmten Bereichen eingeschränkt oder zeitlich begrenzt werden. Alle Gruppen, und alle zugehörigen Nutzer, die dieser Rolle zugeordnet sind, übernehmen automatisch die neuen Berechtigungen, ohne dass individuelle Berechtigungen bearbeitet oder physischen Schlüssel ausgetauscht werden müssen.

Für den Transfer der Daten mit den Schließberechtigungen sowie weiterer Informationen wurde im Teilbereich Fünf eine Anbindung an existierende, externe Speicherlösungen (Off-Chain-Storage) wie Google-Drive und Nextcloud sowie die Bereitstellung als QR-Code umgesetzt (ISO/IEC 18004:2006). Ein sicherer kryptographischer digitaler Fingerabdruck der Daten wird mit dem etablierten Verfahren *SHA256* (RFC 6234) erstellt und als Bestandteil von Transaktionen in den Blöcken der Blockchain gespeichert (Abbildung 5). Diese öffentlich zugänglichen Daten stellen einerseits die Aktualität der Berechtigungen und andererseits die Robustheit gegen unbemerkte Manipulation sicher.

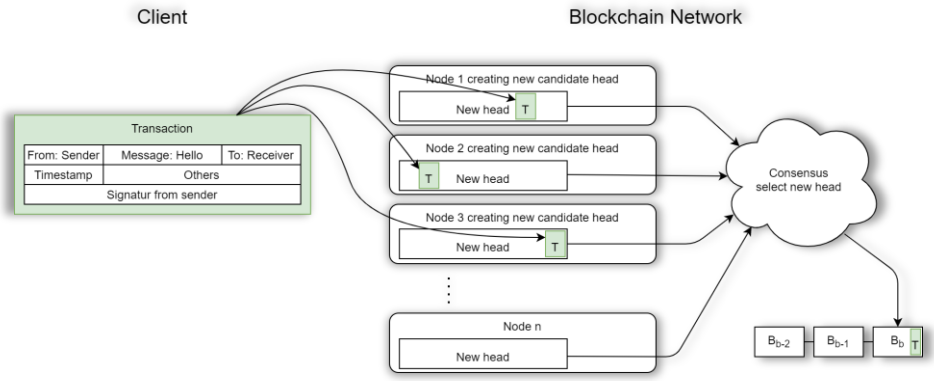


Abbildung 5: Prinzipieller Ablauf der Blockchain mit Transaktionserstellung, Blockbildung, Kandidatenauswahl und Anhängen eines neuen Kopfblocks.

Die Verwendung der externen Speicherlösung erlaubt zum einen die kosteneffiziente Sicherung der Schließregeln und weiterer Daten, welche einen beträchtlichen Umfang annehmen können. Zum anderen kann dies die vollständige Kontrolle über die Komponenten des Schließsystems realisieren, falls vom Schließanlagenbetreiber gewünscht. Aufgrund der Speicherung der vom Umfang her im Wesentlichen konstanten digitalen Fingerabdrücke als Transaktionen in den Blöcken der Blockchain bleiben die damit verbundenen Transaktionskosten gering. Gleichzeitig verringert diese Trennung die Angriffsfläche und erschwert erfolgreiche Attacken signifikant.

Die Speicherung der digitalen Fingerabdrücke der Schließberechtigungen in der Blockchain erfolgt als Bestandteil von Transaktionen, welchen weitere Metadaten, wie Zeitstempel, Absender, digitale Unterschriften etc. hinzugefügt werden (Abbildung 5). Dabei ist jede Transaktion dem *Smart Contract*[5]

[5] https://en.wikipedia.org/wiki/Smart_contract

zugeordnet, welcher die Zuordnung zur betreffenden Schließanlage und der autorisierten Verwaltung herstellt. Die Transaktion wird mittels des Internets an mehrere, zufällig gewählte Knoten des global verteilten Blockchainnetzwerks übermittelt, welche mehrere Transaktionen zusammenkombinieren und um blockspezifische Metadaten wie z.B. den Fingerabdruck des bisherigen Blockchain-Kopfes ergänzen. Jeder dieser Blöcke nimmt als Kandidat eines neuen Kopfblocks am *Consensus*-Auswahlverfahren teil. Das Verfahren bestimmt einen als neuen Kopfblock und erweitert damit die Blockchain.

Die zufällige Verteilung der Transaktionen und die Eigenschaften des Consensus sichern die Übermittlung der Daten gegen Manipulation. Durch die Verkettung mit den vorherigen Blöcken ist deren unerkannte Manipulation unmöglich und die darin enthaltenen Transaktionen mit Schließregeln sind abgesichert. Die weltweite Verteilung wiederum macht eine Behinderung der Datenverteilung äußerst aufwendig. Für die prototypische Realisierung wurde die weltweit verteilte Blockchain *Ethereum Classic* (ETC)[6] genutzt, da diese die notwendigen Eigenschaften und Fähigkeiten bietet.

Die smartphonebasierte Schließapp (Abbildung 17) basiert auf dem Open Source Software Framework *Flutter*[7], das Anwendungen in der Programmiersprache Dart plattformunabhängig entwickelt und ohne großen Anpassungsaufwand für verschiedene Zielplattformen wie Android, iOS, Linux oder auch als Webanwendung erstellen kann. Diese dient dem Nutzer zur Anforderung von Schließaktionen und zur Verwaltung der Identitäten bzw. der dafür notwendigen kryptographischen Schlüsseldaten, sowie der Daten bezüglich der verwendeten Blockchain und der verwendeten externen Speicherlösung. Um verschiedene Rollen, wie Mitarbeiter, Notfall Administrator o.ä., zu ermöglichen können mehrere kryptographische Schlüssel erstellt und mit entsprechenden Rechten versehen werden. In der prototypischen Umsetzung ist ein gesonderter Bereich zur Verwaltung der Schließanlage integriert. Für die Registrierung des Nutzers bei der Verwaltung der Schließanlage ist die Erstellung eines digitalen Schlüsselpaares des auf asymmetrischer Kryptographie basierenden Public-Key-Authentifizierungsverfahren notwendig, wofür eine eigene Seite in der App erstellt wurde. Der private Schlüsselteil verbleibt dabei beim Nutzer und dient als digitaler Nachweis der Identität. Der öffentliche Schlüsselteil kann hingegen auf unterschiedlichen Wegen verteilt werden, z.B. als QR-Code. Diese Codes sind international verbreitet, standardisiert (ISO/IEC 18004:2006) sowie mit vielen Lesegeräten und Smartphones lesbar. Auf diese Weise ist eine manipulations- und angriffssichere Übermittlung zur Verwaltung sichergestellt.

Außerdem realisiert die App die Zwischenspeicherung der Schließberechtigungen durch den automatisierten Download der Daten der externen Speicherlösung sowie des aktuellen Standes der verwendeten Blockchain. Dies erfolgt in regelmäßigen Intervallen, deren Dauer auf der Einstellungsseite der Schließapp angepasst werden kann. Eine explizite Nutzeranforderung ist möglich, erfordert aber ebenso wie die automatisierte Zwischenspeicherung eine bestehende Internetverbindung. Unabhängig von einer Internetverbindung kontaktiert die Schließapp alle Schlösser dieser Schließanlage in Reichweite über eine Bluetoothverbindung und übermittelt die aktuellen Daten zu Schließberechtigungen. Aufgrund der Kenntnis des letzten eigenen Datenstandes besteht nur die Notwendigkeit die seither hinzugekommenen Updates zu laden, wodurch der Datenverkehr sparsame

[6] https://ethereumclassic.org
[7] https://flutter.dev

und effizient stattfindet und andere Dienste nicht beeinflusst. Spezielle Vorkehrung zur Sicherung der Datenintegrität sind in der Schließapp nicht notwendig, da nur das Schloss die Daten auswerten und die Schließentscheidung trifft. Die geladenen Daten verbleiben auf dem Gerät und werden bei späterer Gelegenheit an die Schlösser des Schließsystems übermittelt. Um eine zuverlässige Kommunikation zwischen den verschiedenen Komponenten des Schließsystems zu realisieren, wurden etablierte Protokolle und Werkzeuge eingesetzt, welche eine sichere und skalierbare Datenübertragung gewährleisten. Die Anbindung an die verwendete Blockchain erfolgt über die Internetverbindung mittels der einsatzerprobten Open Source Software Geth[8]. Für die Kommunikation zwischen der Schließapp und den Schlössern wird Bluetooth Low Energy (BLE) verwendet. Dies bietet eine energieeffiziente Verbindung bei gleichzeitig ausreichender Datenrate und Sicherheit. Über definierte GATT-Profile[9] werden dabei Zugriffsbefehle, Statusinformationen und Rückmeldungen zwischen Smartphone und Schloss ausgetauscht. Gleichzeitig wird eine hohe Kompatibilität und Verbreitung mit gängigen Mobilgeräten und ein geringer Energieverbrauch sowohl auf Schloss- als auch auf App-Seite realisiert. Das darin eingebettete Protokoll zum Austausch der Authentifizierungsdaten des Nutzers und somit seiner Identifizierung für eine Schließaktion lehnt sich dabei an das seit Jahrzehnten erprobte und weltweit verbreite *Secure Shell Authentication Protocol* (RFC 4252) an. Dies gestaltet Kommunikationsschnittstellen und unterstützt die Realisierung von Modularität, Fehlerbehandlung und Zustandsverwaltung sowie die wichtige Trennung von Zustands- und Steuerinformationen auf der Ebene des Authentifizierungsprozesses mit klaren Schnittstellendefinitionen. Durch die Anlehnung an bereits erprobte und weltweit etablierte Standards wie RBAC, xCal, QR-Code und die Ethereum-Blockchain ist prinzipiell ein herstellerunabhängiger Datenaustausch und die Verwendung existierender, meist Open Source basierter Softwarekomponenten möglich. Dies verbessert die Zuverlässigkeit, Stabilität und Betriebssicherheit bei gleichzeitig hoher Interoperabilität und Transparenz. Durch die Unabhängigkeit von kommerziellen Herstellern können neue Funktionen, aber auch Fehlerbehebungen, schnell umgesetzt werden.

Die Nutzung von QR-Codes zur Übermittlung digitaler Daten als äußerst effektive Methode wurde auch in der Schließapp verwendet, da so eine schnelle, kontaktlose, abhörsicher und medienbruchfreie Übermittlung wichtiger Daten wie IDs, Konfigurationsparameter oder auch öffentliche Schlüssel realisierbar ist. Hierzu können diese als Bild auf dem Display angezeigt und vom Zielgerät mittels Scanner gelesen werden (Abbildung 17). Da der Code auf einem standardisierten, maschinenlesbaren Format (ISO/IEC 18004:2006) basiert, ist die Wahrscheinlichkeit von Übertragungsfehlern sehr gering. Die integrierte Fehlerkorrektur (Reed-Solomon-Kodierung) ermöglicht zudem das Auslesen des Codes selbst bei teilweiser Beschädigung, Verdeckung, Verschmutzung oder ungünstigen Lichtverhältnissen. Somit ist diese Übertragungsmethode besonders robust und zuverlässig im praktischen Einsatz. Außerdem entfällt der Bedarf an gedruckten Ausweisen, Papierlisten oder anderen physischen Übertragungsmedien, wodurch sich sowohl der Material- und Energieverbrauch als auch logistische Aufwände und die Menge an Abfällen reduzieren.

Die Integration der Verwaltungsfunktionalität als gesonderte Bereich für berechtigte Personen in die Schließapp erlaubt es diese Aufgaben auch ortsunabhängig durchzuführen, etwa bei temporären

[8] https://geth.ethereum.org
[9] https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

Änderungen oder im Notfall. Gleichzeitig entfällt die Notwendigkeit separater Verwaltungssoftware oder stationärer Zugriffspunkte, was sowohl den Schulungsaufwand als auch die IT-Infrastruktur reduziert. Strukturell erfolgt eine weitere Unterteilung in Bereiche zur Verwaltung von Benutzern, Gruppen und Rollen, der Zuweisung bzw. dem Entzug von Schließberechtigungen als auch dem Einrichten neuer Schlösser.

Die Steuerung der Schlösser durchlief mehrere Iterationen, mit dem zentralen Ziel der schrittweisen Miniaturisierung. In jeder Entwicklungsstufe wurde sowohl die technische Funktionalität weiter verfeinert als auch die physische Bauform verkleinert, um schlussendlich einen kompakten, knaufgroßen Prototyp zu realisieren, der sich direkt in marktübliche Türsysteme integrieren lässt.

Zu Beginn wurden auf Basis der funktionalen Anforderungen ein erstes Konzept erstellt (Abbildung 6), welches wesentliche Akteure und Komponenten des Chainlock-Schließsystems sowie ihre gegenseitigen Interaktionen darstellt. Die wesentlichen Bauteile für die Umsetzung, wie Steuerungseinheit, Energieversorgung, Bluetooth-Modul, mechanische Aktoren oder smartphonebasierte Schließapp liegen konzeptionell vor. Die detaillierte Ausgestaltung sowie Details und Randbedingungen möglicher Umnutzungen, Anpassungen oder Weiterentwicklungen bestehender Systeme, z.B. vom Projektpartner sind noch zu untersuchen bzw. zu verifizieren. Die erste Planung orientierten sich noch nicht an der späteren Form, sondern dienten vorrangig dem Funktionsnachweis und dem Abgleich technischer Abhängigkeiten.

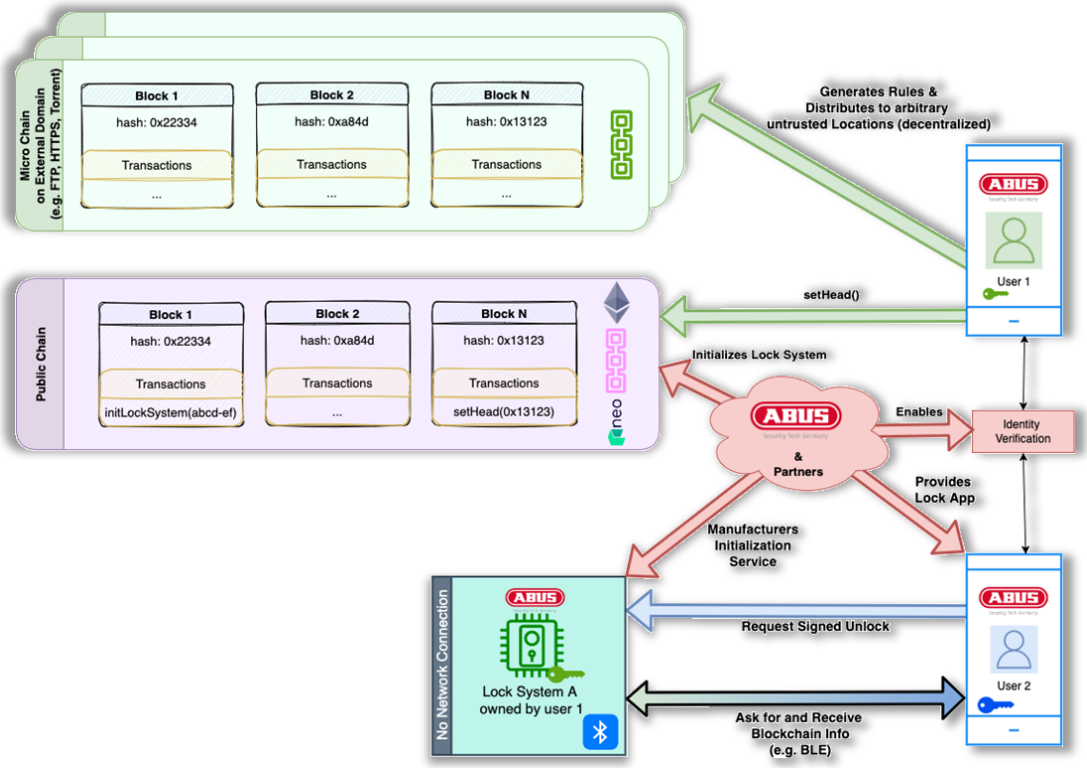


Abbildung 6: Skizze des Chainlock-System. Das Schließsystem hat hierbei keinerlei Netzwerkverbindung und der Besitzer / Administrator benötigt dennoch keinerlei physischen Zugang zur Wartung. Alle benötigten Informationen werden sicher über einen eigentlich unsicheren Kanal (schließender Nutzer) übermittelt.

Im Verlauf ersten Komponentenprobungen musste der präferierte und zunächst eingesetzte *Arduino Nano 33 BLE Sense Rev1* durch einen leistungsfähigeren *Teensy 4.1*[10] in Kombination mit einem zusätzlichen Bluetooth-Modul ersetzt werden. Dieser Schritt war notwendig, da der Arduino Nano BLE Sense trotz seiner Kompaktheit, der BLE-Funktionalität und der integrierten Funktionen in mehreren zentralen Bereichen, speziell der Programmierbarkeit, nicht den geforderten technischen Anforderungen genügte. Die erste reale Umsetzung bestand neben diesem Austausch aus handelsüblichen Komponenten auf Steckbrettern mit offenen Verdrahtungen, um effizient unterschiedliche Konfigurationen der Hardware und vor allem auch komplexe Fehlerdiagnosen durchführen zu können (Abbildung 7).

[10] https://www.pjrc.com/store/teensy41.html

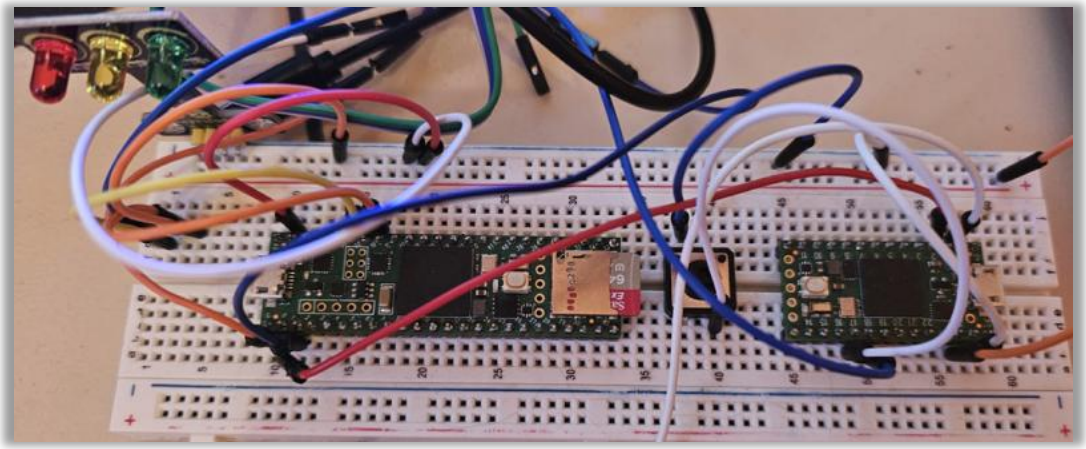


Abbildung 7: Erste Entwicklungsumsetzung der Hardware eines Chainlock-Schlosses auf einem Steckbrett. (Links) Die Hauptplatine mit Prozessor, internem Arbeitsspeicher, SD-Kartenslot und Verkabelung zum (Rechts) Bluetooth-Modul, (Mitte) einem Buzzer für akustische Rückmeldungen und (Oben Links) Farbige Lampen zur visuellen Rückmeldung.

Dieser Stand realisierte die Grundfunktion (z. B. Verarbeitung der Blockchain- und Berechtigungsdaten, Öffnen per App via Bluetooth), war mit einer Abmessung von 16x5x3cm jedoch deutlich größer als das spätere Zielprodukt. Sie dienten der Validierung von Kommunikationswegen, der Ansteuerung der Aktoren, dem Stromverbrauch und der Bearbeitungs- und Reaktionszeiten. Diese auf zwei Komponenten verteilten Realisierung sollte den beim Projektpartner verwendeten, erprobten und energieeffizienten *Nordic NRF52832*-Chip für die Bluetoothverbindung und die direkte Schließzylindersteuerung einsetzen. Dessen Programmierdetails unterschieden sich nach der Komponentenprobung jedoch in essenziellen technischen Bestandteilen ebenfalls so massiv, dass fundamentale Änderungen an der Hardwareprogrammierung, aber auch an der Umsetzung der Schließapp sowie der Blockchainanbindung hätten erfolgen müssen. Der Ersatz durch das weit verbreitete und kostengünstige Bluetooth Low Energy-Modul *Adafruit Bluefruit LE UART Friend* vermied diese Änderungen. Allerdings waren zum einen etliche Erprobungen erforderlich, da die Funktionalität zwar vorhanden war, die Programmierung aber teilweise anders als dokumentiert erfolgen musste. Zum anderen erzwang dieser Ersatz die Notwendigkeit die Ansteuerung des Schließzylindermotors durch den Teensy zu realisieren. Die Erprobungen und weitere Zwischenstände lieferten wichtige Erkenntnisse zur räumlichen Anordnung, der Wärmeentwicklung und dem Energieverbrauch.
In weiteren Entwicklungsschritten wurden kompaktere Aufbauten mit Lochrasterplatinen, festerer Verdrahtung und optimierter Anordnung realisiert. Ein Display zur Darstellung wichtiger Verarbeitungs- und Diagnoseinformationen, zusätzliche RAM sowie die Ansteuerung des Motors wurde hinzugefügt (Abbildung 8). Dieser wichtige Zwischenstand basiert somit auf dem Teensy 4.1 mit *ARM Cortex-M7* Prozessor mit 600 MHz, einer langsamen SD-Card zur Datenspeicherung und den zusätzlichen 128 MB *NAND Flash* für Zwischenergebnisse. Das Bluetooth Modul *Adafruit Bluefruit LE UART Friend* realisiert die Kommunikation mit der Schließapp und das Display gibt Informationen zum Schlossstatus aus. Der vom

Projektpartner im Produkt *wAppLoxx*[11] (Abbildung 9) bereits verwendeten Motoren zur Schließzylindersteuerung funktioniert ebenso wie die *CR2 3V*-Batterie zur Lieferung der für den Betrieb aller Bestandteile notwendigen Energie. Die für die Hardwarerealisierung des Chainlock-Schlosses notwendigen Komponenten sind somit in einer kompakten Bauform umgesetzt und im Zusammenspiel mit der Schließapp, der Blockchain und dem externe Speicherdienste als Gesamtsystem erprob- und demonstrierbar.

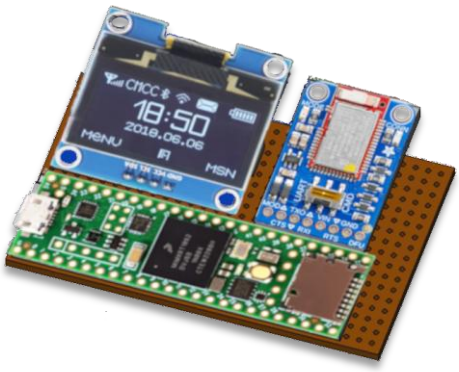


Abbildung 8: Entwicklungsprototyp mit Teensy 4.1 mit SD-Card und Flash (unten), Bluetooth Modul (rechts) und Display (links oben). Die Batterie und Verkabelung finden sich auf der Unterseite der Trägerplatte.

Abbildung 9: ABUS wAppLoxx als Beispiel eines kommerziell vertriebenen Schlosses mit kompletter Elektronik und widerstandsfähigem Stahlgehäuse (Linker Teil) an einem Schließzylinder (Mitte).

Die Abmaßen von 8x5x3 cm, eine Prüfung der Blockchaindaten von jeweils über 20 Sekunden und ein erhebliche Energieverbrauch beschränkten diesen Stand allerdings noch auf prototypische Schlosstypen mit größerer Bauform wie in Abbildung 10 dargestellt und auf dem Demonstratortag 2024 präsentiert.

[11] https://www.abus.com/de/Gewerbe/Zutrittskontrolle/wAppLoxx-System

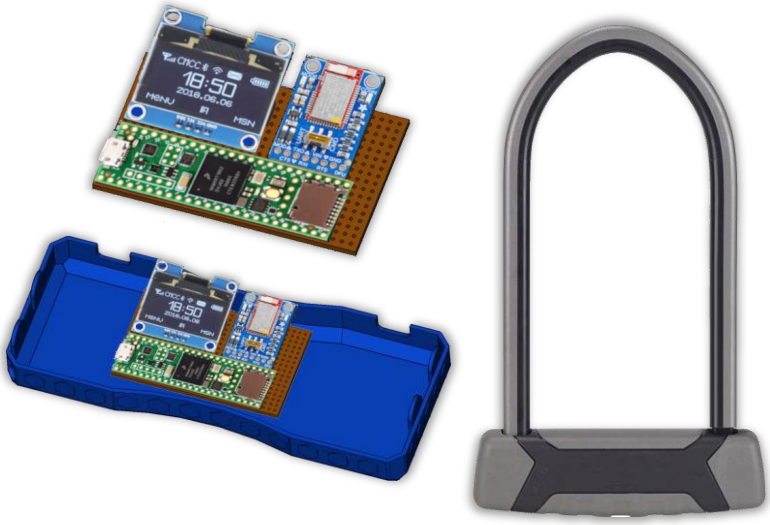


Abbildung 10: (Links oben) Entwicklungsprototypen mit Teensy 4.1, Bluetooth-Modul und Display. (Links unten) Beispielintegration in die Schlosskomponente eines Fahrradbügelschlosses (Rechts) Darstellung eines kommerziell vertriebenen Fahrradbügelschlosses mit konventionellem Schließzylinder.

Aufbauend auf diesem Demonstrationsmuster ist eine Reihe gezielter Weiterentwicklungs- und Optimierungsmaßnahmen sowohl auf technischer als auch auf funktionaler Ebene möglich. Die dafür eingesetzten handelsüblichen Komponenten sind flexibel und für ein breites Spektrum an Einsatzmöglichkeiten und Anwendungsgebiete ausgelegt. Für den im Projekt angestrebten Einsatz zur Verarbeitung von Blockchaindaten, der Bluetoothkommunikation mit der Schließapp und der Steuerung des Schließzylindermotors ist allerdings nur eine spezifische Teilmenge notwendig. Ebenso sind die bisher verwendeten Verbindungen mittels Kabel durch angepasste Platinen ersetzbar. Nicht benötigte Anschlüsse für CAN-Bus, Ethernet oder Audio sowie einige LEDs können entfallen. Eine Veränderung der Positionierung der benötigten Elektronikbauteile in Kombination mit einem adaptierten und kompakter ausgeführten Platinenlayout realisieren die in Abbildung 11 und Abbildung 12 dargestellte mehrlagige Anordnung, deutliche Einsparungen beim Energieverbrauch und eine Beschleunigung der Prüfung der Blockchaindaten auf rund 3 Sekunden. Für eine material- und kostenoptimierte Fertigung wurden im Platinenlayout beide Lagen als eine produziert, deren Auftrennung erst nach dem Bestücken der Platine mit den mikroelektronischen Bauteilen erfolgt (Abbildung 12 rechts).

Im Rahmen der Layoutentwicklung wurden, laut Dokumentation geeignete, Speicherchip zur Zwischenspeicherung von Systemdaten beschafft und in das Design integriert. Dabei traten erhebliche Schwierigkeiten auf, deren Ursache erst nach intensiver Analyse und dem Austausch mit Community- und Supportkanälen gefunden werden konnte und auf eine unzureichende, unübersichtlich strukturierte oder bewusst eingeschränkte Dokumentation des Bauteils zurückzuführen waren. Das Bauteil musste letztendlich ersetzt werden und verursachte somit etliche Komplikationen bei der Entwicklung. Auch der Bereich der Energieeffizienz des Systems, insbesondere der während der Erprobung wichtige Wechsel zwischen Stromnetz- und Batteriebetrieb, stellte eine wiederkehrende Quelle für Herausforderungen und technische Anpassungen dar.

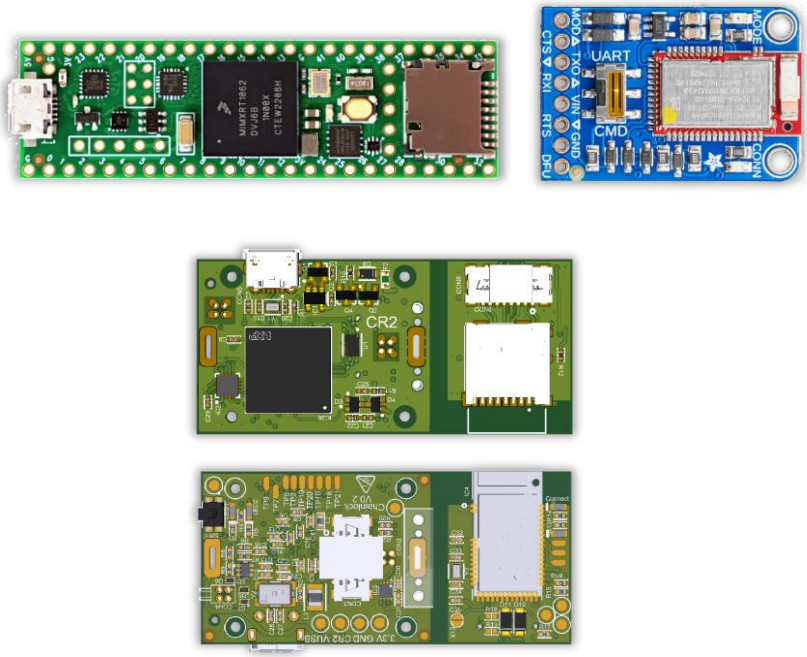


Abbildung 11: Darstellung in gleichem Maßstab. (Oben) Die generischen Versionen des Teensy 4.1 und Adafruit Bluefruit LE UART Friend. (Mitte & Unten) Die Unter- und Oberseite der auf die notwendigen Komponenten reduzierte und teilweise neu angeordneten Version beider Ausgangsplatinen.

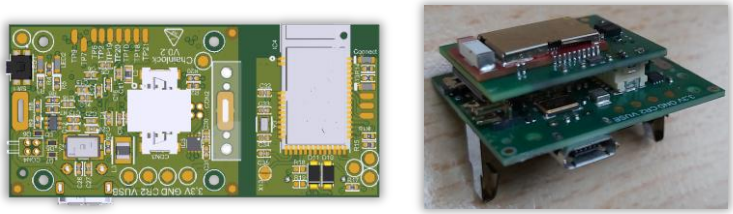


Abbildung 12: (Links) Der senkrechte, dunkelgrüne Bereich im rechten Teil der neuen Platine dient dem Auftrennen der Platine. (Rechts) Diese getrennten Teile ermöglichen die mehrlagige Anordnung zur effizienteren Ausnutzung des Raums im Zylinderknauf.

Mit Batteriekontakten, Trägerstrukturen, LED-Elementen und dem Anschluss des Schließmotors versehen ist ein Einbau in die innere Metallkäfig des Knaufs mit einem Innendurchmesser von 26 mm und einer Innenlänge von 36 mm durchführbar (Abbildung 13). Die äußere Hülle schließt den Knauf ab und versiegelt diesen gegen Umwelteinflüsse wie Wasser und Staub sowie gegen Aufbruchsversuche, wie schematisch in Abbildung 14 gezeigt.

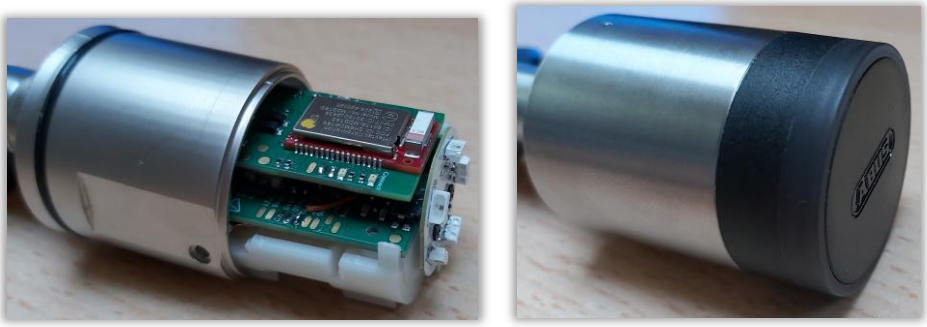


Abbildung 13: (Links) Mehrlagige Elektronikplatinen oberhalb des weißen Batteriefachs, mit LED-Elementen für optische Rückmeldungen der Schließaktionen und der inneren Metallhülle des Knaufs. (Rechts) Vollständig zusammengesetzter Zylinderknauf.

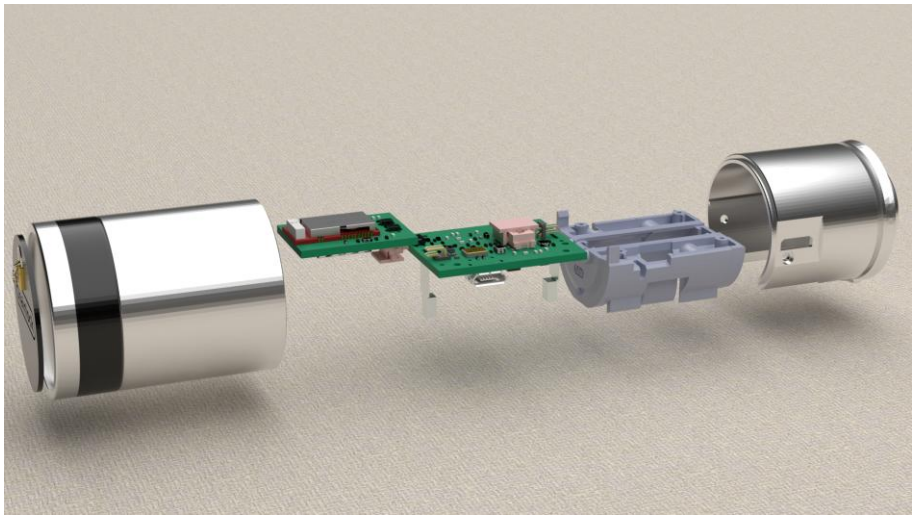


Abbildung 14: 3D-Darstellung der Komponenten des Chainlock-Knaufs.

Um einen beim Projektpartner vorhandenen Schließzylinder und die Bauteile auf der Türinnenseite ergänzt, ergeben die in Abbildung 15 gezeigten Montagschritte das in Abbildung 16 in einer Türdemonstrator montierte System.

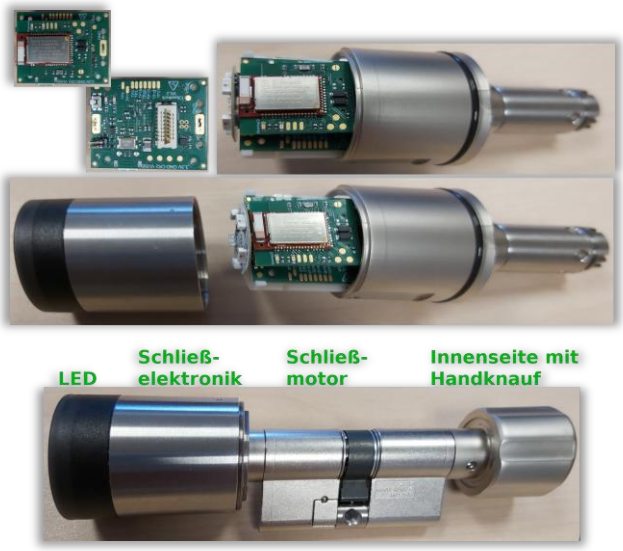


Abbildung 15: Komponenten eines Chainlock-basierten-Schlosses als (Oben links) einzelne elektronische Platinen (Oben rechts) zusammengesetzte, mehrere Lagen umfassende Steuereinheit mit Batteriefach im Knaufkäfig (Mitte) deren Einbau in das Schlossgehäuse mit Knaufhülle (Unten) bis zum fertigen Schließzylinder.

Abbildung 16: Transparente Demonstratortür mit dem Prototyp eines Chainlock-Schließzylinders eingebaut in ein modernes Einsteckschloss.

Die Analyse der aktuellen Lösung bezüglich des Nutzungsprofils der elektronischen Komponenten bei der Datenübertragung, -verarbeitung und -speicherung ergibt Indikatoren für die Nutzung von Hibernate-Modi, welche der weiteren Einsparung von Energie durch zeitweises Deaktivieren nichtbenötigter Komponenten oder auch deren dynamisch Leistungsdrosselung entsprechend der benötigten Arbeitsleistung ermöglicht.

Nutzerinterface

Aus den Use Cases wurden die unterschiedlichen funktionalen Anforderungen an die Interaktionen mit der Chainlock-Schließanlage, den Nutzern und den Schlössern extrahiert. Dabei wurden typische Szenarien wie das Verwalten von Schließberechtigungen, das Hinzufügen, Ändern und Entfernen von Nutzern und auch von Schlössern, sowie die Verwaltung der für den Betrieb notwendigen Konfigurationen systematisch erfasst, priorisiert und in Bedienkonzepte überführt. Diese Herangehensweise ermöglichte sowohl eine klare Funktionstrennung und Benutzerführung als auch die Entwicklung rollenorientierter Nutzeroberflächen, z. B. für Administratoren oder Nutzer. Gleichzeitig kann eine Reduktion auf notwendige Funktionen pro Nutzerrolle erfolgen.

Eine zentrale Anforderung stellt dabei die Lauffähigkeit dieser Nutzungs- bzw. Verwaltungskomponente auf gängigen Systemen, insbesondere den mobilen Systemen auf Basis von Android, iOS und Web dar. Hierdurch sollen sowohl die Schließanlage als auch die Anwendung möglichst unabhängig von spezifischen Betriebssystemen, herstellergebundenen Steuergeräten oder proprietären Frameworks sein. Eine feste Anbindung an bestimmte Anbieter (Vendor-Lock) ist zu vermeiden um das System zukunftssicher, wartbar, erweiterbar, kosteneffizient und flexibel einsetzen zu können. Somit werden Technologien auf Basis offener Standards wie den *RFCs 4252, 6234, 6321 7748*, die *ISO/IEC 18004:2006*, die *ANSI-Norm 359-2004* sowie möglichst weiter internationaler Verbreitung wie die *Ethereum Class* Blockchain priorisiert eingesetzt. Eine lange Bestehens- bzw. Verwendungsdauer sowie eine große Nutzer- und Entwickleranzahl zur Sicherstellung regelmäßige Updates, Fehlerbehebungen und der Weiterentwicklung mit neuen Funktionen waren weitere Auswahlkriterien.

Aufbauend auf diesen Analysen und Kriterien wurde für die Umsetzung des Nutzerinterfaces das Open Source Software Framework Flutter gewählt, welches durch eine einheitliche Codebasis sowohl Android- und iOS- als auch Web-Anwendungen effizient realisieren kann. Die leichte Portierbarkeit auf verschiedenen Endgeräten sowie die konsistente und gleichzeitig moderne, performante und anpassbare Oberfläche begünstigen die Bereitstellung. Gleichzeitig bietet Flutter eine hohe Entwicklungsgeschwindigkeit, eine große Community und umfangreiche Bibliotheken, ohne eine Bindung an einen einzelnen Plattformanbieter zu erzwingen. Deren korrekte Konfiguration im Zusammenspiel mit anderen Plugins und spezifischen Einstellungen stellt allerdings eine zum Teil nicht triviale Herausforderung dar. Eine konsequente Trennung von Front- und Backend durch standardisierte APIs gewährleistet die Robustheit gegenüber Fehlern und Manipulationsversuchen, aber auch die Austauschbarkeit von Bestandteilen wenn sich Funktionen verändern oder Weiterentwicklungen durchgeführt werden. Der modulare Aufbau der Oberfläche ermöglicht die flexible und voneinander unabhängige Weiterentwickelbarkeit, Erweiterbarkeit oder Austauschbarkeit einzelner Funktionsbereiche. Eindeutige und exakt definierte Zustandsmodelle realisieren zuverlässige und nachvollziehbare Aktionen und Anzeigen entsprechend den aktuellen Daten bzw. der erhaltenen standardisierte Backendnachrichten, was sowohl die Wartung als auch die Internationalisierung oder die Anpassung an spezifische Anforderungen einzelner Schließanlagenbetreiber erleichtert.

Das Nutzerinterface (Abbildung 17) besteht einerseits aus der Hauptseite mit den zugehörigen Buttons und Anzeigen zur Anforderung von Schließaktionen und andererseits aus mehreren Verwaltungs- und Einstellungsseiten, welche durch ein Menü erreichbar sind. Eine Seite dient dem Anlegen und Verwalten eigener digitaler Schlüsselpaare zum Nachweis der eigenen Identität, aber auch zum Einlesen der

öffentlichen Schlüssel anderer Nutzer. Weitere Seiten bearbeiten das Anlegen und Verwalten der in der Schließanlage eingesetzten Schlösser, der Konfiguration der Blockchainanbindung, der Verbindungsdaten für den externen Speicher bzw. der vom Nutzer der Schließapp präferierten Darstellungseinstellungen. Aufgrund der beträchtlichen Überschneidungen wurde eine Integration der administrativen Funktionen in die Oberfläche realisiert, welche durch entsprechende Autorisierung aktivierbar ist.

Die Kalenderseite stellt den zentralen Verwaltungsbereich der Schließanlage dar. Diese ermöglicht die übersichtliche Konfiguration, Zuweisung und Veränderung von Schließberechtigungen. Hierzu werden beliebige Mengen an Kalendereinträgen erstellt und mit Mengen an jeweils gewünschten Datums-, Zeit- und Wochentagseinstellungen versehen, z. B. einmalig, täglich, an bestimmten Wochentagen bzw. innerhalb eines bestimmten Zeitraums. Anschließend erfolgt die Zuordnung der verschiedenen Nutzer, Gruppen und Rollen, wodurch die Verbindung sowohl zu den schließberechtigten Personen als auch der zu schließenden Hardware realisiert ist. Im Fall von Änderungen, z.B. der Wochentage, sind von den betroffenen Kalendereinträge nur die zeitlichen Einstellungen anzupassen. Die anschließende, von der Verwaltung auszulösende, Aktualisierungsaktion ermittelt die Menge aller Änderungen, erstellt ein Update der Datensätze des externen Speichers sowie den Hash dieser Datensätze als Transaktionsinhalt für die Blockchain. Ist eine Internetverbindung vorhanden werden der externe Speicher und die Blockchain aktualisiert und somit die Änderungen an den Schließregeln der Anlage verteilt. Alle vorgenommenen Änderungen werden dadurch protokolliert und lassen sich zuverlässig nachvollziehen. Dies erhöht sowohl die Transparenz der Verwaltung als auch die Sicherheit im operativen Betrieb.

Zur Beurteilung der Benutzerfreundlichkeit und Funktionalität erfolgte durch erste Untersuchungen mit ausgewählten Probanden. Diese umfassten typische Use Cases wie das Öffnen eines Schlosses mittels der Schließapp auf dem Smartphone und das Anlegen und Verwalten von Nutzern sowie ihrer Schließberechtigungen. Zentrale Use Cases wie der Datentransfer zum externen Speicher und der verwendeten Blockchain sowie deren Download auf das Smartphone eines Nutzers und deren späterer Transfer zum Schloss wurden umfassender und mehrfach untersucht. Dies lieferte wertvolles qualitatives Feedback zu Navigation, Reaktionszeiten und Verständlichkeit, z.B. Eindeutiger Bezeichner bei der Schlüsselgenerierung oder verbesserter visuelle Rückmeldungen bei Schließaktionen. Weitere systematische Usability-Tests mit größerer Nutzerbasis sind vorgesehen, um das Interface iterativ weiter zu verbessern. Insgesamt bildet die Umsetzung der Chainlock-Schließapp mit Flutter in Kombination mit offenen Schnittstellen und einem modularen Design die Grundlage für eine skalierbare, benutzerfreundliche und zukunftssichere Anwendung, die unabhängig von Plattformanbietern betrieben und weiterentwickelt werden kann.

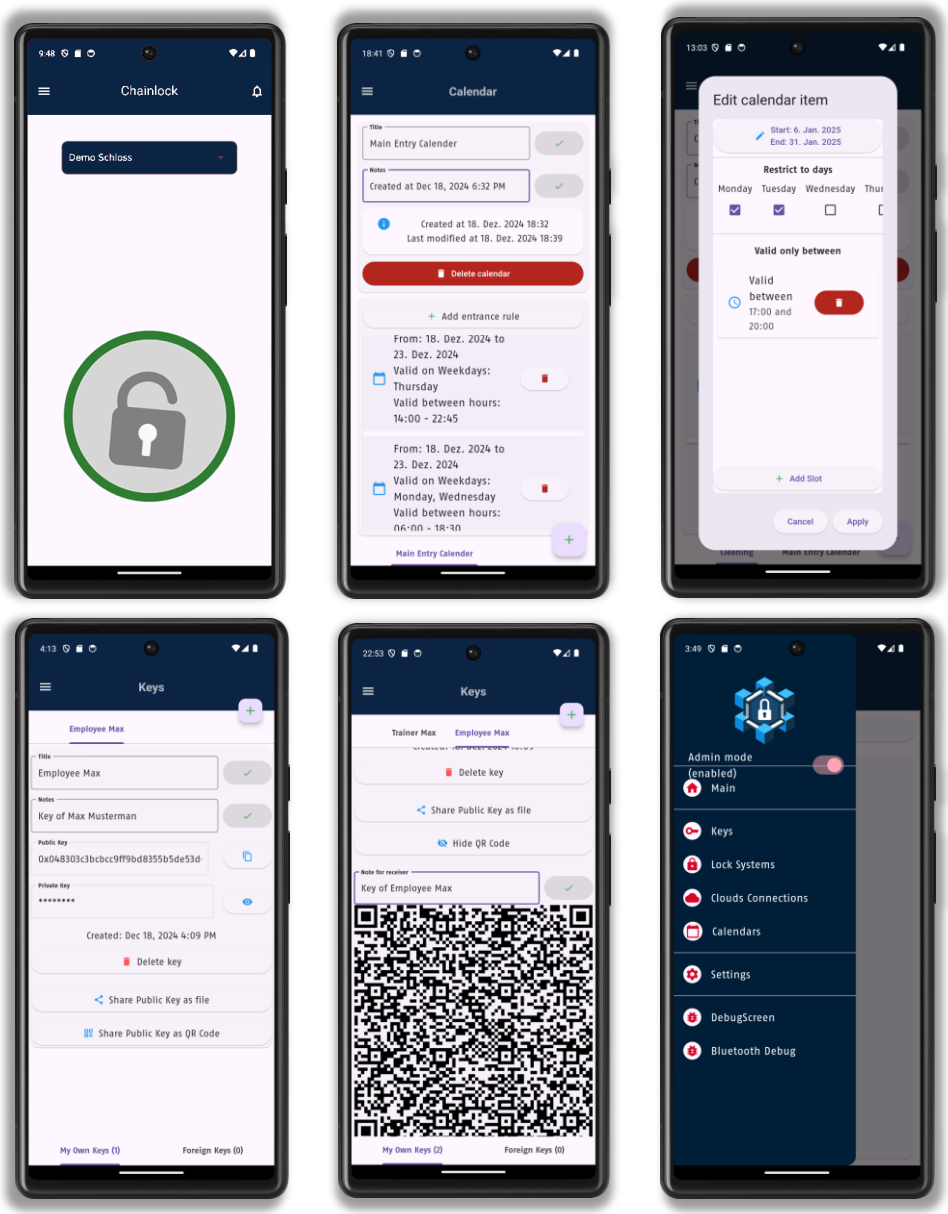


Abbildung 17: Screenshots der aktuellen Version der Steuerungs- und Verwaltungsapp. (Oben) Mit der Schlossauswahl und -schließanforderung, der Übersicht der Schließzeiten einer Gruppe von Schlössern und dem Menü zur Zeitfestlegung. (Unten) Menü zur Erstellung eines neuen Schlüssels für einen Nutzer bzw. eine Rolle und dessen Übertragung mittels QR-Codes. Das allgemeine Menü gruppiert die funktionalen Einheiten.

Arbeitspakete

AP 1 - 1.5 Technologierecherche, Blockchain-Feature-, Hardware- und Sicherheitsanalyse sowie Use Case Definition

Mit Beginn des Projektes Chainlock und des damit einhergehenden Entwicklungsprozesses wurden mehrere Arbeitsschwerpunkte bearbeitet. Zum einen die systematische Technologierecherche bezüglich bestehender Lösungen und Standards im Bereich elektronischer Zutrittskontroll- und Schließsysteme, Features und Randbedingungen von Blockchains, Kommunikationssysteme von Smartphones, kryptografischer Schlüsselverwaltung sowie der plattformunabhängigen Entwicklung von App auf mobilen Endgeräten mit Schwerpunkt auf Smartphones. Zum zweiten die Recherche zu existierenden Hardwaresystemen in den für Schließsysteme relevanten Größen, Bauarten und Formfaktoren sowie die damit einhergehenden Möglichkeiten, Beschränkungen, Sicherheitsanforderungen und -risiken. Und zum dritten die Definition relevanter Use Cases für das angestrebte Schließsystem aufbauend auf typischen Anwendungsbereichen. Diese Schwerpunkte bildeten die konzeptionelle Grundlage für Architekturentscheidungen, Schnittstellendesigns und die Auswahl geeigneter Hardware- und Softwarekomponenten.

Bei den Recherchen lag der Fokus auf der Identifikation offener, sicherer, erprobter, erweiterbarer und standardisierter Technologien, die sich möglichst gut in ein modulares Gesamtsystem integrieren lassen. Besondere Beachtung fanden hierbei Aspekte wie Interoperabilität, langfristige Wartbarkeit, Energieeffizienz und Miniaturisierbarkeit. Darüber hinaus wurde gezielt nach Technologien mit verfügbaren Open-Source-Implementierungen und großer Nutzercommunity gesucht, um Vendor-Lock-in zu vermeiden und eine unabhängige Weiterentwicklung zu ermöglichen. Im Ergebnis wurden Technologien auf Basis offener Standards wie den *RFCs 4252, 6234, 6321 7748*, der *ISO/IEC 18004:2006*, der *ANSI-Norm 359-2004* sowie die *Ethereum Class* Blockchain gefunden.

Die Recherchen zu Hardwaresystemen gestaltete sich komplexer und herausfordernder, da von vielen, fast identischen Komponenten mit fast identischen Spezifikationen und Dokumentationen oft größere Mengen von erheblich unterschiedlichen Realisierungen mit zum Teil gravierenden Detailunterschieden existieren. Einige Features sind zwar spezifiziert und dokumentiert, aber erst bei der realen Erprobung als nicht funktionsfähig oder nicht kompatibel erkennbar. Dies führte mehrfach zu Änderungen der verwendeten Hardware mit dem in Abbildung 14 dargestellt Aufbau des Prototyps.

Parallel wurden zentrale Use Cases für das angestrebte Schließsystem entwickelt und dokumentiert. Diese decken typische Anwendungsbereiche, wie die Anforderung von Schließaktionen per Smartphone, das Verwalten von Nutzern und Schließregeln oder das Hinzufügen neuer Schlösser ab. Die Use Cases wurden in Abstimmung mit den Projektpartnern und externen Auftragnehmern erarbeitet. Sie dienten als Leitfaden für die Systemarchitektur, die Benutzeroberflächen, die Sicherheits- und Kommunikationskonzepte sowie die Eigenschaften und Fähigkeiten der Hardware. Im Ergebnis führte dies über die in Abbildung 1 dargestellten realen Anforderungsszenarien zur in Abbildung 2 gezeigten groben Strukturierung mit dem Anwendungsablauf in Abbildung 3.

AP 2 - 3.4 Implementierung, Frontend, Backend, Schloss, Kommunikation, Schnittstellen und Proof of Concept

Während des Entwicklungsprozesses wurden die Features des Systems in mehreren Entwicklungszyklen realisiert. Der Fokus lag dabei auf der Umsetzung als funktionales Gesamtsystems, das sowohl mit seiner Frontend- als auch der Backend-Realisierung sowie der Schlosshardware einen jeweils funktionsfähigen Stand erreicht, wodurch wiederholt Untersuchungen und Demonstrationen erfolgen konnten.

Das Frontend wurde anfänglich als aus zwei Apps bestehende Lösung konzipiert, eine für normale Nutzer und eine zur Administration. Aufgrund der beträchtlichen Überschneidungen erfolgte aber bereits frühzeitig eine Umstellung hin zu einer App mit einem gesonderten, durch spezifische Einstellungen aktivierbaren Bereich für die Verwaltung, wie in Abbildung 17 dargestellt. Zur Umsetzung wurde nach der vorangegangenen Recherche das Framework Flutter genutzt. In der prototypischen Umsetzung wurden die wichtigsten Use Cases funktional abgebildet, darunter Anforderung von Schließaktionen, die Zuweisung von Berechtigungen mit Zeitfenstern und die Verwaltung von Nutzern.

Das Backend umfasst zum einen die im Hintergrund der Schließapp bereitgestellte Funktionalität zur Verwaltung von Schlössern, Nutzern, Gruppen, Rollen und Schließberechtigungen sowie den Anbindungen an den externen Speicher und die Blockchain. Zum anderen die automatische Kommunikation mit dem externen Speicher und der Blockchain sowie mit den in Reichweite befindlichen Schlössern zur Aktualisierung der Berechtigungsdaten innerhalb der Schließanlage, entsprechend dem Ablaufplanung in Abbildung 3.

Zeitgleich wurde ein funktionaler Hardwareprototyp entwickelt, der ein physisches Schloss mit integrierter Elektronik zur Steuerung der Nutzung kombiniert. Der hierfür ursprünglich vorgesehen *Arduino Nano 33 BLE Sense Rev1* musste frühzeitig durch den leistungsfähigeren Teensy 4.1 und das Bluefruit-Modul ersetzt werden, um die Kommunikation via Bluetooth Low Energy mit der Schließapp, die Datenspeicherung und die kryptographischen Berechnungen zu realisieren, wie in Abbildung 7, Abbildung 8 und Abbildung 10 gezeigt.

Für die Interaktion zwischen Schließapp, externem Speicher und Blockchain wurden existierende Flutter-Plugins und die darin implementierten Kommunikationsprotokolle der Speicheranbieter, z.B. Google Drive und Nextcloud, eingebunden. Aufgrund von deren vielfältigen Einsatzmöglichkeiten und der verschiedene Nutzungsmodi erwies sich die geeignete Konfiguration als Herausforderung. Für die Kommunikation zwischen Schließapp und Schloss wurden weitere Flutter-Plugins eingebunden und das darin realisierten rudimentäre Protokoll um ein eigens definiertes Kommunikationsprotokolle ergänzt. Dieses ermöglicht den Austausch großer Teil der Blockchain oder auch nur einzelner, noch benötigter Blöcke sowie die Übertragung von Differenzen bei der Aktualisierung der Schließberechtigungen.

Durch die partielle Funktionsfähigkeit einzelner Zwischenstände konnten die zu diesem Zeitpunkt vorhanden Features des Systems untersucht, Defizite und Schwächen frühzeitig erkannt und gegebenenfalls nachjustiert oder mikroelektronische Bauteile ersetzt werden. Somit konnten die jeweiligen Teile der Funktionskette, wie die Benutzerverwaltung, die Kommunikation mit der Blockchain

oder Schließaktionen eines Schlosses nachvollziehbar demonstriert werden, beispielsweise während der Demonstratortage. Der letztendliche Nachweis der Gesamtfunktionalität bestätigt die technische Umsetzbarkeit und dient als Basis für mögliche Testeinsätze im realen Umfeld.

AP 4 - 4.2 Ergebniskonsolidierung und Dokumentation

Die im Verlauf der Entwicklung erlangten Entwürfe, Konzepte, Teilergebnisse und Beschreibungen wurden in der eingesetzten Projektmanagementplattform Confluence zusammengestellt. In Verbindung mit dem darin enthaltenen Ticketsystem können der Projektverlauf, also bisherige Arbeitsschritte und der aktuelle Stand, sowie Entwicklungsentscheidungen nachvollzogen werden. Die Programmquellen wie Source Code, Assets, Konfigurationen der Buildumgebungen, Testdaten u.ä. wurde in der Quellenverwaltungsplattform GitHub gesichert. Für ein darauf aufbauendes Folgeprojekt bzw. externe Partner ist somit eine belastbare und strukturierte Wissensbasis bereitgestellt.

Meilensteine

Meilenstein M1 wurde erreicht.
Die zentrale Use Cases und die zugehörigen technischen Konzepte wurden für alle beteiligten Systemkomponenten, wie Schließapp, Schloss, Datenspeicher und Blockchain, systematisch definiert und entsprechend dokumentiert. Die Verarbeitungsprozesse der Blockchain wurden umfassend untersucht und die relevanten Informationen zu Eckdaten wie Kommunikationsschnittstellen, Speicher- und Ressourcenverbrauch etc. ermittelt. In Zusammenarbeit mit dem extern beauftragten Sicherheitsexperten wurden einschlägige Sicherheitsrichtlinien recherchiert, auf Besonderheiten des Projektes und potenzielle Angriffsvektoren und -methoden hin taxiert sowie die Ergebnisse dokumentiert. Daraus resultierende Modifikationen in Bezug auf Architektur und Programmierung erfolgten ebenso wie die durch Miniaturisierung notwendigen. Somit konnte eine kompakte Umsetzung der im Projekt vorgesehenen Lösung erfolgen.

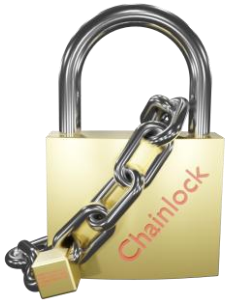
Meilensteine M2 und M3 wurde erreicht.
Ein lauffähiger Prototyp des administrativen Frontends zur Verwaltung der Schließanlage mit den Schlössern, Nutzer und Schließberechtigungen wurde ebenso umgesetzt wie die backendseitigen Anbindungen zum externen Speicher und der verwendeten Blockchain. Unterschiedliche Entwicklungsstände realer mit angepasster Embedded-Hardware prototypisch realisierter Demonstratoren sind verfügbar und wurden auf mehreren Demonstratortagen der Blockchain Schaufensterregion Mittweida präsentiert und ihr Zusammenspiel erfolgreich den interessierten Besuchern und dem Fachpublikum gezeigt. Erste Untersuchungen zur Nutzbarkeit, Funktionseffizienz, Usability und Bedienbarkeit sind erfolgt und die zugehörigen Ergebnisse wurden erfasst.

Die entwickelten Konzepte sowie verschiedene Zwischenstände der Hard- und Software wurden im Jahr 2023 auf der internationalen Konferenz *PErvasive Technologies Related to Assistive Environments (PETRA)* am 05.07.2023, der *Blockchain Autumn School (BAS)* am 14.09.2023 und auf dem *Demonstratortag* der Blockchain Schaufensterregion Mittweida am 15.09.2023 präsentiert. Im Jahr 2024 folgten Beiträge und Präsentationen auf der *International Conference on Computing, Networking and Communications* (ICNC) am

19.02.2024, auf dem *Demonstratortag* der Blockchain Schaufensterregion Mittweida am 18.09.2024 mit einem Beitrag im *MDR Sachsenspiegel* sowie auf der internationalen *3rd Blockchain and Cryptocurrency Conference* (B2C) am 17.10.2024. Präsentationen und Demonstrationen der Prototypen einem breiten Publikum gegenüber sind zur *Nacht der Wissenschaft* der Hochschule Mittweida am 20.06.2025 sowie beim *Demonstratortag* 2025 geplant.

Design

Für Vorträge, Poster, Websites und die mobile App wurden ein Logo und eine Präsentationsvorlage entworfen:



Juristischer Rahmen

Im Rahmen der Entwicklung des digitalen Schließsystems waren neben den technischen Aspekten auch rechtliche Fragestellungen von zentraler Bedeutung. Insbesondere im Hinblick auf Datenschutz, Nutzungsrechte und die Einbindung externer Anbieter waren umfassende juristische Beratung und Unterstützung sowie die Prüfung verschiedener Rahmenbedingungen erforderlich. Ziel war es, ein rechtssicheres Fundament für den angestrebten Vertrieb bzw. den Systembetrieb sowie für die Interaktion mit Nutzern und Partnern zu schaffen.

Zu diesem Zweck wurden in enger Zusammenarbeit mit der Rechtsanwältin Katja Schulze als juristische Fachberaterin mehrere Vertragswerke und Regelwerke entwickelt:

Vertragsvorlagen für Anbieter von Drittsystemen:
Für die Integration bzw. Nutzung externer Hard- oder Softwarekomponenten wurden spezielle Vereinbarungen geschaffen. Diese legen technische Schnittstellen, Gewährleistungsansprüche sowie die Verantwortlichkeit für sicherheitsrelevante Aspekte fest.

Allgemeine Geschäftsbedingungen (AGB):
Die AGB bilden die rechtliche Grundlage für sämtliche vertraglichen Beziehungen rund um das System. Sie schaffen Transparenz für Nutzer und Partner, regeln den Leistungsumfang und sichern das Unternehmen gegenüber rechtlichen Risiken ab.

Beurteilung von Vertragsvorlagen potenzieller Nutzung der Dienste Dritter:
Diese untersuchen die Besonderheiten bei der Nutzung der Dienste Dritter durch Schließanlagenbetreiber bzw. durch den Dienstanbieter im Fall einer zukünftigen Ausgründung. Hierzu werden die vertraglichen Bestimmungen großer Cloud-Dienste auf ihre Nutzbarkeit, Einschränkungen und Haftungsansprüche sowie Datenschutzbestimmungen im Einklang mit der DSGVO geprüft. Besonderheiten bei der Bereitstellung eigener Cloud-Dienste, im Fall einer zukünftigen Ausgründung, wurden untersucht und für als Randbedingungen für zukünftige Entwicklungsentscheidungen festgehalten.

Durch diese Maßnahmen konnte sichergestellt werden, dass das entwickelte System nicht nur technisch, sondern auch juristisch belastbar ist. Außerdem sollten frühzeitig Risiken erkannt und vermieden, sowie rechtlich aufwändige und schwer handhabbare Folgen während des Betriebes minimiert werden.

Eventuelle Notwendigkeit zur softwareseitigen Offenlegung des Prototypencodes und die damit einhergehenden Anforderungen an Softwarequalität, die Unternehmensformen und Einschränkungen bezüglich späterer geplanter Markteinführungen wurden untersucht und die juristischen Rahmenbedingungen ermittelt.

Unterschiedliche Szenarien der Systembereitstellung und -nutzung wurden während der Bearbeitung des Projektes identifiziert, welche eine komplexere Betrachtung der rechtlichen Situation durch die juristische Begleitung des Projektes erforderten. Insbesondere ergaben sind unterschiedliche Abstufungen der Herstellerunabhängigkeit des Schließanlagenbesitzer. Eine vollständige Umsetzung der Schließanlagenbestandteil durch den Besitzer realisiert zwar die größtmögliche Unabhängigkeit und erfordert keinen vertrauenswürdigen Dritten, benötigt aber die Bereitstellung der für den externen Speicher notwendige Servertechnik. Diese muss Redundanzen für Dienstunterbrechungen im Fall von Wartungsarbeiten, Unfällen oder Angriffen vorgehalten werden. Zusätzlich ist eine ausreichende Abdeckung mit Mobilfunk- oder WLAN-Netzen, ebenfalls wieder mit Redundanzen, zu realisieren, um die Datenverteilung zu den Smartphones der Nutzer zu gewährleisten. Demgegenüber ist auch eine teilweise Umsetzung durch den Schließanlagenbetreiber möglich, wobei nur die Hardware beschafft und die Berechtigungen verwaltet werden. Der Bereitstellung und Wartung der Server, die Schließapp und der Mobilfunknetze erfolgt durch Drittanbietern. Diese Variante erfordert weniger Ressourcen auf Seiten des Besitzers, aber Vertrauen in die korrekte Arbeitsweise der genutzten Komponenten. Für das Projekt ergaben sich daraus wesentliche Fragen bezüglich Produkthaftung für Dienste ohne eigene Kontrolle und die damit verbundenen Vertragsklauseln gegenüber Käufern, aber auch gegenüber diensterbringenden Dritten, sowie einiger für die Entwicklung notwendiger Entscheidungen. Durch die wiederholte juristische Beratung und Unterstützung konnten diese Entscheidungen getroffen und Hindernisse für nachfolgende Entwicklungen beseitigt werden.

Personal

Trotz intensiver Suche blieb die Personalsituation schwierig und es konnten im Projektzeitraum nur 1,5 der 2,0 Personalstellen besetzt werden, sodass die verbleibende 0,5 Stelle unbesetzt blieb und die Personalausgaben geringer ausfallen. Die vollständige Besetzung aller Personalstellen wurde angestrebt, konnte aber nicht realisiert werden.

Die für die juristische Begleitung zuständige Frau Katja Schulze unterstützte das Projekt. Rechtliche Abwägungen speziell im Zusammenhang mit der Blockchain-Technologie, bei Haftungs- und Datenschutzfragen bei der Nutzung von Diensten dritten Parteien und damit einhergehender Implementierungsabhängigkeiten stellten hier den Schwerpunkt dar.

Daraus folgende Anpassungen der Softwarearchitektur wurden mit Herrn Markus Straßburg begutachtet, welcher die IT-technische Begleitung realisiert. Diese Beratungen verbesserten die Schließapp in Bezug auf die Datensicherheit und ihre weitestmögliche Anlehnung an die ISO/IEC 27001.

Technik

Aufgrund der im Jahr 2023 aufgetreten Lieferengpässe und sanktionsbedingter Einschränkungen bei verschiedenen Hardwarekomponenten sowie den Preissteigerungen in vielen Bereichen wurden nicht alle Sachausgaben realisiert. Da einige Komponenten allerdings auch günstiger wurden konnte deren kostenneutrale Beschaffung im Jahr 2024 durchgeführt werden.

Wissenschaftliche Publikationen zum Projekt erfolgten bei:

[1] Robert Manthey, Richard Vogel, Matthias Baumgart, Christian Roschke, Marc Ritter, and Matthias 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 (Corfu, Greece, 2023-07-05) (PETRA '23). ACM, 120–122. https://doi.org/10.1145/3594806.3594842

[2] Robert Manthey, Richard Vogel, and Matthias Vodel. 2023. Chainlock - Blockchain-gestützte, smarte Schließanlagen. In Konferenzband zum Scientific Track der Blockchain Autumn School 2023 (2023-09-14), Vol. 2. Hochschule Mittweida, 4.

[3] Robert Manthey, Richard Vogel, and Matthias Vodel. 2024. Decentralized Offline Smart Lock - Chainlock. In 3rd Blockchain and Cryptocurrency Conference (B2C) (2024-10-17). International Frequency Sensor Association (IFSA), 4. https://doi.org/10.13140/RG.2.2.27372.58246

[4] Richard Vogel, Robert Manthey, Matthias Baumgart, Christian Roschke, Marc Ritter, and Matthias Vodel. 2024. Tamperproof Data Transmission to Offline IoT Devices in a Zero-Trust Environment. In 2024 International Conference on Computing, Networking and Communications (ICNC) (Big Island, HI, USA, 2024-02-19). IEEE, 817–822. https://doi.org/10.1109/ICNC59896.2024.10555945

Teilnahmen an öffentliche Veranstaltungen zur Präsentation des Projektes:

[1] Demonstratortag 2023, Mittweida

[2] Demonstratortag 2024, Mittweida, https://mwe-mittweida.de/blockchain-demonstratortag-2024-ein-erfolgreiches-finale-der-blockchain-autumn-school/

[3] Beitrag im *MDR Sachsenspiegel: Demonstratortag zur Blockchain-Technologie in Mittweida*, 2024-09-18, https://www.ardmediathek.de/video/mdr-sachsenspiegel/demonstratortag-zur-blockchain-technologie-in-mittweida/mdr-sachsen/Y3JpZDovL21kci5kZS9iZWl0cmFnL2Ntcy80MmYxMzlhMS01M2U2LTQxZWMtODczMS03ZDgyMGNiMGQxMjA

[4] Nacht der Wissenschaft 2025, Mittweida, geplant

[5] Demonstratortag 2025, Mittweida, geplant

2. **Vergleich des Stands des Vorhabens mit der ursprünglichen (bzw. mit Zustimmung des Zuwendungsgebers geänderten) Arbeits-, Zeit- und Ausgabenplanung.**

   Der Vorhabenstand entspricht der nachfolgenden, angepassten Verteilung:
   TODO (Tabelle mit Finanzplanänderungen)

3. **Haben sich die Aussichten für die Erreichung der Ziele des Vorhabens innerhalb des angegebenen Berichtszeitraums gegenüber dem ursprünglichen Antrag geändert (Begründung)?**

   Nein.

4. **Sind inzwischen von dritter Seite Ergebnisse bekannt geworden, die für die Durchführung des Vorhabens relevant sind? (Darstellung der aktuellen Informationsrecherchen nach Nr. 2.1 BNBest-BMBF 98).**

   Nein.

5. **Sind oder werden Änderungen in der Zielsetzung notwendig?**

   Nein.

6. **Erfindungen/Schutzrechtsanmeldungen und erteilte Schutzrechte, die vom ZE oder von am Vorhaben Beteiligten gemacht oder in Anspruch genommen wurden, sowie deren standortbezogene Verwertung (Lizenzen u.a.) und erkennbare weitere Verwertungsmöglichkeiten**

   Keine.

7. **Fortschreibung des Verwertungsplans. Diese soll, soweit im Einzelfall zutreffend, Angaben zu folgenden Punkten enthalten.**

   Über künftigen Produktions- und Vertriebspartner kann das entwickelte System weiterentwickelt und angeboten werden. Entsprechende juristisch abgestimmte Vorlagen und Hinweise für AGBs und Vertragsregelungen mit Herstellern, Dienstleistern und Kunden wurden erarbeitet. Die grundlegenden Features wurden implementiert und funktionieren im Rahmen der Prototypenentwicklungsphase.
   Vorhaben für die weitere Entwicklung sind die Erhöhung der Schließzyklen des Schlossprototyps, dessen energetische und elektronische Optimierung unter Beachtung der für die industrielle Fertigung notwendigen Randbedingungen sowie die Integration der „Chainlock“-App sind die verschiedenen App-Stores. Außerdem sind Feedbacks und Verbesserungen der App im Rahmen weiterer Testphasen zu erheben und einzuarbeiten. Eine Anbindung anderer Projekte wie beispielsweise ID-Ideal ist zu prüfen.
   Konzepte für eine weitere Ausgestaltung sind vorhanden. Das aufgebaute Knowhow in den Bereichen Embedded-Hardware-Prototyping und generischer App-Strukturen mit Flutter können auf weitere Bereiche angewandt und angepasst werden.