Fraunhofer FIT

Fraunhofer-Institut für Angewandte Informationstechnik FIT

# Moderne Blockchain-Wallets

**Studie**

# Moderne Blockchain-Wallets

## Studie

**Disclaimer**

Diese Studie wurde vom Fraunhofer-Institut für Angewandte Informationstechnik FIT nach bestem Wissen und unter Einhaltung der nötigen Sorgfalt erstellt. Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen übernehmen keinerlei Garantie dafür, dass die Inhalte dieser Studie gesichert, vollständig für bestimmte Zwecke brauchbar oder in sonstiger Weise frei von Fehlern sind. Die Nutzung dieser Studie geschieht ausschließlich auf eigene Verantwortung. In keinem Fall haften das Fraunhofer FIT, seine gesetzlichen Vertreter und/oder Erfüllungsgehilfen für jegliche Schäden, seien sie mittelbar oder unmittelbar, die aus der Nutzung der Studie resultieren.

**Bildquellen**



**Empfohlene Zitierweise**

Radlinski, M.; Trauth, D.; Prinz, W. (2024): Moderne Blockchain-Wallets.
Fraunhofer-Institut für Angewandte Informationstechnik FIT.
https://doi.org/10.24406/publica-3383

# Inhaltsverzeichnis


# Spotlight

»Der beste Blockchain-Use-Case ist der, bei dem man die Blockchain nicht sieht.«

**Prof. Wolfgang Prinz, PhD**
Leiter des Blockchain Reallabors
Professor an der RWTH Aachen University
Stellv. Institutsleiter Fraunhofer FIT
Leiter der Abteilung Kooperationssysteme am
Fraunhofer-Institut für Angewandte Informationstechnik FIT

**10** verschiedene Wallets-as-a-Service Anbieter auf Handhabbarkeit untersucht

**Barrierefreie** Benutzerinteraktion durch gewohnten Web2 Login

**7** Wallets mit **Sicherheit** durch **Mehrparteienprinzip**

**6** Wallets mit **Gebühren-übernahme-automatik**

# Executive Summary

»Wallets spielen eine zentrale Rolle im Web3, da sie die sichere Verwaltung digitaler Identitäten und Vermögenswerte ermöglichen und somit eine Grundlage für die Interaktion in dezentralisierten Netzwerken bilden. Diese Studie untersucht verschiedene Blockchain-Wallets, insbesondere von Wallet-as-a-Service (WaaS)-Anbietern. Sie hebt die Wichtigkeit einer nahtlosen Benutzerinteraktion hervor und untersucht verschiedene Aspekte von WaaS, wie Sicherheit, Kosten, unterstützte Blockchain Protokolle, Frameworks und die Benutzer- sowie Entwicklerfreundlichkeit.

Die Studie stellt fest, dass eine gute Benutzerfreundlichkeit entscheidend für den Erfolg von Unternehmen ist, die WaaS-Wallets anbieten. Sie zeigt, dass die nahtlose Interaktion durch Funktionen wie Gebührenübernahmeautomatik verbessert werden kann und dass WaaS-Unternehmen verschiedene Architekturen entwickeln, um die Sicherheit der Wallets zu gewährleisten, ohne dass der Benutzer die privaten Schlüssel verwalten muss.

Es werden zehn verschiedene WaaS-Anbieter verglichen, und die Ergebnisse zeigen, dass einige Anbieter wie Circle, Coinbase WaaS, Crossmint, Magic, Privy und Web3Auth Gebührenübernahmeautomatiken unterstützen, die eine nahtlose Benutzerinteraktion fördern. Die Studie schließt mit verschiedenen Szenarien für die Auswahl von WaaS-Wallets abhängig von den Bedürfnissen des Unternehmens.«

**Prof. Wolfgang Prinz, PhD**
Leiter des Blockchain Reallabors
Professor an der RWTH Aachen University
Stellv. Institutsleiter Fraunhofer FIT
Leiter der Abteilung Kooperationssysteme am
Fraunhofer-Institut für
Angewandte Informationstechnik FIT

# Einleitung

Die Studie von 2017 mit dem Titel »Zahlungsverkehr 4.0« behandelt das Thema der Digitalisierung von Zahlungsprozessen [2]. Sie befasst sich nicht nur mit der Digitalisierung von Bargeld, sondern beschreibt ebenso das steigende Interesse in Blockchain. Besonders unterstreicht die Studie potenzielle Interaktionsinnovationen, neue Geschäftsmodelle und neue Kommunikationslösungen, welche mit Blockchain-Technologien einhergehen. Ebenso wird eine digitale und flexible Anpassung als eine Notwendigkeit angesehen.

Geschäftsmodelle, welche auf Blockchain-Technologien basieren und Benutzer sowohl aktiv als auch passiv mit der Blockchain interagieren lassen, benötigen einen Umgang mit Blockchain-Wallets. Solche Wallets sind benutzer-unfreundlich, wodurch die Nutzerakzeptanz erschwert wird und eine Verbreitung gehemmt wird. Die Hürde besteht in dem Aufwand, welcher mit einer Blockchain-Wallet einhergeht [1].

Eine Alternative zu den Wallets sind Custodial-Wallets [4]. Custodial-Wallets werden von Dritten betrieben, welche die Vermögenswerte der Nutzer verwalten und für die Sicherheit der Wallets verantwortlich sind. Analog zu diesen Wallets stehen Banken, welche ebenso die Vermögenswerte der Nutzer verwalten. Ein Geschäftsmodell, welches durch die Custodial-Wallets und auch durch Mehrparteienprinzip-Wallets entstanden ist, nennt man Wallet-as-a-Service.

Diese Studie befasst sich ausschließlich mit Wallet-as-a-Service Anbietern, welche versprechen eine gute Benutzerfreundlichkeit zu gewährleisten.

## Blockchain-Wallets

Blockchain-Wallets bestehen aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel dient als Adresse und der private Schlüssel dient zum Unterschreiben und Ausführen von Transaktionen. Bei Blockchain-Wallets bekommt der Benutzer den privaten Schlüssel und einen Wiederherstellungssatz, welcher dazu dient, die Wallet an anderen Geräten wiederherzustellen, falls die ursprüngliche Wallet verloren oder gelöscht sein sollte. In diesem Fall kann nur der Besitzer des privaten Schlüssels oder des Wiederherstellungssatzes die Wallet wiederherstellen. Sollten diese Schlüssel inklusive Wallet verloren gehen, so gehen auch die gesamten Vermögenswerte verloren [3].
Bargeld funktioniert analog. Wird das Bargeld verloren, so verliert der ursprüngliche Besitzer die Vermögenswerte.

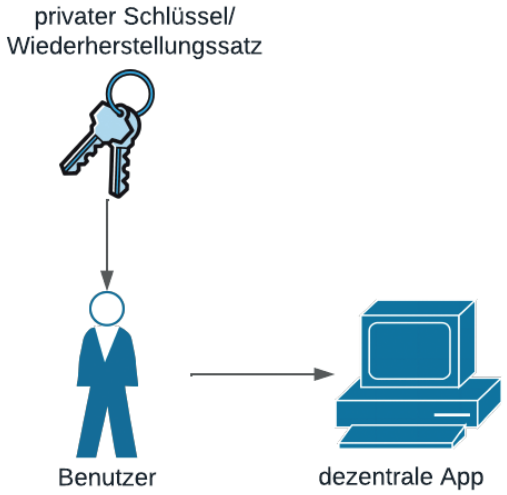



*Abbildung 1: Non-Custodial-Wallet*

Bei Custodial-Wallets verwalten Anbieter die jeweiligen privaten Schlüssel inklusive Wiederherstellungssatzes [4]. Abbildung 1 zeigt die Verwaltungsmethode einer Non-Custodial-Wallet wohingegen Abbildung 2 eine Custodial-Wallet visualisiert.

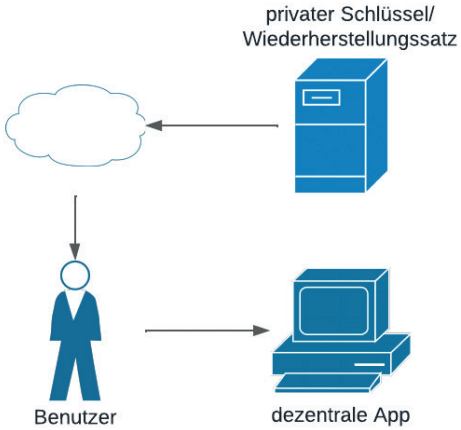



*Abbildung 2: Custodial-Wallet (vereinfacht)*

In beiden Fällen authentifiziert sich der Benutzer bei einer dezentralen App mit einer Unterschrift mit Hilfe des privaten Schlüssels. In Abbildung 2 besitzt der Benutzer jedoch nicht direkt die Schlüssel, sondern hat nur Zugriff auf diese. Dieser Zugriff kann durch Web2 Authentifizierungs-methoden realisiert werden wie zum Beispiel E-Mail, Google etc.

## Wallet-as-a-Service

Wallet-as-a-Service (WaaS) ist ein Geschäftsmodell, welches Unternehmen erlaubt eine Walletinfrastruktur in ein System zu integrieren. WaaS können sowohl auf den Prinzipien von Custodial und Non-Custodial-Wallets basieren [5]. Im Rahmen der Benutzerfreundlichkeit und Massenadoption

werden WaaS-Unternehmen betrachtet und evaluiert, welche sich auf Web2 Authentifikationsmethoden beziehen, wobei der Benutzer von der Verwaltung der Schlüssel entlastet wird. Im Fall dieser Wallets erstellen WaaS-Unternehmen unterschiedliche Architekturen, um die Sicherheit der Wallets zu gewährleisten.

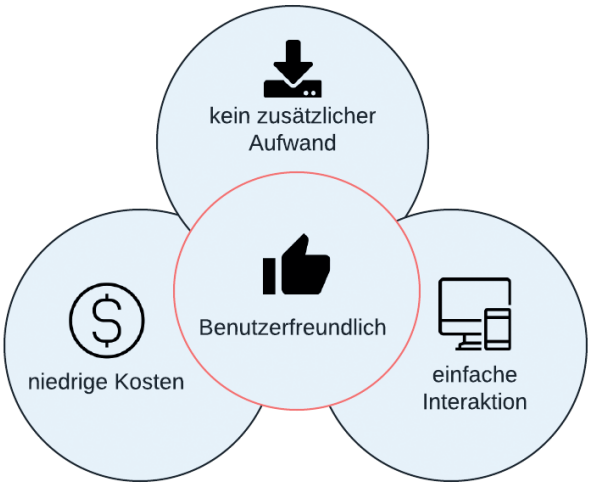
## Kriterien von Wallet-as-a-Service-Wallets

Im Hinblick auf Benutzerfreundlichkeit gibt es zwei Anwender, welche von WaaS-Wallets betroffen sind:

- Programmierer, welche die WaaS- Infrastruktur in ein Projekt integrieren müssen
- Benutzer, welche mit der Benutzer-oberfläche der Implementierung interagieren

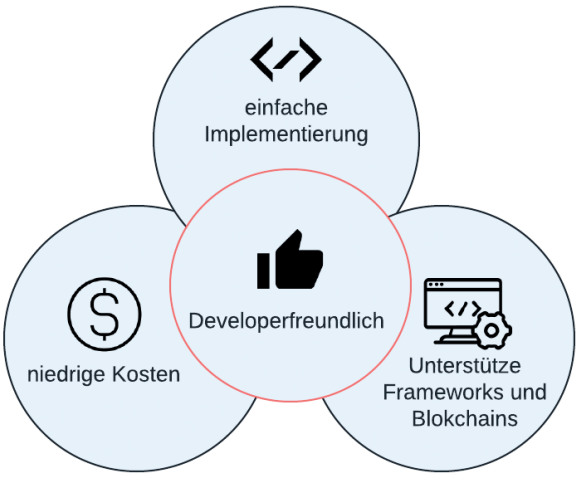
## Anwender

Für den Nutzer ist eine besonders nahtlose Interaktion mit der Benutzeroberfläche von größter Bedeutung. Dazu gehört eine einfache oder bekannte interaktionsweise, welche keinen zusätzlichen oder unüblichen Aufwand aufbereitet. Ebenso sind hier die miteinhergehenden Kosten zu beachten. Hierbei entscheidet der Programmierer oder das Unternehmen, welche Partei die Kosten übernimmt.




## Programmierer

Für den Programmierer ist die Integrierung von WaaS-Software von besonderer Bedeutung. Darunter fällt der eigene benötigte Implementierungsaufwand und die unterstützten Frameworks und Blockchains. Ebenso sind die Kosten zu beachten, welche eine WaaS-Software mit sich bringt.



# Untersuchte Wallets

Diese Studie bietet einen Vergleich von 10 verschiedenen WaaS-Unternehmen. Im weiteren Verlauf werden die untersuchten WaaS vorgestellt und ihre jeweiligen Versprechen dargelegt. Die Reihenfolge erfolgt in alphabetischer Sortierung und soll keinerlei Wertung widerspiegeln.

1. **Circle** verspricht eine sichere Wallet mit benutzerfreundlichen Interaktionen, schneller Implementierung und einer Skalierbarkeit für Milliarden von Nutzern [6]
2. **Coinbase-WaaS** verspricht eine nahtlose Interaktion von Benutzern mit Blockchain, wodurch diese sich nicht um Wiederherstellungssätze kümmern müssen und der Sicherheit von Coinbase vertrauen [7]
3. **Crossmint** verspricht eine interoperable NFT-Wallets mit hoher Sicherheit [8]
4. **Fireblocks** verspricht eine skalierbare, flexible und sichere Wallet für tausende von Unternehmen [9]
5. **Fordefi** verspricht eine Non-Custodial-Wallet für nahtlose Benutzerinteraktion [10]
6. **Magic** verspricht eine stressfreie und nahtlose Web3 Erfahrung [11]
7. **Privy** verspricht eine sichere WaaS-Wallet für hohe Benutzerintegration in kurzer Programmierzeit [12]
8. **Self Chain** verspricht eine Layer-1 Blockchain inklusive schlüsselfreier WaaS-Wallets [13]
9. **Walt.id** verspricht eine simple Infrastruktur für digitale Wallets und Identitäten [14]
10. **Web3Auth** verspricht eine sichere, skalierbare Non-Custodial WaaS durch social logins [15]

# Wallets im Vergleich

In diesem Abschnitt werden die 10 WaaS-Anbieter einer eingehenden Untersuchung unterzogen, um die Benutzerfreundlichkeit ihrer Wallets zu bewerten. Unterteilt wird das Kapitel in die individuellen Wallet-Funktionalitäten und Besonderheiten, die unterstützen Blockchains, die einhergehenden Kosten, und zuletzt Developer- und Benutzerfreundlichkeit.

## Wallet-Funktionalitäten und Besonderheiten

Die vorgestellten WaaS-Unternehmen haben verschiedene Besonderheiten und Ziele, welche diese verfolgen. Somit wurden in Tabelle 1 die jeweiligen Merkmale aufgelistet. Zu beachten ist, dass Benutzerfreundlichkeit hier nicht explizit als eine Besonderheit notiert wurde, weil dieses Merkmal von vielen der WaaS-Unternehmen versprochen wird und im zugehörigen Kapitel später untersucht wird.

**Tabelle 1: Waas Besonderheiten**

| WaaS | Besonderheiten |
|---|---|
| Circle | Volle Kontrolle über Benutzerschlüssel |
| Coinbase-Waas | Wallets mit Coinbase-Integration |
| Crossmint | NFT-Fokussiert inklusive NFT-Erstellung |
| Fireblocks | Verschiedene Verwaltungsarten für Privatbenutzer |
| Fordefi | Kontrollcenter |
| Magic | Patentiertes Schlüssel-Management |
| Privy | Benutzerorientierte dynamische Anpassung |
| Self Chain | Eigene Blockchain |
| Walt.id | Digitale Identitäten |
| Web3Auth | Account abstraction, Eigentumsübertragung |

Viele der WaaS-Unternehmen benutzen Mehrparteienberechnung und unterstützen Gebührenübernahmeautomatiken. In Tabelle 2 wurde notiert welche dieser Unternehmen jeweils die Technologien unterstützen:

**Tabelle 2: Mehrpartei-Wallet und Gebührenübernahmeautomatik**

| WaaS | Mehrpartei -Wallet | Gebührenübernahme -automatik |
|---|---|---|
| Circle | √ | √ |
| Coinbase-Waas | √ | √ |
| Crossmint | √ | √ |
| Fireblocks | √ | x |
| Fordefi | √ | x |
| Magic | x | √ |
| Privy | x | √ |
| Self Chain | √ | x |
| Walt.id | x | x |
| Web3Auth | √ | √ |

## Sicherheit mit Mehrparteienprinzip

Das Mehrparteienprinzip, im Englischen Multi-Party Computation (MPC), basiert auf den Prinzipien der Kryptographie, wobei mehrere Teilnehmer an einer Aufgabe beteiligt sind [16]. Mehrpartei-Wallets benutzen die Technologie, wobei mehrere Server jeweils nur einen Teil des privaten Schlüssels speichern. Ein anderer Ansatz wäre, dass die Server private Informationen halten, welche nur der Nutzer entschlüsseln kann [17]. Mit Hilfe dieses Systems kann nur der Benutzer die privaten Schlüssel benutzen ohne, dass er die Schlüssel selbst verwalten muss. WaaS-Unternehmen benutzen diese Technologie für ihre Wallets um sichere Non-Custodial-Wallets für Nutzer zu erschaffen. Das Unternehmen selbst hat bei solchen Wallets keinen Zugriff auf die privaten Schlüssel der Nutzer.

Abbildung 3 stellt eine Visualisierung dieser Funktion anhand von drei Schlüsseln dar. Je nach Implementierung sind für die Berechnung des richtigen privaten Schlüssels jeweils 1 bin n Teilschlüssel notwendig.

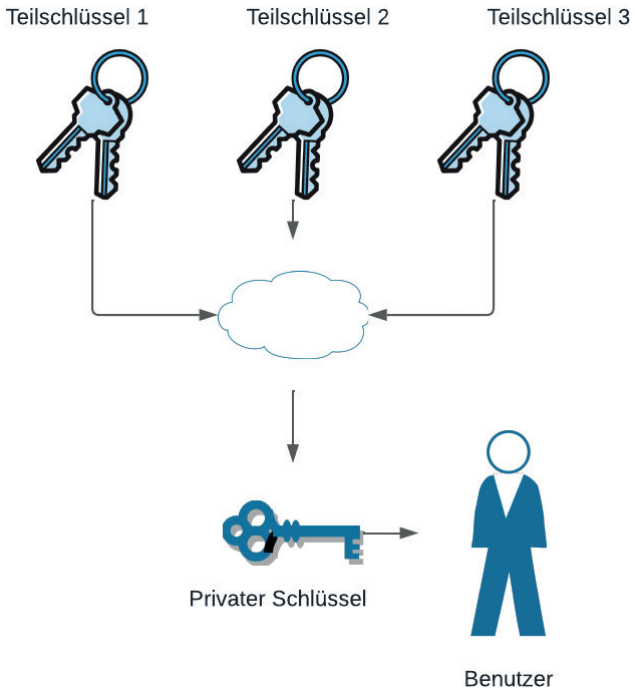



*Abbildung 3: Mehrpartei-Wallet (vereinfacht)*

## Gebührenübernahmeautomatik

Der Ethereum Standard ERC-4337 führte die Funktionalität von Gebührenübernahme-automatik, im Englischen Paymaster, ein [18]. Diese sind smart contracts, welche Kosten von Transaktionen bezahlen, ohne, dass der Benutzer für diese haften muss. Im klassischen Sinn sind hierfür Account-Abstraction-Wallets notwendig. Zum Vereinfachen wird in dieser Studie der Begriff der Gebührenübernahmeautomatik mit der Funktionalität für Transaktionen anderer Teilnehmer zu bezahlen gleichgesetzt. Somit beinhaltet der Begriff ebenso Funktionalitäten von Tankstellen, im Englischen Gas Stations [6]. Solche Gas Stations beinhalten Blockchain spezifische Tokens, welche zum Bezahlen von Transaktionen benutzt werden können.

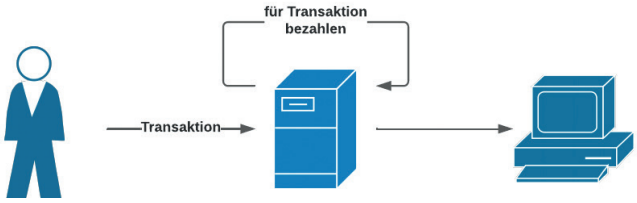



*Abbildung 4: Gebührenübernahmeautomatik (vereinfacht)*

*Anwendungsbeispiel*

Angenommen eine Firma benutzt Ethereum als Blockchain. Diese Firma benutzt WaaS-Wallets für ihre Benutzer. Als Treueprogramm verschenkt die Firma eigene Treue-ERC-20-Tokens an Ihre Kunden. Möchte nun ein Kunde die Tokens an eine andere Wallet verschicken, werden hier Transaktionskosten berechnet, welche in ETH, dem Ethereumnativen Token, bezahlt werden müssen. Hat die Firma aber eine Gebührenübernahmeautomatik eingebaut, so werden die Transaktionskosten von dieser bezahlt. Der Kunde muss somit keine ETH-Tokens auf die neue Kundenwallet überweisen und kann direkt die Treue-ERC-20-Tokens verschicken.

Diese Funktionalität stellt eine nahtlose Interaktion vom Benutzer und Blockchain dar und fördert die Benutzerfreundlichkeit. Zu beachten ist jedoch, dass bei solchen Anwendungen das Unternehmen, welches WaaS-Wallets benutzt für die Kosten aufkommen muss.

## Unterstütze Blockchains

Für Unternehmen ist die Blockchain auf welcher programmiert wird von besonderer Bedeutung, insbesondere wenn es um die Programmiersprache und die Funktionalitäten von Blockchains geht. Somit ist ein wichtiger Aspekt die unterstützen Blockchains, welche WaaS anbieten. In Tabelle 3 ist eine Übersicht aufgelistet welche Blockchains jeweils unterstützt werden.

Auffallend ist, dass bei Walt.id keine Blockchain steht. Der Grund ist, dass IOTA die einzige unterstütze Blockchain war, welche nicht den aktuellen Anforderungen mehr entspricht. Das Walt.id Wallet Kit wird ebenso im Jahr 2024 abgestellt [19]. Somit wird im weiteren Verlauf Walt.id nicht weiter verglichen.

Außerdem steht unter Privy „alle EVM-kompatible Blockchains". EVM steht für Ethereum Virtual Machine und definiert die Programmiersprache und Funktionsweise der Ethereum Blockchain. EVM-kompatible Blockchains sind Blockchains welche den Prinzipien von Ethereum folgen und den Gleichen EVM code lesen und verarbeiten können [20]. Solche Blockchains wären zum Beispiel Arbitrum, Polygon, Optimism und viele weitere Blockchains [21].

**Tabelle 3: Unterstützte Blockchains [(E) = eingeschränkt]**

| WaaS | Unterstütze Blockchains |
|---|---|
| Circle | Ethereum, Polygon, Avalanche (E) |
| Coinbase -WaaS | Arbitrum, Avalanche C-Chain, Base, Binance Smart Chain, Ethereum, Fantom Opera, Gnosis, Optimism, Polygon |
| Crossmint | Apex (E), Aptos (E), Arbitrum One, Arbitrum Nova, Astar zkEVM, Base, BSC, Etherum (E), Optimism, Polygon, Solana, Sui (E), Zora |
| Fireblocks | Arbitrum, Astar, Aurora_dev, Avalanche (C-Chain), Axelar, Base, Bitcoin, BSC, Canto, Celestia, Celo, Chiliz, Cosmos, dYdX, Etherum, Evmis, Fantom, HAT Chain, KAVA, Linea, Matic, Moonbeam, Miinriver, Oasys, Osmosis, Ronin, RSK, Shimmer, SmartBCH, Songbird, TokenX, TRON, Velas, XDC Network, zkEVM, Solana, Algorand |
| Fordefi | Bitcoin, Cosmos Hub, Akash, Archway, Axelar, Celestia, dYdX, Dymension, Noble, Osmosis, Sei, Stride, Solana, Arbitrum One, Avalanche, Base, BNB, Blast, Canto, Conflux, Dymension, Ethereum, Fantom, Gnosis, Kava, Linea, Manta Pacific, Mantle, Merlin, Optimism, Polygon, Polygon zkEvm, Scroll, Xai, zkLink Nova, zkSync Era |
| Magic | Polygon, Ethereum, Solana, Flow, Aptos, Algorand, Arbitrum, Avalanche, Base, BSC, Bitcoin, Celo, Chiliz, Cosmos, Cronos, Fantom, Harmony, Hedera, ICON, Loopring, Moonbeam, Neat, Optimism, Polkadot, Tezos, ZetaChain, Ziliqa |
| Privy | alle EVM-kompatible Blockchains |
| Self Chain | Self Chain |
| Walt.id | - |
| Web3Auth | alle secp256k1 & ed25519 curve Blockchains, Ethereum, Arbitrum, Avalanche, Base, BSC, Celo, Cronos, Flare, Harmony, Klaytyn, Moonbeam, Moonriver, Neon, Optimism, Polygon, SKALE, Songbird, zkEVM, zKyoto, Solana, XRPL, Algorand, Aptos, Cosmos, ImmuTabelleX, Near, Polkadot, Polymesh, StarkEx, StarkNet, Tezos |

## WaaS-Kosten

WaaS-Kosten tragen nicht dazu bei, wie die Benutzerinteraktion mit der Benutzeroberfläche aussieht und wie Benutzerfreundlich diese ist. Jedoch sind diese Werte für ein Unternehmen, welches solche Infrastrukturen einbauen von großer Bedeutung. Tabellen 4-6 vergleicht diese Kosten, wobei erkennbar ist, dass unterschiedliche WaaS-Unternehmen ver-schiedene Kostenpläne verfolgen. In diesen Tabellen ist auffällig, dass bei Self Chain keine Daten angegeben werden, dies ist darauf zurückzuführen, dass das Unternehmen noch in der Anfangsphase ist und in Zukunft die Implementierungen vornehmen wird. Walt.id wird auf Grund der Schließung der Wallet nicht berücksichtig.

Diese Kosten stehen allein zum Vergleich und werden nicht in den Faktor Benutzerfreundlichkeit miteinberechnet.

**Tabelle 4: WaaS-Kosten von Circle und Magic (Kosten pro Wallet)**

| WaaS | <1.000 | <5.000 | <10.000 | <25.000 | <50.000 | <100.000 | <250.000 | >250.000 |
|---|---|---|---|---|---|---|---|---|
| Circle | 0$ | 0,05$ | 0,047$ | 0,04$ | 0,035$ | 0,03$ | 0,025$ | 0,02$ |
| Magic | 0$ | 0,05$ | 0,1$/ individuell | 0,1$/ individuell | 0,1$/ individuell | 0,1$/ individuell | 0,1$/ individuell | 0,1$/ individuell |

**Tabelle 5: WaaS-Kosten von Privy, Web3Auth und Fireblocks (Kosten pro Monat)**

| WaaS | <1.000 | <2.500 | <10.000 | >10.000 |
|---|---|---|---|---|
| Privy | 0$ | 99$ | 299$ | individuell |
| Web3Auth | 0$ | 69$ (<3000) | 399$ | individuell |
| Fireblocks | 500-550$ | 500-550$ | 500-550$ (<7.500) | individuell |

**Tabelle 6: WaaS-Kosten von Coinbase-WaaS, Crossmint, Fordefi, Self Chain und Walt.id**

| WaaS | Kosten |
|---|---|
| Coibase-WaaS | 39$ für 300.000 tägliche API-Interaktionen, sonst individuell |
| Crossmint | individuell |
| Fordefi | individuell |
| Self Chain | - |
| Walt.id | - |

## Developerfreundlichkeit

Developerfreundlichkeit spielt eine essenzielle Rolle, wenn es um den Erfolg des Unternehmens geht. Wenn eine schnelle Implementierung notwendig ist, so ist eine einfache Developeroberfläche erwünscht. Solche Oberflächen tragen auch dazu bei, dass weniger Fehler entstehen und das System robuster ist. Bei WaaS-Wallets, welche kostenlose Pläne anbieten (sehe Tabelle 4) wurden Demos erstellt, um die Developerfreundlichkeit zu testen.

## Unterstütze Frameworks

Je nach Erfahrungen, Kenntnissen und Spezialisierungen von Programmieren sind die unterstützen Frameworks der WaaS-Unternehmen zu beachten. Tabelle 7 listet alle unterstützten Frameworks auf der folgenden Seite auf.

**Tabelle 7: WaaS – Unterstützte Frameworks und SDKs**

| WaaS | Frameworks und SDKs |
|---|---|
| Circle | REST APIs, iOS, Android, React Native, Node.js, web SDK (Javascript) |
| Coinbase-WaaS | viem, React |
| Crossmint | React, iOS SDK, Android SDK |
| Fireblocks | Rest API, JacaScript, Python, Java, Rust |
| Fordefi | Ract Native, Android >=v7.0, iOS >=v13 |
| Magic | Javascript, React Native, Android, iOS, Flutter, Unity,Server side SDK |
| Privy | NextJS, React, React Native |
| Self Chain | - |
| Walt.id | - |
| Web3Auth | React, Next JS, React Native, Vue, Angular, Javasript, Web SDK, Android SDK, iOS SDK, Flutter, Unity |

Hierbei ließe sich mit Magic, Privy und Web3Auth am schnellsten eine funktionierende Demo erstellen. Während der Implementierungsphase waren die Server von Corssmint nicht zu erreichen und somit konnte hierbei keine Demo erstellt werden. Ein Serverausfall erzeugt eine Unzuverlässigkeit und spiegelt sich negativ auf das Unternehmen wider.

Des Weiteren wurde eine Demo mit der Circle-Wallet entwickelt, wohingegen der Developer-aufwand höher ist als bei den Konkurrenten, wobei der Programmierer mehr Kontrolle über die Wallets hat.

## Handhabbarkeit

Um Blockchain Anwendungen ohne weiteren Aufwand an den Nutzer zu bringen ist eine nahtlose Interaktion von großer Bedeutung. Somit gilt, dass je einfacher ein System zu benutzen ist, desto wahrscheinlicher ist es, dass Benutzer mit diesem Interagieren. Alle in der Studie genannten Wallets versprechen Möglichkeiten, dass der Nutzer sich über gewohnte Web2 Login Optionen anmelden kann. Besonders im Umgang mit der Wallet tritt die Funktionalität einer Gebührenübernahmeautomatik dazu bei, dass der Nutzer sich nicht um die Blockchain spezifischen Transaktionen kümmern muss.

Für Benutzer welche erfahrener mit Blockchain sind könnte die Verwendung einer häufig benutzten oder nachhaltigen Blockchain (Tabelle 3) dazu beisteuern, dass die Benutzer mit höherer Wahrscheinlichkeit mit dem System interagieren.

# Schlussfolgerung

Untersucht wurden WaaS-Funktionalitäten, Kosten, unterstützte Blockchains und Frameworks, und die Benutzer und Developerfreundlichkeit. Speziellen Wert wurde auf die Benutzerfreundlichkeit gelegt, denn diese ist ausschlaggebend zum Erfolg eines Unternehmens, welche WaaS-Wallets anbieten. Eine nahtlose Interaktion kann mit Hilfe von einer Gebührenübernahmeautomatik verbessert werden, wobei folgende Wallets diese unterstützen: Circle, Coinbase WaaS, Crossmint, Magic, Privy und Web3Auth. Von diesen sechs WaaS-Unternehmen war eine gute Implementierung ohne Server Fehlern bei Circle, Magic, Privy und Web3Auth möglich. Von diesen vier WaaS-Wallets unterscheidet sich Circle darin, dass diese einen größeren Programmieraufwand erfordert, um die Sicherheit und Interaktion der Wallet zu gewährleisten. Ein größerer Programmieraufwand kann als negativ angesehen werden, wohingegen eine größere Kontrolle für manche Unternehmen erwünscht sein könnten. Ein negativer Aspekt von Circle wäre hierbei, dass nur zwei Blockchains voll unterstützt werden, wohingegen Magic, Privy und Web3Auth über 10 Blockchains unterstützen.

Im Folgenden werden verschiedene Szenarien aufgelistet und die dazu passenden WaaS-Wallets.

Ein Produkt wird schnell entwickelt, welches Grundfunktionalitäten einer Blockchain-Wallet beinhaltet:

- Magic, Privy und Web3Auth

Hohe Kontrolle über Wallet-Management und Arbeitsablauf ist erwünscht:

- Circle und Fireblocks

NFTs sind ein wichtiger Aspekt des finalen Produktes. Eine leichte Integrierung mit verschiedenen Funktionalitäten ist hierbei gefragt:

- Magic und Corssmint (wobei Crossmint in der Vergangenheit von Serverausfällen betroffen war)

# Referenzen


[1] Hajjar, B. J. (n.d.). What's a DEFI wallet & how to choose the right one for my business. RIF. https://rif.technology/content-hub/defi-wallet/ (Zuletzt aufgerufen am: 2024, Mai 09)

[2] Bruck, C. (n.d.). „zahlungsverkehr 4.0" - welche auswirkungen hat das ... Zahlungsverkehr 4.0. https://www.bearingpoint.com/files/Studienergebnisse_BearingPoint_Studie_Zahlungsverkehr_4.0.pdf?download=0&itemId=386092 (Zuletzt aufgerufen am: 2024, Mai 10)

[3] Suratkar, S., Shirole, M., & Bhirud, S. (2020, September). Cryptocurrency wallet: A review. In 2020 4th international conference on computer, communication and signal processing (ICCCSP) (pp. 1-7). IEEE.

[4] Merten, L. (2023, November 13). Was sind Custodial Wallets?. Blockchainwelt. https://blockchainwelt.de/Custodial-wallet/ (Zuletzt aufgerufen am: 2024, Mai 10)

[5] Editor, B. (2023, November 21). What is wallet-as-a-service (WAAS)?. Medium. https://blog.bitgo.com/what-is-wallet-as-a-service-waas-a44f84fe8d70 (Zuletzt aufgerufen am: 2024, Mai 11)

[6] Programmable wallets: Wallet as a Service. Circle. (n.d.). https://www.circle.com/en/programmable-wallets (Zuletzt aufgerufen am: 2024, Mai 12)

[7] Embedded wallets - coinbase developer platform. Embedded Wallets - Coinbase Developer Platform. (n.d.). https://www.coinbase.com/de/developer-platform/products/embedded-wallets (Zuletzt aufgerufen am: 2024, Mai 12)

[8] Custodial NFT wallets: Embedded wallets as a Service. Custodial NFT Wallets | Embedded Wallets as a Service. (n.d.). https://www.crossmint.com/products/Custodial-wallet-as-a-service (Zuletzt aufgerufen am: 2024, Mai 12)

[9] Wallets as a service. Fireblocks. (2024, March 19). https://www.fireblocks.com/platforms/wallets-as-a-service/ (Zuletzt aufgerufen am: 2024, Mai 12)

[10] Wallet as a Service. Wallet as a service. (n.d.). https://www.fordefi.com/wallet-as-a-service (Zuletzt aufgerufen am: 2024, Mai 12)

[11] The leading wallet-as-a-service plus essential NFT capabilities. Magic. (n.d.). https://magic.link/ (Zuletzt aufgerufen am: 2024, Mai 12)

[12] Onboard all your users to web3. Privy. (n.d.). https://www.privy.io/ (Zuletzt aufgerufen am: 2024, Mai 12)

[13] Self chain. Self Chain. (n.d.). https://selfchain.xyz/ (Zuletzt aufgerufen am: 2024, Mai 12)

[14] Powerful digital identity and wallet infrastructure. walt.id. (n.d.). https://walt.id/ (Zuletzt aufgerufen am: 2024, Mai 12)

[15] Web3Auth. (n.d.-b). Key management sdks with MPC and AA enabled. https://web3auth.io/ (Zuletzt aufgerufen am: 2024, Mai 12)

[16] Goldreich, O. (1998). Secure multi-party computation. Manuscript. Preliminary version, 78(110), 1-108.

[17] What is MPC (Multi-Party Computation)?. Fireblocks. (2022, November 21). https://www.fireblocks.com/what-is-mpc/ (Zuletzt aufgerufen am: 2024, Mai 18)

[18] Lin, Z., Wang, T., Zhao, C., Zhang, S., Yang, Q., & Shi, L. A Measurement Investigation of ERC-4337 Smart Contracts on Ethereum Blockchain.

[19] Introduction: Wallet kit. walt.id. (n.d.-a). https://docs.walt.id/v/web-wallet (Zuletzt aufgerufen am: 2024, Mai 19)

[20] Hildenbrandt, E., Saxena, M., Rodrigues, N., Zhu, X., Daian, P., Guth, D., ... & Rosu, G. (2018, July). Kevm: A complete formal semantics of the ethereum virtual machine. In 2018 IEEE 31st Computer Security Foundations Symposium (CSF) (pp. 204-217).IEEE.

[21] Top-Ethereum-ökosystem-Währungen nach Marktkapitalisierung. CoinGecko. (n.d.). https://www.coingecko.com/de/categories/ethereum-ecosystem (Zuletzt aufgerufen am: 2024, Mai 19)

# Autor

**Mikolaj Radlinski**

Fraunhofer-Institut für
Angewandte Informationstechnik FIT

# Experten

**Prof. Wolfgang Prinz, PhD**
Leiter des Blockchain Reallabors
Professor an der RWTH Aachen
Stellv. Institutsleiter am Fraunhofer FIT
Leiter für die Abteilung Kooperationssysteme

Fraunhofer-Institut für Angewandte Informationstechnik FIT

**Dr. Daniel Trauth**
Wissenschaftlicher Mitarbeiter

Fraunhofer-Institut für Angewandte Informationstechnik FIT

## Kontakt

Fraunhofer-Institut für Angewandte
Informationstechnik FIT
Schloss Birlinghoven
53757 Sankt Augustin
info@fit.fraunhofer.de
www.fit.fraunhofer.de