Bundesamt
für Sicherheit in der
Informationstechnik

Abschlussbericht Projekt 374

Sicherheitsuntersuchung ausgewählter Blockchain-Anwendungen

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: blockchain@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Einleitung 5
Kurzzusammenfassung der Studienergebnisse 6
1 Einführung in DLT am Beispiel Blockchain 7
1.1 Nachvollziehbarkeit 7
1.2 Abstreitbarkeit 7
1.3 Konsistenz 7
1.4 Eindeutigkeit 8
1.5 Ausgeglichenheit 8
2 Berücksichtigte Merkmale und Bewertungskriterien 9
2.1 Merkmale 9
2.2 Bewertung 12
2.2.1 Marktrelevanz und Bekanntheit 12
2.2.2 Reifegrad 13
2.2.3 Sicherheitsmechanismen/Softwarequalität 13
2.2.4 Evaluierbarkeit 14
2.2.5 Kryptographische Mechanismen 14
2.2.6 Performance/Skalierbarkeit 15
2.2.7 Nutzerfreundlichkeit 15
2.2.8 Sicherheitsvorfälle 16
2.2.9 Lizenzierung 16
2.2.10 Formale Sicherheitsnachweise 17
3 Auswertung der Ergebnisse 18
3.1 Arten von Angeboten 18
3.2 Herkunft 19
3.3 Lizenzierung 23
3.4 Marktrelevanz 25
3.5 Reifegrad 27
3.6 Performance 30
3.7 Sicherheit 31
4 Schlussfolgerungen 35
5 Auswahl der zu untersuchenden Produkte 37
6 Generelle Untersuchungsmethodik 40
6.1 Review des technischen Konzepts 40
6.2 Einrichtung einer Testumgebung 40
6.3 Statische Codeanalyse / Static Application Security Testing (SAST) 41
6.4 Abhängigkeiten-Analyse / Software Composition Analysis (SCA) 41

6.5 Manuelles Review des Quelltextes ... 41
6.6 Reverse Engineering ... 42
6.7 Dynamic Application Security Testing (DAST) ... 43
6.7.1 Fuzzing ... 43
6.7.2 Fehlererkennung ... 43
6.8 Analyse des Netzwerkverkehrs ... 44
7 Grundsätzliche Beobachtungen und typische Schwächen ... 45
8 Schlussfolgerungen ... 47

Einleitung

Seit der Veröffentlichung des Bitcoin-Whitepapers[1] im Jahr 2008 ist die Blockchain-Technologie, sowie darauf basierende Angebote und Produkte, ein wichtiges Thema im Diskurs von Wirtschaft, Politik und Gesellschaft. Als Reaktion auf diesen Trend veröffentlichte das BSI im Jahr 2018 das Positionspapier „Blockchain sicher gestalten“[2] und die Bundesregierung begann mit den Vorbereitungen für die Erstellung einer Blockchain-Bundesstrategie[3].

Da die Sicherheit und der sichere Einsatz dieser neuen Technologie ein zentraler Faktor ist, der den zukünftigen Erfolg bestimmt, entschloss sich das BSI dazu, eine Studie zur Sicherheit des Blockchain-Ökosystems durchführen zu lassen.

Im Rahmen dieser Studie sollte der Sicherheitsstand von aktuellen Blockchain-Angeboten umfassend untersucht werden. Dieses Ziel sollte in zwei Hauptarbeitspaketen erreicht werden. Zunächst sollte im Rahmen einer Marktanalyse ein umfassender Überblick über existierende Blockchain-Technologien erstellt werden (mindestens 300). Die ermittelten Technologien sollten bereits einer ersten Bewertung unterzogen werden, bei der insbesondere der erste Eindruck der verwendeten Sicherheitsmechanismen, die Softwarequalität und die bisher bekannt gewordenen Sicherheitsvorfälle einbezogen werden. Anschließend sollten, basierend auf den Ergebnissen der vorläufigen Bewertung, eine feste Anzahl von Blockchain-Angeboten (jedoch mindestens fünf) ausgewählt und anschließend einer umfassenden und detaillierten Sicherheitsanalyse unterzogen werden (dieses Arbeitspaket wird im Folgenden „AP5“ genannt). Dabei sollten möglichst verschiedene Arten von Angeboten, Anwendungsbereiche und Mechanismen abgedeckt werden, sowie eine angemessene Kombination aus theoretischen und praktischen Methoden angewendet werden. Zu den praktischen Methoden gehören beispielsweise Codeanalyse, Messungen, aktive und passive Seitenkanalangriffe, Fuzzing und Penetration Testing. Die Untersuchung beinhaltete als potenzielle Schwachstellen sowohl Programmfehler als auch Zufallszahlenerzeugung, Seitenkanäle, kryptographische Schwächen und weitere in Abstimmung mit vom BSI festzulegenden Aspekten.

Als Ergebnis dieser Studie sollte ein umfassendes IT-Security-Lagebild für Blockchain-Anwendungen entstehen, das durch eine fundierte Testmethodik gestützt wird.

[1] https://bitcoin.org/bitcoin.pdf

[2] Dieses wurde mittlerweile zu einem umfangreichen Leitfaden ausgebaut, siehe www.bsi.bund.de/Blockchain

[3] Diese Strategie liegt nun vor und kann unter www.bmwi.bund.de abgerufen werden.

Kurzzusammenfassung der Studienergebnisse

Im Rahmen dieser Studie konnten die folgenden wesentlichen Ergebnisse und Schlussfolgerungen erarbeitet werden:

- Über 25% aller Angebote aus dem Blockchain-Ökosystem stammen aus der USA. Aus Deutschland stammen nur 9 der im Rahmen der Marktanalyse ermittelten 303 Angebote (siehe Abschnitt 19).
- Mining-Software wird zum überwiegenden Teil von Privatpersonen entwickelt (71%, siehe Abschnitt 19).
- Ein wesentlicher Teil der verfügbaren Mining-Hardware stammt aus China (50%, siehe Abschnitt 19).
- Blockchain-Clients und Hardware-Wallets besitzen den höchsten durchschnittlichen Reifegrad, während Blockchain-Anwendungen am geringsten entwickelt sind (siehe Abschnitt 3.5).
- Nahezu keine Angebote können einen formalen Sicherheitsnachweis vorweisen (siehe Abschnitt 31).
- Die meisten der acht detailliert untersuchten Blockchain-Angebote besitzen ein hohes Sicherheitsniveau und im Rahmen des verfügbaren Untersuchungsaufwands dieser Studie konnten keine schwerwiegenden Schwachstellen gefunden werden.
- Ein detailliert untersuchtes Angebot ist jedoch fundamental unsicher, ein weiteres ist anfällig gegenüber Phishing-Angriffen.
- Alle gefundenen Probleme wurden den jeweiligen Herstellern gemeldet. Reaktionen auf die Meldung von weniger kritischen Schwachstellen waren überwiegend positiv. Auf die Meldung der beiden kritischen Probleme erfolgte jeweils keine Reaktion. Keines der in diesen Fällen gemeldeten Probleme ist nach unserem aktuellen Kenntnisstand behoben.
- Grundsätzliche Probleme, die im Rahmen dieser Studie aufdeckt wurden, sind der hohe Grad an gemeinsam verwendeten Code-Bausteinen zwischen den untersuchten Angeboten (insbesondere was kryptographische Verfahren angeht), die ungewöhnliche Wahl der kryptographischen Primitiven sowie die hohe Anzahl an Abhängigkeiten zu externen Programmbibliotheken, die in veralteten Versionen (teilweise mit bekannten Sicherheitslücken) eingesetzt werden (siehe Abschnitt 7).

Um ein tiefergehendes Verständnis der Sicherheitseigenschaften von existierenden Blockchain-Angeboten zu erlangen, bietet sich aufbauend auf dieser Studie insbesondere die Untersuchung der sogenannten „Bitcoin Improvement Proposals“ (ein de-facto Standard im Blockchain-Ökosystem) und deren Implementierungen an.

1 Einführung in DLT am Beispiel Blockchain

Die Blockchain-Technologie erlangte zuerst Bekanntheit über die kryptographische Währung „Bitcoin". Wenn man über Sicherheitsmechanismen und Sicherheitsgarantien der Blockchain redet, meint man in der Regel die Blockchain, wie sie von Bitcoin benutzt wird. Im Folgenden werden daher die wichtigsten Entwurfsziele von Bitcoin genannt und es wird erklärt, welche Mechanismen der Blockchain zusammen mit welchen Annahmen diese Ziele erreichen. Das Blockchain-Netzwerk besteht aus einer Menge unabhängiger Teilnehmer, die miteinander über „Rundrufe" (broadcasts) kommunizieren. Wesentliche Entwurfsmerkmale der Blockchain-Technologie sind der Verzicht auf zentrale Instanzen, ein Konsensmechanismus und die Unveränderbarkeit der Blockchain. Im Folgenden werden die wesentlichen Ziele der Bitcoin-Blockchain skizziert. Für weiterführende Informationen sei auf den im Mai 2019 veröffentlichten Leitfaden „Blockchain sicher gestalten" des BSI verwiesen.

1.1 Nachvollziehbarkeit

Nachvollziehbarkeit wird in Bitcoin dadurch erreicht, dass alle Bezahlvorgänge als eine Transaktion eines gewissen Betrags zwischen einem Sender und einem Empfänger organisiert werden. Diese Transaktionen werden zunächst in Blöcken zusammengefasst und anschließend an alle Teilnehmer des Bezahlsystems übermittelt. Jeder Teilnehmer speichert diese Blöcke lokal in einer stetig wachsenden Liste. Da jeder Teilnehmer über die vollständige Transaktionsliste verfügt, ist die Korrektheit jeder einzelnen Transaktion nachvollziehbar.

1.2 Abstreitbarkeit

Während es in konventionellen Währungen unmöglich ist, das (Bar-)Geld einer fremden Person auszugeben, ist es in einem System, in dem Zahlungen nur als eine elektronische Transaktion repräsentiert sind, durchaus denkbar, dass Transaktionen in fremdem Namen verfasst werden. Bitcoin löst dieses Problem dadurch, dass alle Transaktionen von dem Sender kryptographisch signiert werden. Teilnehmer werden durch eine Adresse identifiziert, die aus ihrem öffentlichen Schlüssel abgeleitet wird. Unter der Annahme, dass kein Angreifer Signaturen fälschen kann, können Teilnehmer nur über Geld verfügen, das sie selbst in Form von Transaktionen erhalten haben.

1.3 Konsistenz

In konventionellen Bezahlsystemen autorisieren Banken als zentrale Institutionen Transaktionen und wachen so darüber, dass ein Kontoinhaber nur das Geld ausgeben kann, über das er verfügt. In einem dezentralen System können Teilnehmer Geld mehrfach ausgeben („double spending"), wenn Transaktionen nicht überprüft werden. Um Transaktionen zu autorisieren, prüft sie ein (beliebiger) Teilnehmer auf Richtigkeit und fasst mehrere Transaktionen in einem Block zusammen. Zusätzlich enthält ein bestätigter Block immer die eindeutige Information darüber, welcher Block der Vorgängerblock war – also auf der Basis welchen „Kontostands" aller Teilnehmer die in dem Block enthaltenen Transaktionen bestätigt wurden. Um einen solchen Block in die Blockchain eintragen zu können, muss der Teilnehmer außerdem eine signifikante Menge an Rechenleistung aufbringen und den Beleg dafür – den Proof of Work – an den Block anfügen. Der Proof of Work bedingt zweierlei. Zum einen ist das Erstellen von Blöcken an die Investition von Rechenzeit gebunden: Das Autorisieren von Transaktionen kostet Strom. Zum anderen „bremst" der Proof of Work die Erstellung neuer Blöcke: Kein Teilnehmer kann beliebig schnell neue Blöcke erzeugen. Nur dann, wenn ein Angreifer – oder ein Zusammenschluss mehrerer Angreifer – in etwa die Hälfte der gesamten Rechenleistung des Netzwerks kontrolliert, kann er frei diktieren, welche Transaktionen validiert werden und welche nicht. Ist eine Transaktion bereits eine gewisse Zeit in der Blockchain verewigt, ist es fast unmöglich, sie durch eine neue Transaktionsgeschichte zu überschreiben – solange der Proof of Work hinreichend „schwer" zu erbringen ist und solange ehrliche Teilnehmer die Mehrheit der Rechenleistung stellen.

1.4 Eindeutigkeit

Da es jedem Teilnehmer prinzipiell möglich ist, einen neuen Block zu schaffen und es ihm freigestellt ist, welche Transaktionen er dabei berücksichtigt, kann es jederzeit dazu kommen, dass unterschiedliche Blöcke mit dem gleichen Vorgängerblock veröffentlicht werden – die Blockkette bekommt also einen neuen Strang. Um zu verhindern, dass der Zustand der Blockchain auf diese Weise divergiert, gilt die einfache Regel, dass neue Blöcke immer am aktuell längsten Strang der Blockchain angehängt werden müssen. Halten sich mehr als 50% aller Teilnehmer an dieses Prinzip, ist es einem Angreifer nicht möglich, einen neuen (bösartigen) Strang in der Blockchain zu erzeugen, der von anderen Teilnehmern anerkannt wird.

1.5 Ausgeglichenheit

Das bisher beschriebene System bietet für Teilnehmer keinen Anreiz, sich an der Verifizierung von Blöcken zu beteiligen. Der Proof of Work erfordert die Investition von Rechenzeit, die sich nicht lohnt, wenn man nicht eine selbstgemachte Transaktion bestätigt wissen will. Um dieses Problem zu lösen, erhalten Teilnehmer nach der Bestätigung eines Blocks eine Belohnung in Form neu geschaffener („abgebauter“ oder „geschürfter“) Bitcoins. Zusätzlich ist es dem Sender ebenfalls möglich, für die Bestätigung seiner Transaktion eine Belohnung zu vergeben.

2 Berücksichtigte Merkmale und Bewertungskriterien

2.1 Merkmale

Im Blockchain-Ökosystem gibt es eine nahezu unüberschaubare Vielzahl von unterschiedlichen Angeboten[4]. Die 303 Angebote, die im Rahmen der Marktanalyse betrachtet wurden, wurden daher zunächst hinsichtlich ihrer Art kategorisiert. Dafür wurden die folgenden Klassen berücksichtigt:

Basistechnologie	Unter einer Basistechnologie verstehen wir eine Blockchain-Technologie, deren Ziel und Zweck die Verwendung als Plattform oder Framework für die Erstellung von weiteren, auf der Technologie aufbauenden Anwendungen ist. Die Abwicklung von Zahlungsverkehr ist insbesondere in der Technologiekonzeption nicht vorgesehen. Ein prominentes Beispiel dafür ist „Hyperledger“, eine Blockchain-Lösung, die die Digitalisierung von Unternehmensprozessen vereinfachen soll. Merkmale von Basistechnologien unterscheiden sich häufig hinsichtlich ihrer Konsensverfahren und ihres Rechtemanagements, bieten jedoch fast immer eine Form von „Smart Contracts“ an, die zur Realisierung von weiterführenden Anwendungen auf Basis der Blockchain genutzt werden können.
Digitale Währung	Unter einer Digitalen Währung verstehen wir eine Blockchain-Technologie, deren Ziel und Zweck ausschließlich die Abwicklung und Dokumentation von digitalem Zahlungsverkehr ist. In Abgrenzung zu einer Basistechnologie bietet eine Digitale Währung selbst keine Mechanismen, um weiterführende Anwendungen zu realisieren, sondern ist auf die Verwaltung von sogenannten „Coins“ ausgerichtet, die wie ein digitales Abbild einer Münze verstanden werden können. Das prominenteste Beispiel für eine digitale Währung ist „Bitcoin“ das in seiner ursprünglichen Konzeption explizit dafür entwickelt wurde, digitalen Zahlungsverkehr zu realisieren. Auch wenn es einige Anwendungen gibt, die die Bitcoin-Blockchain als sicheren Datenspeicher nutzen, ist die Nutzung in dieser Form nicht offiziell vorgesehen. Bitcoin selbst bietet insbesondere keine ausreichend ausdrucksmächtigen Smart Contracts an, die geeignet sind, weiterführende Anwendungen zu realisieren. Eine eindeutige Trennung von Blockchain-Angeboten in Basistechnologien und digitalen Währungen ist jedoch nicht immer möglich. „Ethereum“ ist beispielsweise sowohl als digitale Währung konzipiert als auch – über den Mechanismus der Smart Contracts – als Basistechnologie zur Realisierung von weiterführenden Anwendungen. Fälle, bei denen keine eindeutige Differenzierung möglich ist, wurden in der Auswertung entsprechend gekennzeichnet.
Blockchain-Anwendung	Unter einer Blockchai□n-Anwendung verstehen wir Angebote, die auf der Grundlage einer Basistechnologie (oder ggf. einer digitalen Währung) eine zusätzliche Dienstleistung anbieten. Blockchain-Anwendungen werden in der Regel als Smart Contract realisiert, können aber auch eine bereits bestehende Blockchain als Datenspeicher nutzen oder in anderer Form damit interagieren. Bekannte Beispiele für Blockchain-Anwendungen sind die sogenannten „dApps“ – Anwendungen, die auf Basis der Ethereum-Blockchain entwickelt werden. Von Blockchain-Anwendungen angebotene Dienstleistungen werden häufig über

[4] Unter Angeboten im Sinne dieser Studie verstehen wir alle Produkte und Technologien, die mit dem Blockchain-Ökosystem in Verbindung stehen. Im Folgenden verwenden wir dafür die Begriffe „Angebot“, „Produkt“ und „Technologie“ synonym.

	sogenannte „Token“ bezahlt. Token sind eine in der Regel über einen Smart Contract realisierte Form von Digitaler Währung, die – unabhängig von der zugrundeliegenden Basistechnologie – für eine einzelne Anwendung genutzt werden kann. Token werden in der Regel genauso gegen Echtgeld gehandelt, wie die „Coins“ einer Digitalen Währung.
Blockchain-Client	In diese Kategorie fällt jede Software, die dafür geeignet ist, aktiv an einem Blockchain-Netzwerk teilzunehmen (als sogenannte „Full Node“). Das bedeutet, dass der Client auch dazu geeignet sein muss, selbst Transaktionen zu verifizieren und „Mining“ zu betreiben. Ein bekanntes Beispiel hierfür ist „Bitcoin Core“, der offizielle Client zur Teilnahme an der Bitcoin-Blockchain.
Mining-Software	In Abgrenzung zu Blockchain-Clients ist Mining-Software nur dazu geeignet, für eine oder mehrere Blockchain-Technologien Mining zu betreiben. Insbesondere bietet Mining-Software in der Regel keine Funktionalitäten zum Durchführen von Transaktionen.
Mining-Hardware	Mining-Hardware ist spezialisierte Hardware, die speziell dafür entwickelt wurde, Mining in einem (oder manchmal auch mehreren) Blockchain-Netzwerken zu betreiben.
Blockchain-Wallet (Hardware)	In diese Kategorie fallen alle hardwarebasierten Produkte, deren Zweck die sichere Speicherung des zur Teilnahme an einer Blockchain notwendigen Schlüsselmaterials ist. In der Regel wird von einer einzelnen Blockchain-Wallet die Speicherung von Schlüsselmaterial für mehrere verschiedene Digitale Währungen oder Basistechnologien unterstützt. Ein bekanntes Beispiel ist „Trezor“.
Blockchain-Wallet (Software)	Schlüsselmaterial wird nicht nur mithilfe sicherer Hardware gespeichert, sondern häufig auch in Software. Anders als Hardware-Wallets bieten softwarebasierte Lösungen häufig noch weitere Funktionalität, die über die reine Speicherung hinausgeht, wie beispielsweise das Auslösen von Transaktionen.
Wallet-Generatoren	Obwohl so gut wie alle Blockchain-Clients und viele softwarebasierte Blockchain-Wallets bereits in der Lage sind, das Schlüsselmaterial zur Erzeugung des Wallets selbst zu generieren, existiert dennoch eine weitere Klasse an Angeboten, die sich ausschließlich der Generierung von Wallets widmet. Meistens handelt es sich dabei um Web-Applikationen, bei denen sich Nutzer auf Knopfdruck neue Wallets generieren lassen können. In der Regel bieten Wallet-Generatoren darüber hinaus keine weitere Funktionalität.

Die meisten Klassen von Angeboten sind nur für einen bestimmten Anwendungszweck geeignet – beispielsweise für das Speichern von Wallets. Blockchain-Anwendungen (aber in bestimmten Fällen auch Basistechnologien und Digitale Währungen) existieren jedoch für vielfältige Einsatzzwecke, die von der Realisierung eines digitalen Grundbuchs über das Erfassen aller Stationen der Lieferkette eines Produktes bis hin zur Abwicklung von Transaktionen in lokalen Energiemärkten reichen. Die Auswahl der im Rahmen dieser Studie betrachteten Anwendungsfelder erfolgte in Anlehnung an die Anwendungsfelder, die im Konsultationspapier der Bundesregierung im Rahmen der Blockchain-Strategie vorgestellt wurden[5]. Folgende Anpassungen wurden daran vorgenommen:

- Zusammenfassung von Internet of Things (IoT) und Industrie 4.0: Die beiden Anwendungsfälle lassen nach unserer Auffassung nicht getrennt voneinander definieren, da das Internet of Things eine der Grundlagen der Industrie 4.0 darstellt. Anwendungen, die für den Einsatz im IoT ausgelegt sind, lassen

[5] Die finale Version der Blockchain-Strategie ist erst nach der Durchführung der wesentlichen Teile dieser Studie erschienen. Darin findet sich keine explizite Auflistung von potenziellen Anwendungsfeldern mehr. Stattdessen fokussiert die Strategie konkrete Umsetzungsprojekte in den Bereichen Verwaltung, Gesundheit, digitale Identitäten, Logistik und Bildung.

sich somit auch häufig auf Industrie 4.0 anwenden. Umgekehrt basieren Anwendungen für den Einsatz im Rahmen von Industrie 4.0 häufig auf dem Internet of Things.

- Erweiterung von Logistik zu „Supply Chain Management“: Unserer Auffassung nach ist der Begriff Logistik zu eng gefasst. Anwendungen, die sich beispielsweise mit nachvollziehbaren Lieferketten beschäftigen, würden klassischerweise nicht dem Begriff Logistik zugeordnet werden. Im Blockchain-Kontext sind das jedoch häufige Anwendungsfälle. Im Rahmen dieser Studie erweitern wir daher das Anwendungsfeld Logistik zu Supply-Chain-Management. Dieser Begriff umfasst sowohl Angebote im Kontext von Lieferketten als auch im Bereich der Logistik.
- Einführung des zusätzlichen Anwendungsfelds „Spiel“: Im Rahmen der Marktanalyse hat sich herausgestellt, dass es zahlreiche blockchain-basierte Spiele gibt, die den im Konsultationspapier vorgeschlagenen Anwendungsfeldern bisher nicht zugeordnet werden können.

Insgesamt wurden daher Anwendungen, Basistechnologien und Digitale Währungen (falls möglich) den folgenden Anwendungsfeldern zugeordnet:

- Finanzsektor
- Rechtemanagement
- Verwaltung
- IoT / Industrie 4.0
- Supply-Chain-Management
- Identitätsmanagement
- Energie
- Datenspeicher
- Gesundheit
- Spiel
- Plattformökonomie
- Mobilität

Alle Anwendungen, Basistechnologien und Digitalen Währungen, die sich keinem der dargestellten Anwendungsfelder zuordnen ließen, wurden unter der Kategorie „Sonstiges“ zusammengefasst.

Zusätzlich zu den oben genannten Produktmerkmalen wurden für Basistechnologien, Digitale Währungen und Blockchain-Anwendungen (falls möglich und sinnvoll) noch die folgenden Fragestellungen beantwortet:

- **Berechtigungsmodell**: Wer kann Informationen in der Blockchain einsehen und abspeichern?
- **Grad der Dezentralisierung**: Ist die Blockchain vollständig dezentral oder benötigt sie bestimmte zusätzliche Vertrauensanker?
- **Konsensmodell**: Welches Verfahren zur Sicherstellung eines Konsenses wird in dem verteilten Netzwerk angewendet?
- **Smart Contracts**: Erlaubt die Blockchain den Einsatz von Smart Contracts und wenn ja in welcher Form?
- **Gespeicherte Informationen**: Für welche Klasse von Informationen ist das Produkt gedacht?

Für alle Arten von Angeboten wurde außerdem noch die **Herkunft** des Angebots ermittelt. Bei Produkten, die von einer Firma hergestellt und vertrieben werden, wurde das Land des Firmenhauptsitzes ermittelt. In allen anderen Fällen wurde (beispielsweise anhand der Code-Beiträge auf Entwicklerplattformen) ermittelt, ob das Produkt von bis zu drei Privatpersonen entwickelt wird oder von einer Community (vier oder mehr Personen).

2.2 Bewertung

Nach Ermittlung der in Abschnitt 9 dargestellten Merkmale wurde für alle Angebote eine erste Bewertung anhand öffentlich verfügbarer Informationen vorgenommen. Dabei wurden die im Folgenden dargelegten Bewertungskriterien berücksichtigt. Falls zu einem Kriterium keine Information auffindbar war oder das Kriterium auf das Produkt nicht anwendbar war, wurde das Symbol „-“ eingetragen.

2.2.1 Marktrelevanz und Bekanntheit

In dieser Kategorie wurde auf einer Skala von 1 bis 5 bewertet, wie stark das betrachtete Angebot auf dem Markt (der Blockchain-Angebote) vertreten ist. *Objektive* Bewertungen in dieser Kategorie wurden für Digitale Währungen, Basistechnologien und Blockchain-Anwendungen sowie für Mining-Software vorgenommen. Basistechnologien und Digitale Währungen basieren in der Regel auf Coins, die auf dem Markt gehandelt werden und deren Wert daher objektiv bestimmbar ist und ein starkes Indiz für die Marktrelevanz des Angebots darstellt. Funktionalitäten, die von Blockchain-Anwendungen bereitgestellt werden, können in der Regel über Token in Anspruch genommen werden. Genau wie Coins, werden auch Token auf dem Markt gehandelt und dienen daher als geeigneter Bewertungsmaßstab für die Marktrelevanz der zugrundeliegenden Blockchain-Anwendung. In Summe wurde der folgende Bewertungsmaßstab angelegt:

Bewertungsmaßstab: Marktrelevanz und Bekanntheit	
Bewertete Arten von Angeboten: Basistechnologien, Digitale Währungen und Blockchain-Anwendungen	
Bewertung	***Kriterium***
1	Der Marktanteil des Coins/Tokens ist weniger als 0.2%.
2	Der Marktanteil des Coins/Tokens ist bei 0.2-0.9%.
3	Der Marktanteil des Coins/Tokens ist bei 1-9%.
4	Der Marktanteil des Coins/Tokens ist bei 10-30%.
5	Der Marktanteil des Coins/Tokens ist bei mehr als 30%.

Die Bewertung wurde im Monat Januar vorgenommen und an der Gesamtmarktkapitalisierung von 121.275.489.930 US-Dollar zum Stichtag des 17.1.2019 ausgerichtet.

Mining-Software wird in der Regel für einen spezifischen Mining-Pool eingesetzt. Die Berechnungsgeschwindigkeit des zugehörigen Mining-Pools ist daher ein geeigneter Indikator für die Marktrelevanz der Mining-Software. Daher wurde der folgende Bewertungsmaßstab eingesetzt:

Bewertungsmaßstab: Marktrelevanz und Bekanntheit	
Bewertete Arten von Angeboten: Mining-Software	
Bewertung	***Kriterium***
1	Die Mining-Software bedient einen Mining-Pool für eine oder mehrere Mining-Algorithmen mit einer Hash-Rate von weniger als 106 Hashes pro Sekunde.

2	Die Mining-Software bedient einen Mining-Pool für eine oder mehrere Mining-Algorithmen mit einer Hash-Rate im Bereich von 10^6 Hashes pro Sekunde.
3	Die Mining-Software bedient einen Mining-Pool für eine oder mehrere Mining-Algorithmen mit einer Hash-Rate im Bereich von 10^9 Hashes pro Sekunde.
4	Die Mining-Software bedient einen Mining-Pool für eine oder mehrere Mining-Algorithmen mit einer Hash-Rate im Bereich von 10^{12} Hashes pro Sekunde.
5	Die Mining-Software bedient einen Mining-Pool für eine oder mehrere Mining-Algorithmen mit einer Hash-Rate im Bereich von 10^{15} Hashes pro Sekunde.

Für alle anderen Arten von Angeboten war es im Rahmen des Arbeitsaufwands dieser Studie nicht möglich, zu einer objektiven Einschätzung der Marktrelevanz zu kommen, weil die Anzahl der Nutzer häufig nicht veröffentlicht wird und auch nicht anderweitig belastbar zu ermitteln ist. In diesen Fällen wurde eine *subjektive* Bewertung (ebenfalls von 1 bis 5) anhand der folgenden Kriterien vorgenommen:

- Anzahl der Google-Suchergebnisse
- Anzahl der Downloads im Google Play Store
- Anzahl der Diskussionen in einschlägigen Foren
- Informationen in Sekundärliteratur

2.2.2 Reifegrad

Der Reifegrad von Blockchain-Angeboten wurde ebenfalls auf einer Skala von 1 bis 5 gemäß den folgenden Kriterien bewertet:

Bewertungsmaßstab: Reifegrad	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
1	Zu dem Angebot ist nur ein Whitepaper oder eine Webseite vorhanden.
2	Das Angebot befindet sich in einem frühen Stadium: es existiert ein früher Prototyp des Produkts oder von Teilen des Produkts.
3	Das Angebot befindet sich in der Test-Phase, die noch nicht für den produktiven Einsatz gedacht ist („Beta-Phase“).
4	Das Angebot ist frisch auf dem Markt **und** Meldungen auf Entwicklungsplattformen (z.B. bei Github) werden beachtet.
5	Das Angebot ist ausgereift und wird produktiv eingesetzt **und** es existiert ein dokumentierter. Prozess zur Meldung von Sicherheitslücken **und** Meldungen auf Entwicklungsplattformen (z.B. bei Github) werden schnell beantwortet und bearbeitet.

Da der Fokus dieser Studie insbesondere auf den Sicherheitseigenschaften von Blockchain-Angeboten liegt, ist die Existenz eines dokumentierten Prozesses zur Meldung von Sicherheitslücken aus Sicht des FZI ein notwendiges Kriterium, um den höchsten Reifegrad zu erreichen.

2.2.3 Sicherheitsmechanismen/Softwarequalität

Die verwendeten Sicherheitsmechanismen und die Softwarequalität ließen sich im Rahmen des begrenzten Umfangs der Marktanalyse nur oberflächlich bewerten. Daher erfolgte die Bewertung der Angebote nur in zwei Kategorien gemäß dem folgenden Bewertungsschema:

Bewertungsmaßstab: Sicherheitsmechanismen/Softwarequalität	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
0	Die verwendeten Mechanismen oder die Qualität der Software sind augenscheinlich unzureichend.
1	Die Software-Architektur ist augenscheinlich durchdacht und die verwendeten Sicherheitsmechanismen scheinen für den Anwendungsfall gut geeignet.

Für die Einteilung der Angebote in die beiden Kategorien wurden insbesondere die folgenden Kriterien berücksichtigt:

- Es existieren Testfälle
- Es existieren Kommentare zum Code
- Es existiert Dokumentation
- Der Code ist organisiert
- Die beschriebenen Sicherheitsmechanismen erscheinen für den Anwendungsfall plausibel
- Subjektive Einschätzung der Code-Qualität

2.2.4 Evaluierbarkeit

Insbesondere im Hinblick auf die detaillierte Analyse von ausgewählten Technologien wurden alle Angebote hinsichtlich ihrer Evaluierbarkeit auf einer Skala von 1 bis 3 gemäß dem folgenden Schema bewertet:

Bewertungsmaßstab: Evaluierbarkeit	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
1	Die zu untersuchende Technologie ist kaum dokumentiert **oder** die Evaluation bedingt die Durchführung von Seitenkanalangriffen oder anderer Angriffe auf Ebene der Hardware **oder** der Evaluationsaufwand ist aus anderen Gründen außergewöhnlich hoch.
2	Die zu untersuchende Technologie ist wenig dokumentiert und die Evaluation bedingt nur die Analyse von Software.
3	Zu der zu untersuchenden Technologie steht Dokumentation zur Verfügung, wichtige Teile des Quellcodes sind öffentlich.

In Kategorie 1 fallen insbesondere auch alle Angebote, zu denen zum Zeitpunkt der Erstellung des Marktüberblicks (zwischen November 2018 und Februar 2019) ausschließlich ein Whitepaper existiert oder bei denen nicht deutlich wird, wie das beworbene Produkt zu erwerben ist.

2.2.5 Kryptographische Mechanismen

In Abgrenzung zu dem Bewertungskriterium „Sicherheitsmechanismen/Softwarequalität“ wurden für dieses Kriterium ausschließlich die verwendeten kryptographischen Maßnahmen bewertet. Da bei der Implementierung solcher Mechanismen jedoch häufig Fehler passieren, die nur nach intensiver Analyse

auffallen, wurde auch hier nur eine oberflächliche Einteilung in zwei Kategorien, gemäß der folgenden Tabelle vorgenommen:

Bewertungsmaßstab: Kryptographische Mechanismen	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
0	Die eingesetzten kryptographischen Mechanismen sind augenscheinlich für den Anwendungszweck nicht geeignet oder werden falsch angewendet (beispielsweise Verwendung des Electronic Code Book (ECB) Betriebsmodus oder offensichtliche Verwendung einer falschen Schlüssellänge).
1	Es werden kryptographische Mechanismen eingesetzt, die augenscheinlich dem Stand der Wissenschaft entsprechen.

2.2.6 Performance/Skalierbarkeit

Im Rahmen der Marktanalyse wurde zusätzlich die Performance von Basistechnologien, digitalen Währungen und, falls angebracht, von Blockchain-Anwendungen bewertet. Da für die meisten Anwendungsfälle insbesondere die Transaktionsgeschwindigkeit relevant ist, wurde dieses Kriterium, gemäß der folgenden Tabelle, als Approximation für die Gesamtperformance herangezogen.

Bewertungsmaßstab: Performance/Skalierbarkeit	
Bewertete Arten von Angeboten: Basistechnologien, Digitale Währungen und Blockchain-Anwendungen	
Bewertung	***Kriterium***
1	Der Anzahl der möglichen Transaktionen pro Sekunde ist sehr gering (Referenz: Bitcoin ~10 Transaktionen/Sekunde).
2	Die Anzahl der möglichen Transaktionen pro Sekunde ist gering (Referenz: Ethereum ~20 Transaktionen/Sekunde).
3	Die Anzahl der möglichen Transaktionen pro Sekunde ist mittel (Referenz: DASH 1.500 Transaktionen/Sekunde).
4	Die Anzahl der möglichen Transaktionen pro Sekunde ist hoch (Referenz: Hyperledger 3.500 Transaktionen/Sekunde).
5	Die Anzahl der möglichen Transaktionen pro Sekunde ist sehr hoch (Referenz: VISA 24.000 Transaktionen/Sekunde).

2.2.7 Nutzerfreundlichkeit

Für die Bewertung der Nutzerfreundlichkeit wurde vor allem berücksichtigt, inwiefern den Nutzern eines Angebots ausreichend Dokumentation und Hilfestellung zur Einrichtung und Anwendung zur Verfügung gestellt wird und ob das Angebot für die Nutzung durch „unbedarfte“ Nutzer ausgelegt wurde. Die Einstufung erfolgte gemäß der folgenden Tabelle:

Bewertungsmaßstab: Nutzerfreundlichkeit	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***

1	Es steht kaum Dokumentation zur Verwendung des Angebots zur Verfügung oder die Einrichtung ist außergewöhnlich aufwändig.
2	Die Benutzung des Angebots erfordert Expertenwissen, aber es steht Dokumentation zur Verfügung, um sich das notwendige Wissen anzueignen.
3	Es steht ausführliche Dokumentation zur Verwendung des Angebots zur Verfügung oder werden von Nutzern erstellt und veröffentlicht, das Angebot ist für mehrere Plattformen erhältlich, die Einrichtung ist einfach.

2.2.8 Sicherheitsvorfälle

Durch die Analyse von vergangenen Sicherheitsvorfällen lassen sich unter Umständen Rückschlüsse auf die allgemeine Sicherheit von Produkten ziehen. Dazu ist es weniger relevant, *ob* es in der Vergangenheit Sicherheitsvorfälle gab (auch in den sorgfältigst entwickelten Produkten finden sich immer wieder Sicherheitslücken), als vielmehr wie damit umgegangen wurde und ob die Lücken selbst darauf schließen lassen, dass bereits Standardpraktiken der IT-Sicherheit unzureichend umgesetzt wurden. Alle Angebote wurden daher, gemäß der folgenden Tabelle, in vier Kategorien eingeteilt:

Bewertungsmaßstab: Sicherheitsvorfälle	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
1	Es wurden in der Vergangenheit Sicherheitsvorfälle bekannt, die auf eine gravierende Vernachlässigung von Standardpraktiken der IT-Sicherheit schließen lassen. Die Behebung der Sicherheitslücken erfolgte nicht oder nur sehr langsam.
2	Es wurden in der Vergangenheit Sicherheitsvorfälle bekannt, die auf eine Vernachlässigung von Standardpraktiken der IT-Sicherheit schließen lassen. Die Behebung der Sicherheitslücken erfolgte jedoch unverzüglich.
3	Es wurden in der Vergangenheit nur Sicherheitsvorfälle bekannt, von denen kaum Gefahr für das System oder die Nutzer ausging. Die Handhabung der Sicherheitsvorfälle war vorbildlich.
-	Es sind keine Vorfälle bekannt[6]. Eine Bewertung ist nicht möglich.

2.2.9 Lizenzierung

Für alle Angebote wurde erfasst, ob der Quelltext des Produktes (oder der Firmware, falls es sich um Hardware handelt) öffentlich verfügbar ist und falls ja, unter welcher Lizenz er steht. Die Bewertung wurde anhand der folgenden Einteilung durchgeführt:

Bewertungsmaßstab: Lizenzierung	
Bewertete Arten von Angeboten: alle	
Bewertung	***Kriterium***
1	Das Angebot ist proprietär und der Quellcode kann von keinem Dritten eingesehen werden.
2	Das Angebot ist proprietär, erfährt aber regelmäßig Sicherheitsaudits durch Dritte **oder** das Angebot ist proprietär, aber der Code ist trotzdem öffentlich.

[6]Es ist wichtig, darauf hinzuweisen, dass sich hieraus keine Schlussfolgerungen bezüglich der Sicherheit des Produktes ableiten lassen. Nur weil bisher keine Sicherheitsvorfälle bekannt geworden sind, ist ein Produkt nicht notwendigerweise sicher.

3	Das Angebot ist unter einer Lizenz mit strengem Copy-Left-Effekt lizenziert: GPLv3, GPLv2, Affero GPL, Creative Commons BY-SA.
4	Das Angebot ist unter einer Lizenz mit wenig Nutzungseinschränkungen lizenziert: Apache, LGPL, MPL.
5	Das Angebot ist unter einer vollständig liberalen Lizenz lizenziert: MIT, BSD, ISC, Public Domain.

2.2.10 Formale Sicherheitsnachweise

In der modernen Kryptographie haben formale Sicherheitsnachweise einen sehr hohen Stellenwert. So ist es heutzutage selbstverständlich, dass alle professionell eingesetzten Public-Key-Verschlüsselungsverfahren in einem geeigneten Modell als sicher bewiesen wurden. Auch bei komplexeren Protokollen setzen sich formale Sicherheitsnachweise mehr und mehr durch. Da Basistechnologien und Digitale Währungen in der Regel verschiedene Mechanismen zu neuartigen Protokollen kombinieren, um dadurch starke Sicherheitseigenschaften zu erreichen (beispielsweise die „Unveränderlichkeit“), wäre auch hier ein formaler Sicherheitsnachweis wünschenswert. Parallel zu den formalen Sicherheitsmodellen der Kryptographie hat sich für Software-Anwendungen die formale Verifikation durchgesetzt. In dieser Kategorie wurde daher zusätzlich ermittelt, ob eine formale Verifikation durchgeführt wurde oder nicht. Ähnlich wie bei der Implementierung von kryptographischen Mechanismen lassen sich im Rahmen einer Marktanalyse existierende Sicherheitsnachweise und formale Verifikationen nicht im Detail auf Korrektheit prüfen.

Die Einteilung der Angebote erfolgte wie im Folgenden dargestellt:

Bewertungsmaßstab: Formale Sicherheitsnachweise	
Bewertete Arten von Angeboten: Basistechnologien, Digitale Währungen und Blockchain-Anwendungen	
Bewertung	***Kriterium***
0	Es existieren keine formalen Sicherheitsnachweise für die Sicherheitsgarantie der Technologie.
1	Es existieren formale Sicherheitsnachweise in einer wissenschaftlichen Publikation oder in einem Whitepaper.

3 Auswertung der Ergebnisse

Im Rahmen dieser Studie wurden *303* unterschiedliche Angebote mit Blockchain-Bezug untersucht. Für jede Angebotsart wurden nahezu alle relevanten Angebote berücksichtigt. Für Digitale Währungen, Basistechnologien und Blockchain-Anwendungen wurden beispielsweise alle Produkte bis Platz 40 der Marktkapitalisierung gemäß „CoinMarketCap“ berücksichtigt, was einer Abdeckung von 91% des gesamten Marktes entspricht. Die hier berücksichtigten Angebote liefern daher einen repräsentativen Überblick über den Markt.

Die im Rahmen der Marktanalyse und Bewertung erarbeiteten Ergebnisse stehen in Form einer CSV-Datei zur Verfügung, die sich für die Erstellung von weitergehenden Auswertungen eignet. Die Datei enthält alle in Abschnitt 9 aufgeführten numerischen Bewertungen sowie Freitexteinträge, die in verschiedenen Fällen die Bewertungsgrundlagen näher erläutern.

In den folgenden Abschnitten stellen wir ausgewählte Auswertungen der ermittelten Daten dar, welche aus unserer Sicht die interessantesten und aufschlussreichsten Ergebnisse enthalten.

3.1 Arten von Angeboten

Abbildung 1 zeigt die Einteilung der untersuchten Angebote hinsichtlich ihrer Art. Auffallend ist, dass Blockchain-Anwendungen fast 35% des gesamten Marktes ausmachen.

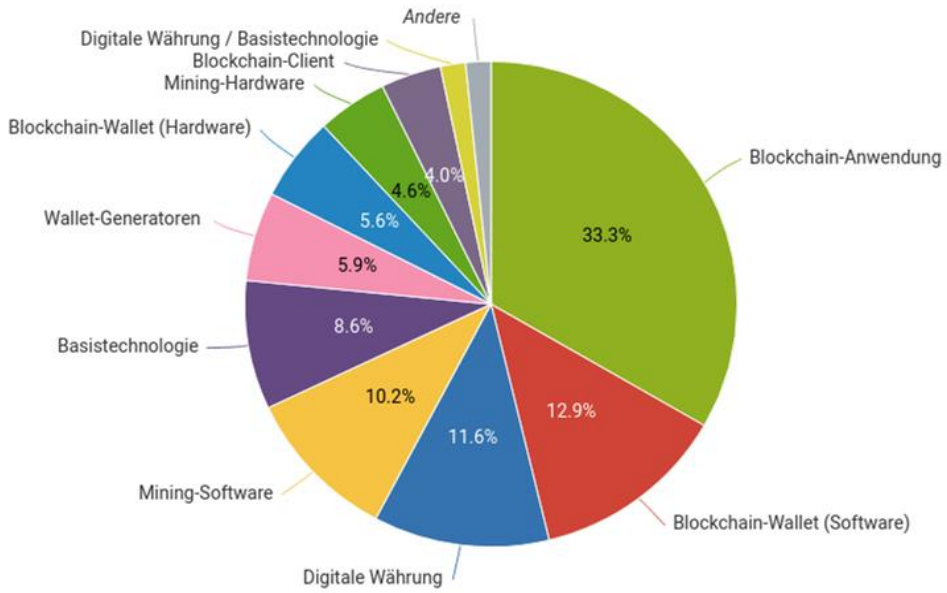

Abbildung 1: Art der untersuchten Angebote. Unter „Andere“ werden verschiedene Angebote zusammengefasst, deren Art jeweils nicht eindeutig bestimmbar ist (beispielsweise, weil sie sowohl als Anwendung als auch als Digitale Währung gedacht sind) und die zusammengenommen weniger als 1,7% des gesamten Marktes ausmachen.

Abbildung 2 zeigt, welche der untersuchten Blockchain-Anwendungen für welches Anwendungsfeld entwickelt wurden. Falls eine Anwendung für zwei oder drei Anwendungsfelder geeignet ist, wurde jeweils die dominante Anwendung berücksichtigt. Beispielsweise können grundsätzlich so gut wie alle Anwendungen prinzipiell als Datenspeicher genutzt werden, auch wenn das nicht ihr eigentlicher Anwendungszweck ist. Anwendungen, die viele unterschiedliche Anwendungsfälle unterstützen, wurden als Plattform unter Plattformökonomie eingeordnet.

Die Auswertung zeigt deutlich, dass Blockchain-Anwendungen stark im Finanzsektor sowie für Spiele genutzt werden, während die Verwendung für IoT, Identitätsmanagement, Verwaltung und Energie nur in

geringem Maße erfolgt. Ein großer Teil der untersuchten Anwendungen ließ sich keinem der eingangs definierten Anwendungsfelder zuordnen.

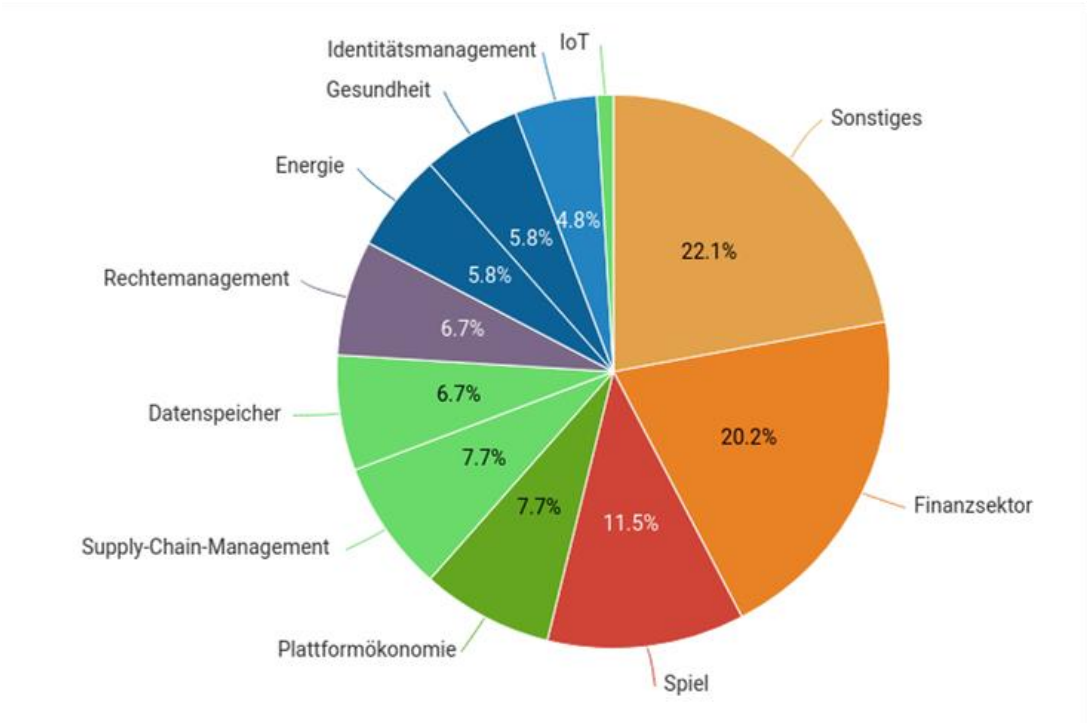

Abbildung 2: Anwendungsfelder der untersuchten Blockchain-Anwendungen, Digitalen Währungen und Basistechnologien. „Sonstiges“ bedeutet, dass das Produkt keinem der eingangs aufgelisteten Anwendungsfelder zugeordnet werden kann.

3.2 Herkunft

Abbildung 3 zeigt die Herkunft der untersuchten Angebote. Auffallend ist hier insbesondere, dass über ein Viertel aller Blockchain-Angebote aus den USA stammt, während Deutschland nur mit knapp 3% vertreten ist. Im Verhältnis zur Bevölkerungsgröße stammen überdurchschnittlich viele Angebote (12) aus Estland. Ein Grund dafür könnte im Erfolg der konsequenten Digitalisierungsstrategie des Landes liegen. Auffallend ist außerdem, dass ein signifikanter Teil der Produkte nicht von einer Firma hergestellt und vertrieben wird, sondern von Privatpersonen oder einer Community. Abbildung 4 zeigt die Herkunft von Angeboten mit Marktdurchdringung 4 und 5 und Abbildung 5 zeigt die Herkunft von untersuchten Angeboten mit Reifegrad 4 und 5.

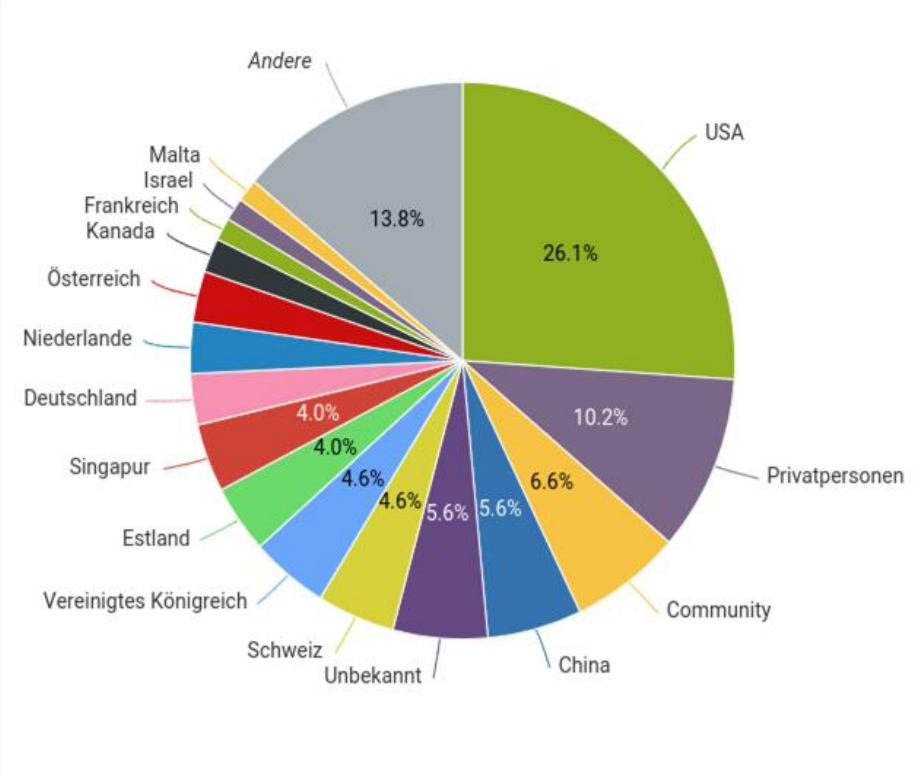

Abbildung 3: Herkunft der untersuchten Produkte. Die Kategorie „Andere" fasst alle Länder zusammen, aus den drei oder weniger Produkte stammen.

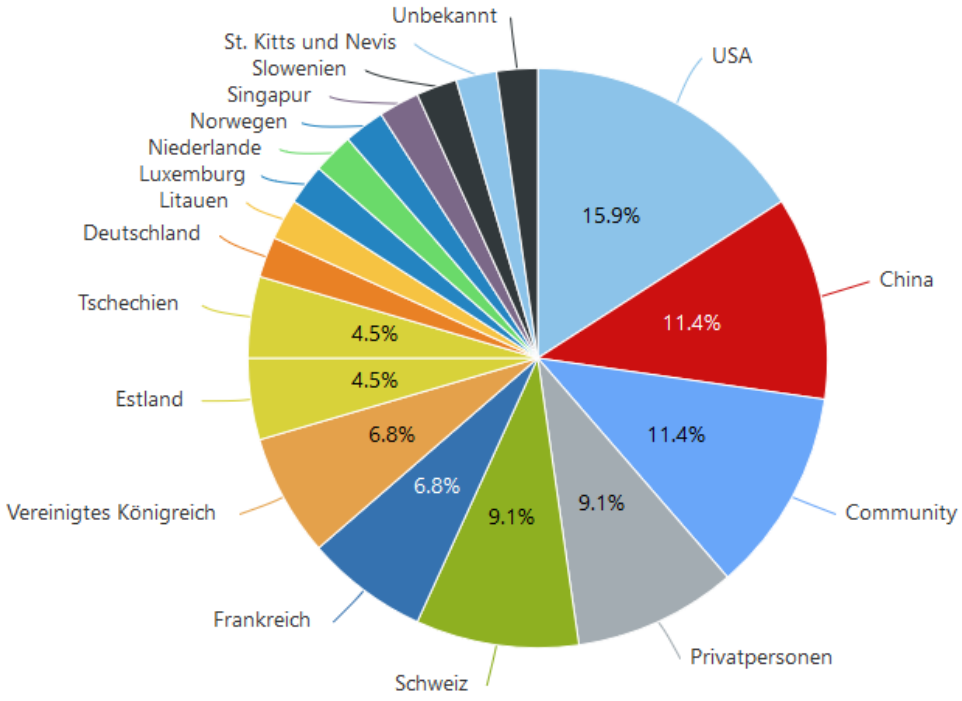

Abbildung 4: Herkunft der untersuchten Produkte mit Marktdurchdringung 4 und 5.

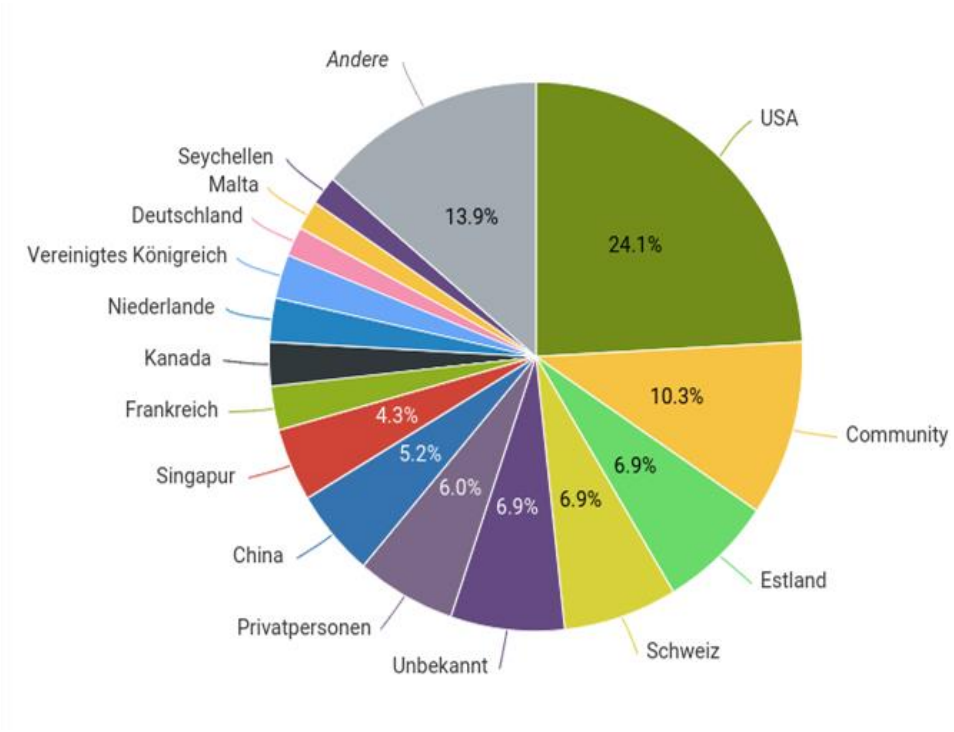

Abbildung 5: Herkunft der untersuchten Produkte mit Reifegrad 4 und 5.

Abbildung 6 und 7 zeigen die Aufteilung der Herkunft von Basistechnologien und Digitalen Währungen sowie von Blockchain-Anwendungen. Auffallend ist, dass der asiatische Raum (China und Singapur) und Community-entwickelte Lösungen bei Digitalen Währungen und Basistechnologien stark vertreten sind, während überraschend viele Blockchain-Anwendungen aus Estland kommen. Die USA ist in beiden Kategorien stark vertreten.

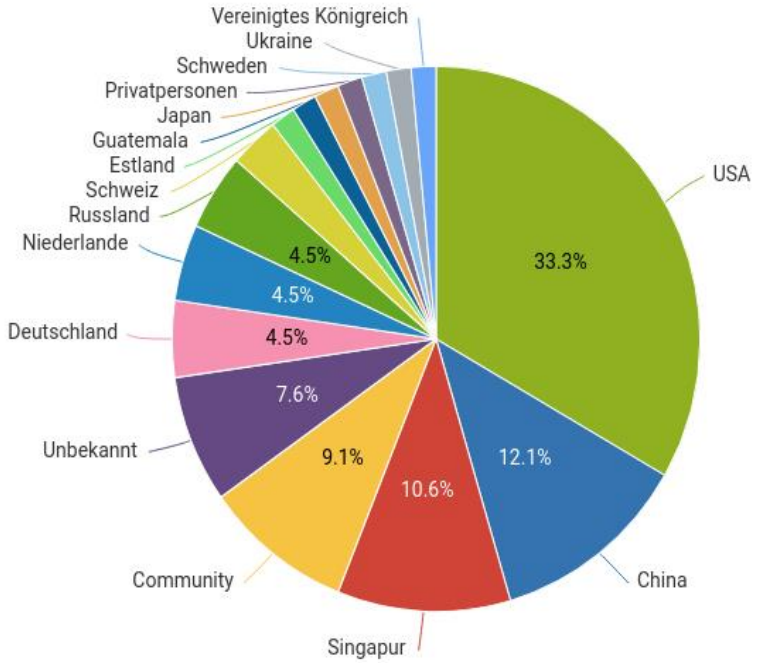

Abbildung 6: Herkunft von Basistechnologien und Digitalen Währungen.

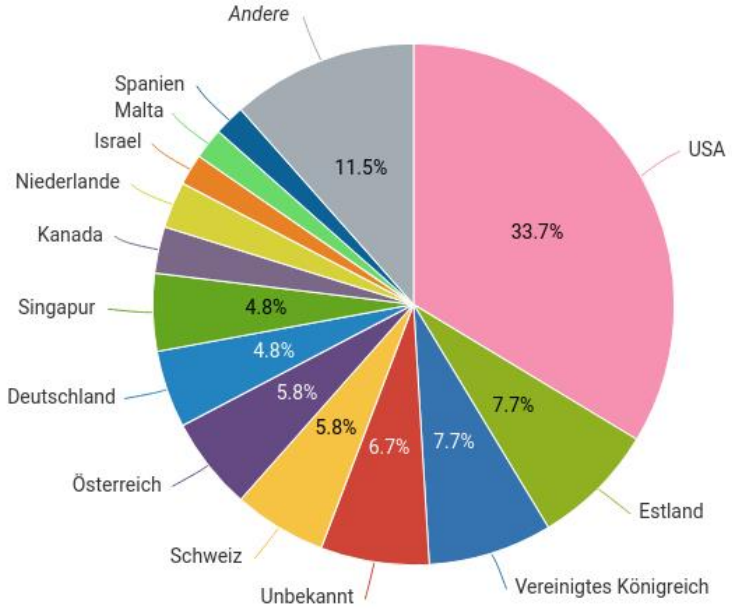

Abbildung 7: Herkunft von Blockchain-Anwendungen. Die Kategorie „Andere" fasst alle Länder zusammen, aus denen drei oder weniger Produkte stammen.

Abbildungen 8 und 9 verdeutlichen, dass der größte Teil der Mining-Software von Privatpersonen entwickelt wird, während die Hälfte der Mining-Hardware aus China stammt.

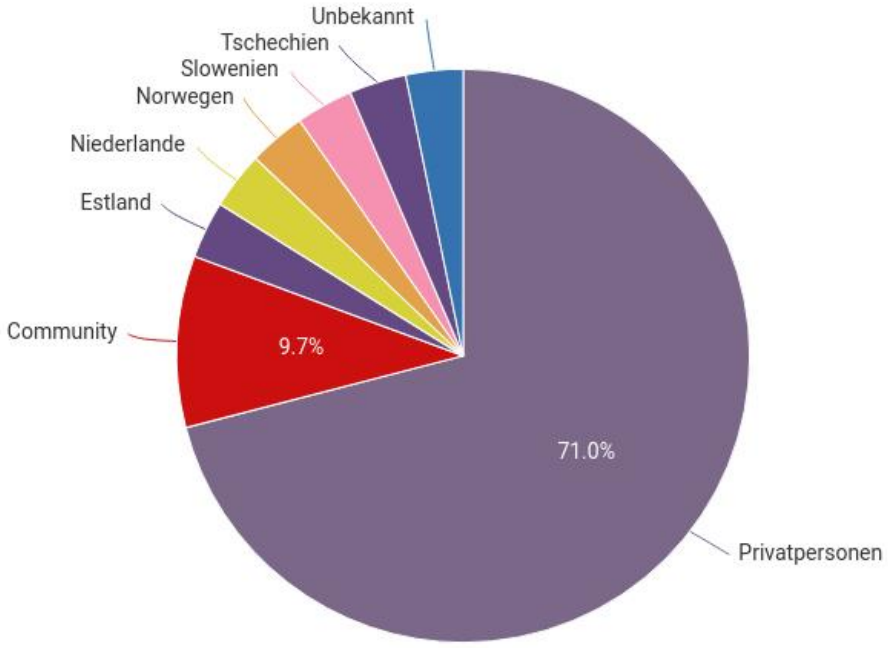

Abbildung 8: Herkunft von Mining-Software.

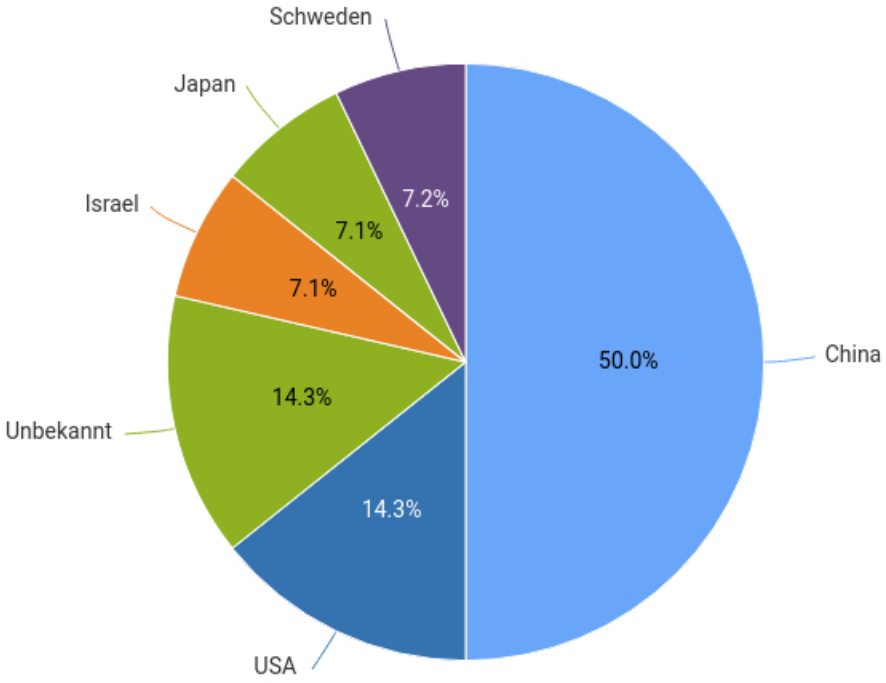

Abbildung 9: Herkunft von Mining-Hardware.

3.3 Lizenzierung

Bei knapp der Hälfte der untersuchten Angebote steht öffentlicher Quellcode zur Verfügung, bei fast der Hälfte davon (22,5%) ist dieser sogar unter einer sehr liberalen Lizenz veröffentlicht worden. Insgesamt entsteht also der Eindruck, dass Blockchain-Angebote tendenziell eher offen und transparent entwickelt werden. Einzig Mining-Hardware und Blockchain-Anwendungen stellen hier eine Ausnahme dar. Alle Mining-Hardware-Produkte, die untersucht wurden, besitzen keinen öffentlichen Quellcode und werden vollständig proprietär entwickelt. Bei Blockchain-Anwendungen zeigt sich ein ähnliches Bild wie auch in anderen untersuchten Kategorien: Bei einem großen Teil der Anwendungen lässt sich die Lizenzierung nicht feststellen (beispielsweise, weil nicht klar ist, ob es überhaupt ein Produkt gibt) oder der Code des Produktes ist nicht öffentlich. Abbildungen 10 und 11 visualisieren die Ergebnisse.

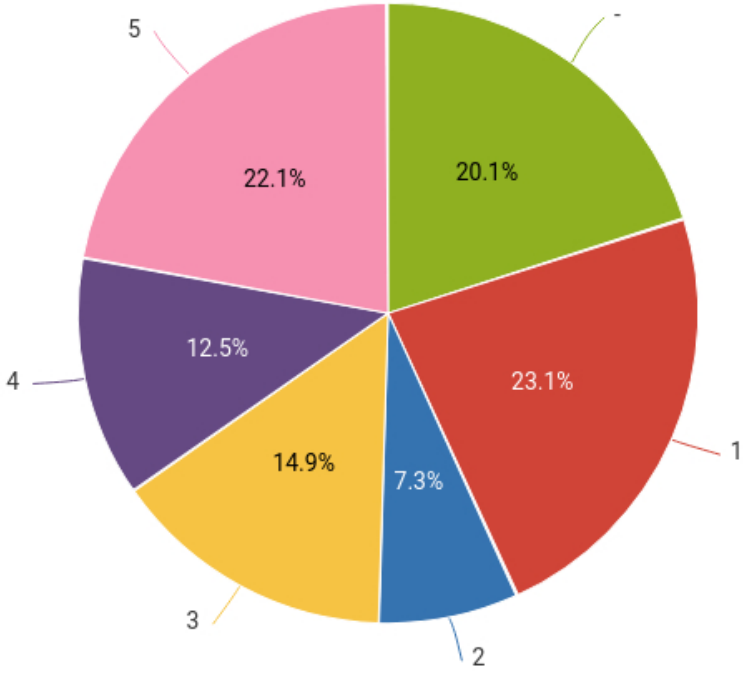

Abbildung 10: Lizenzierung der untersuchten Produkte gemäß den in Abschnitt 2.2.9 festgelegten Kriterien.

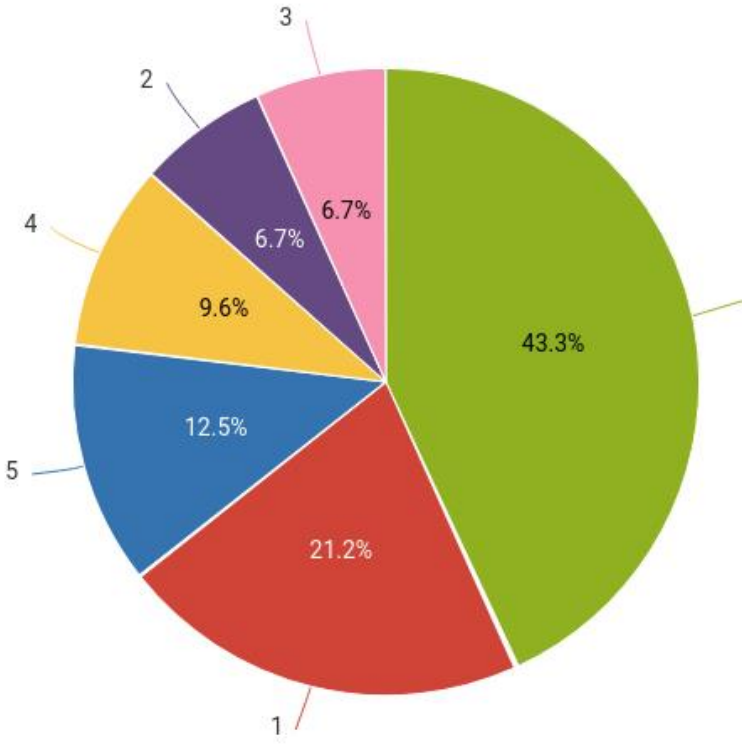

Abbildung 11: Lizenzierung der untersuchten Blockchain-Anwendungen gemäß den in Abschnitt 2.2.9 festgelegten Kriterien.

3.4 Marktrelevanz

Hinsichtlich der Marktrelevanz ist auffällig, dass ein großer Teil der Angebote (fast 50%) auf dem Markt nahezu unbekannt sind. Auch hier tragen die Blockchain-Anwendungen den größten Teil bei: Fast 70% aller Anwendungen haben eine sehr geringe Marktrelevanz.

Die Kategorien zwei bis vier sind bei allen Angeboten ungefähr gleich verteilt und weisen keine statistischen Auffälligkeiten auf. Abbildung 12 und 13 visualisieren diese Ergebnisse.

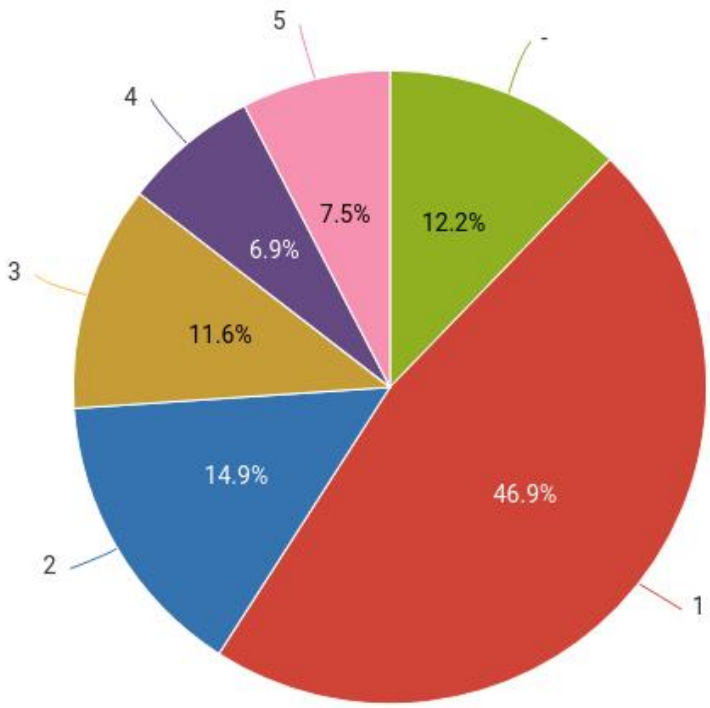

Abbildung 12: Marktrelevanz aller untersuchten Produkte. „-“ bedeutet, dass eine Beurteilung der Relevanz nicht vorgenommen werden konnte (beispielsweise aufgrund fehlender Informationen).

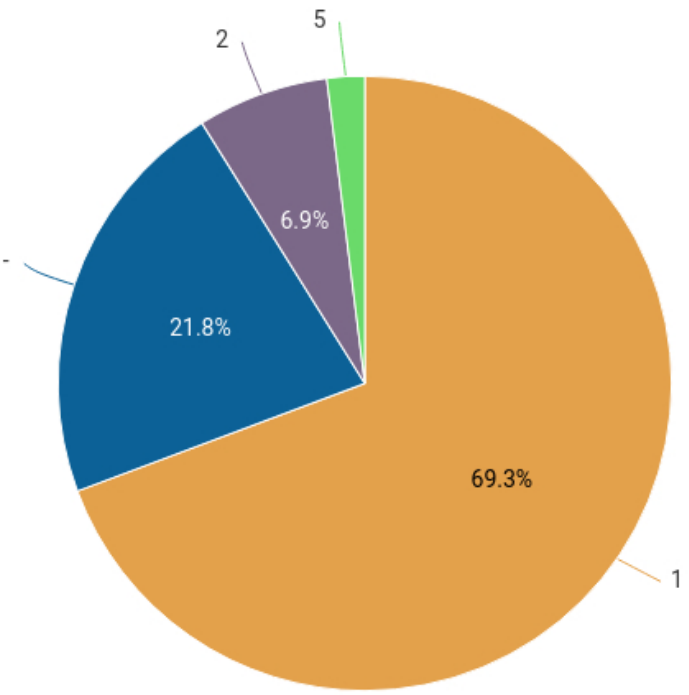

Abbildung 13: Marktrelevanz der untersuchten Blockchain-Anwendungen. „-“ bedeutet, dass eine Beurteilung der Relevanz nicht vorgenommen werden konnte (beispielsweise aufgrund fehlender Informationen).

Bei der Analyse aller Angebote mit Marktrelevanz 4 oder 5 (Abbildung 14) hinsichtlich ihrer Art zeigt sich, dass Blockchain-Anwendungen im Verhältnis zu ihrer Gesamtanzahl stark unterrepräsentiert sind – nur die Anwendungen „Circle Pay“ und „Whisper“ fallen in diese Kategorie. Hingegen besitzen insbesondere Wallets, Mining-Software und Blockchain-Clients eine hohe Relevanz auf dem Markt.

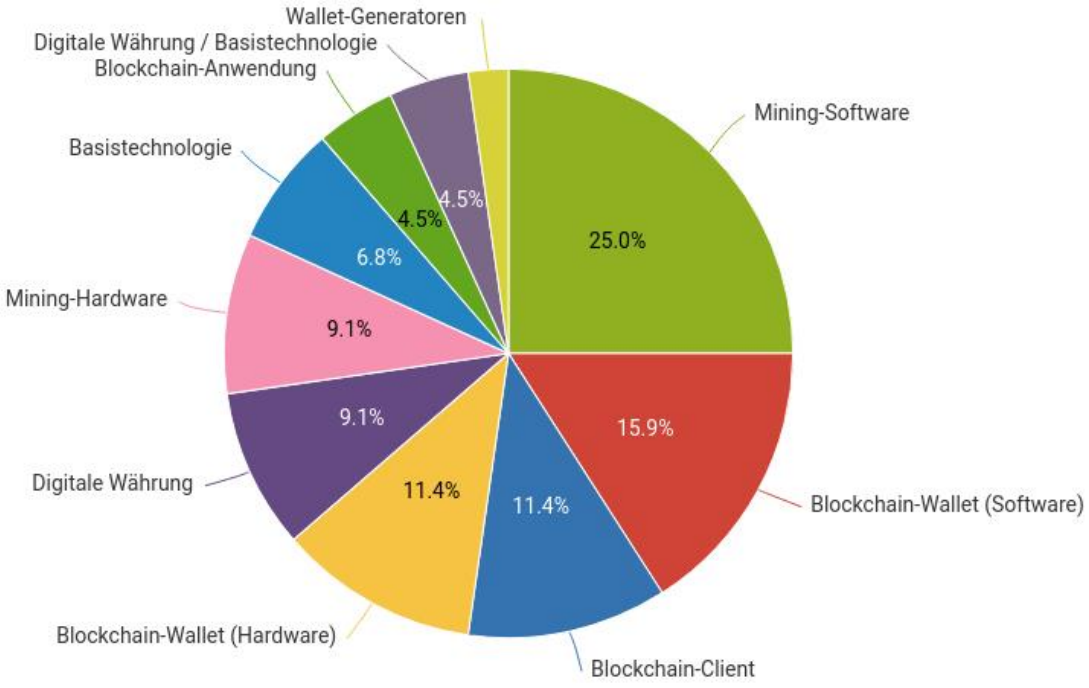

Abbildung 14: Aufteilung der untersuchten Arten von Angeboten mit Marktrelevanz 4 und 5 (insgesamt 44).

3.5 Reifegrad

Hinsichtlich des Reifegrads ist vor allem auffällig, dass sich ein großer Teil der untersuchten Blockchain-Anwendungen in einem frühen Entwicklungsstadium befindet. So haben über 50% der untersuchten Anwendungen Reifegrad 1 oder 2 (was bedeutet, dass zu dem Angebot nicht mehr als eine Webseite und ggf. eine prototypische Implementierung existiert) und nur circa 7% der Angebote Reifegrad 5 (was unter anderem bedeutet, dass es einen dokumentierten Prozess zur Meldung von Sicherheitslücken gibt). Abbildung 15 zeigt die Auswertung des Reifegrads der untersuchten Blockchain-Anwendungen.

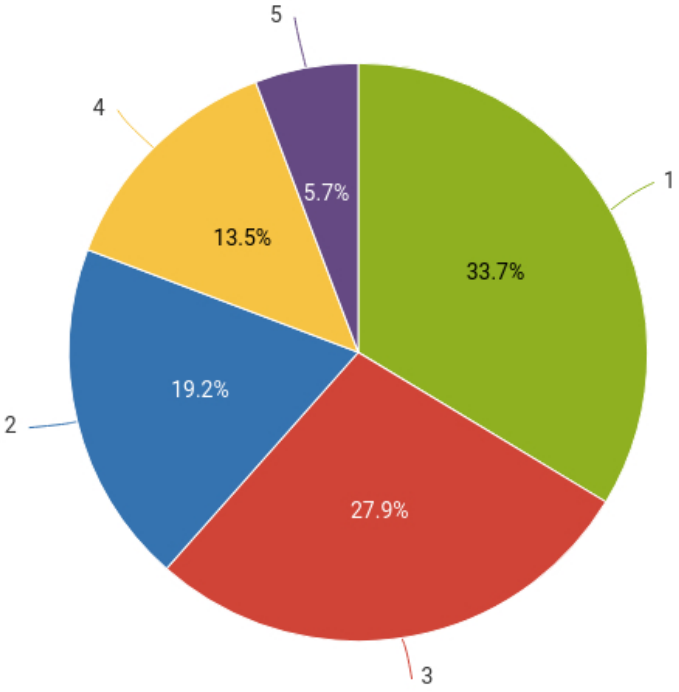

Abbildung 15: Reifegrad von Blockchain-Anwendungen gemäß den in Abschnitt 2.2.2 festgelegten Kriterien.

Auch im Gesamtüberblick (Abbildung 16) entsteht der Eindruck, dass die auf dem Markt verfügbaren Angebote nicht unbedingt ausgereift sind. So befinden sich insgesamt nur knapp 40% der Angebote im Reifegrad 4 oder 5.

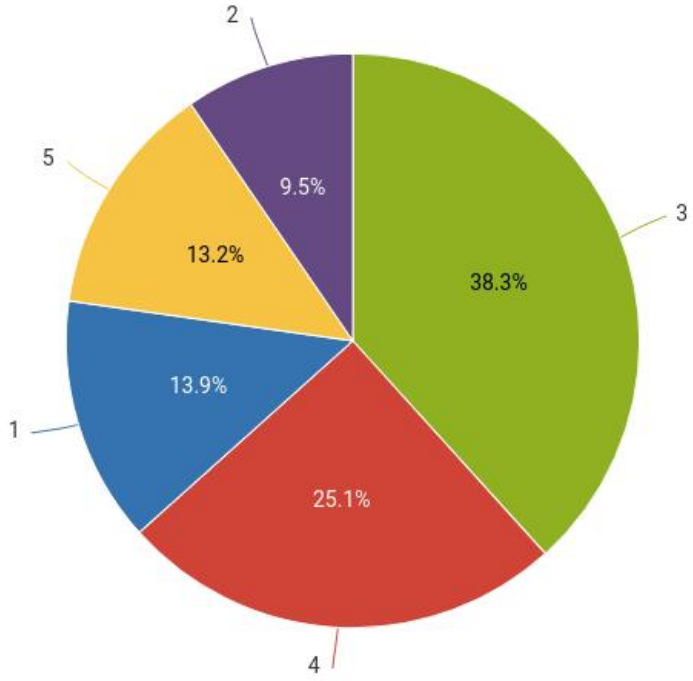

Abbildung 16: Reifegrad aller untersuchten Angebote anhand der in Abschnitt 2.2.2 festgelegten Kriterien.

Betrachtet man die Verteilung der Arten von Angeboten, die Reifegrad 1 oder 2 aufweisen (Abbildung 17), fällt auf, dass der Großteil davon Blockchain-Anwendungen sind. Auch unter Berücksichtigung der Tatsache, dass Blockchain-Anwendungen über 30% der insgesamt untersuchten Angebote ausmachen, sind sie mit 75% in dieser Auswertung doch überproportional vertreten.

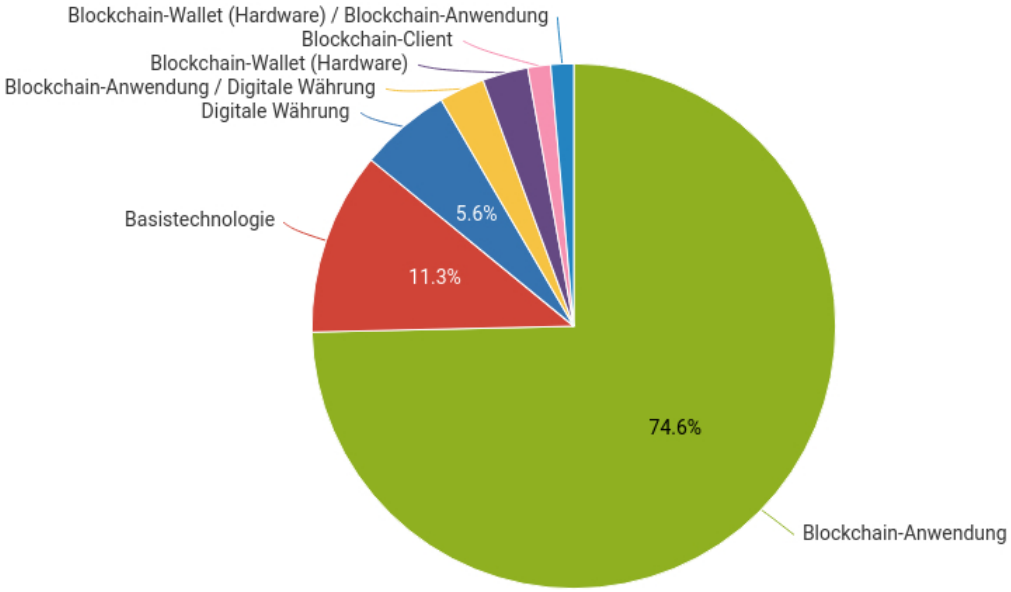

Abbildung 17: Arten von Angeboten mit Reifegrad 1 und 2 gemäß den in Abschnitt 2.2.2 dargestellten Kriterien.

Anders sieht es hingegen bei Hardware-Wallets aus. Hier befinden sich über 40% der Produkte sogar im Reifegrad 5 und über 20% der Produkte im Reifegrad 4 (siehe Abbildung 18). Damit Hardware-Wallets in der Regel Schlüsselmaterial für Zugriffe auf höhere Geldbeträge verwaltet wird, ist es jedoch auch nicht erstaunlich, dass Sicherheit bei Herstellern und Kunden einen hohen Stellenwert hat.

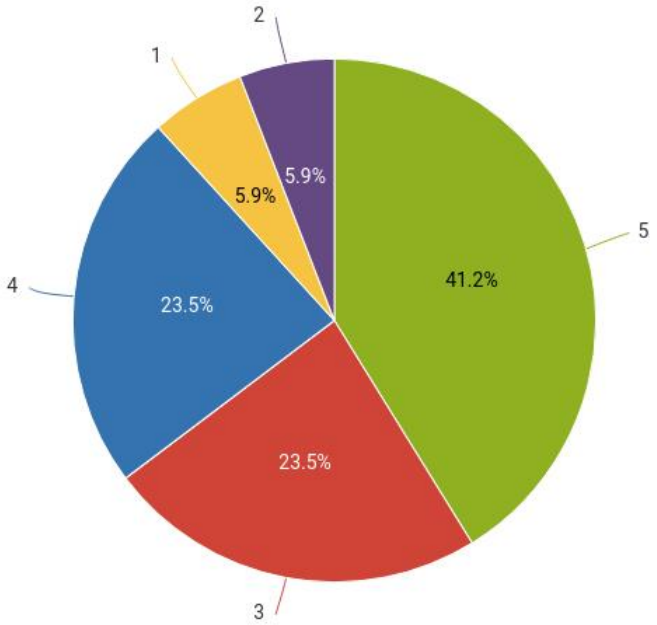

Abbildung 18: Reifegrad von Hardware-Wallets gemäß den in Abschnitt 2.2.2 dargestellten Kriterien.

Abbildung 19 zeigt den durchschnittlichen Reifegrad der untersuchten Arten von Angeboten. Es ist klar zu erkennen, dass Blockchain-Anwendungen im Durchschnitt den geringsten Reifegrad besitzen, während Blockchain-Clients und Hardware-Wallets durchschnittlich sehr ausgereift sind.

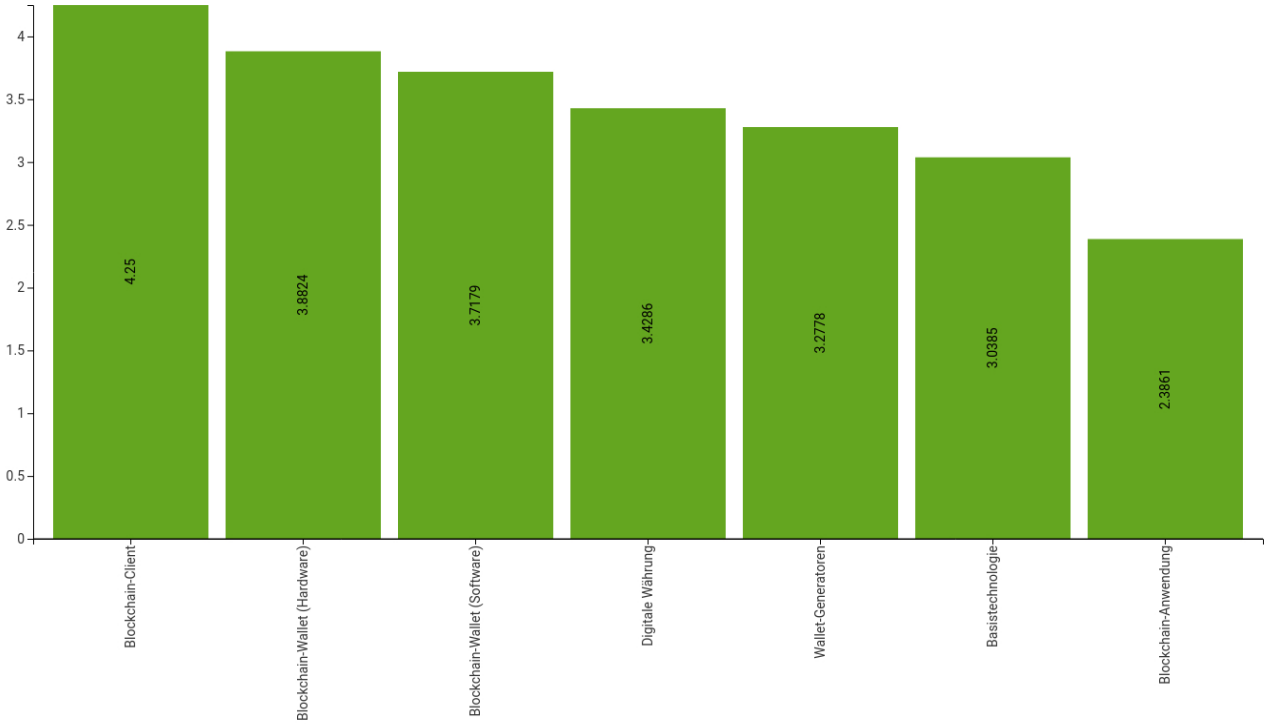

Abbildung 19: Durchschnittlicher Reifegrad der untersuchten Produkte nach Produktklasse gemäß den in Abschnitt 2.2.2 dargestellte Kriterien.

3.6 Performance

Wie es auch in anderen Kategorien der Fall ist, lässt sich die Performance der Blockchain-Anwendungen in den meisten Fällen nicht beurteilen. Für die Fälle, bei denen eine verlässliche Aussage möglich ist, wird deutlich, dass nur ausgesprochen wenige Anwendungen eine hohe Performance erreichen. Die meisten Anwendungen befinden sich in den Kategorien 1 und 2 (zwischen 1 und 20 Transaktionen pro Sekunde). Bei Basistechnologien und Digitalen Währungen lässt sich häufiger eine Einschätzung treffen, die Verteilung der Performance ist jedoch ähnlich. Abbildungen 20 und 21 visualisieren diese Ergebnisse.

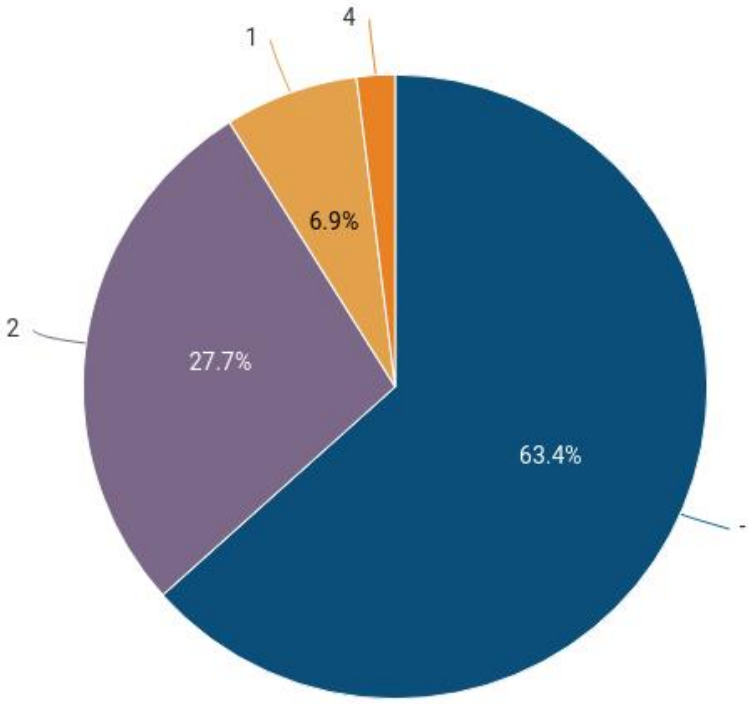

Abbildung 20: Performance der untersuchten Blockchain-Anwendungen gemäß den in Abschnitt 2.2.6 festgelegten Kriterien.

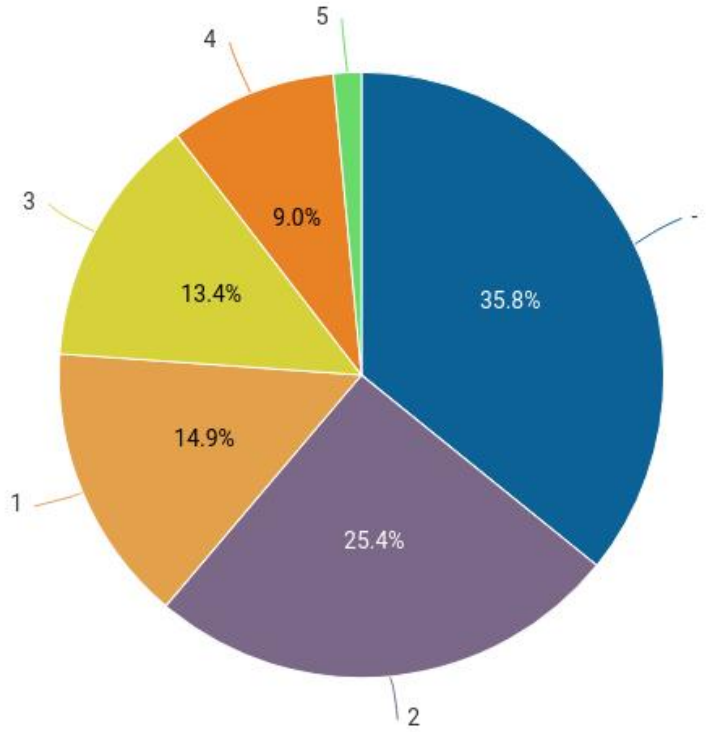

Abbildung 21: Performance der untersuchten Basistechnologien und Digitalen Währungen gemäß den in Abschnitt 2.2.6 festgelegten Kriterien.

3.7 Sicherheit

Bei einem Großteil der untersuchten Angebote (über 85%) sind bisher keine Sicherheitslücken bekannt geworden (siehe Abbildung 22). Diese Statistik allein gibt jedoch keinen Aufschluss über die Sicherheit, da es auch bedeuten kann, dass die allermeisten Produkte bisher noch nicht untersucht wurden. Tatsächlich konnten wir im Rahmen unserer Recherchen nur bei „Hyperledger“[7] und „Augur“[8] eine beauftragte und veröffentlichte umfassende Sicherheitsanalyse finden (wie man sie beispielsweise im Rahmen eines „Penetration Testing Reports“ erwarten würde). In drei weiteren Fällen (ausschließlich Hardware-Wallets) haben Forschungsgruppen oder Firmen, die nicht in Zusammenhang mit dem Hersteller stehen, umfassende Sicherheitsanalysen durchgeführt und mindestens im Rahmen eines öffentlich verfügbaren Vortrags publiziert.

In allen anderen Fällen existieren zwar möglicherweise Beschreibungen von gefundenen Sicherheitslücken (auf Blogging-Plattformen, privaten Webseiten, teilweise auch auf den Webseiten der Hersteller); diese sind jedoch nicht Teil einer umfassenden, veröffentlichten Sicherheitsanalyse.

[7]https://wiki.hyperledger.org/download/attachments/2393550/management_report_linux_foundation_fabric_august_2017_v1.1.pdf?version=1&modificationDate=1548107421000&api=v2
[8]https://blog.openzeppelin.com/serpent-compiler-audit-3095d1257929/

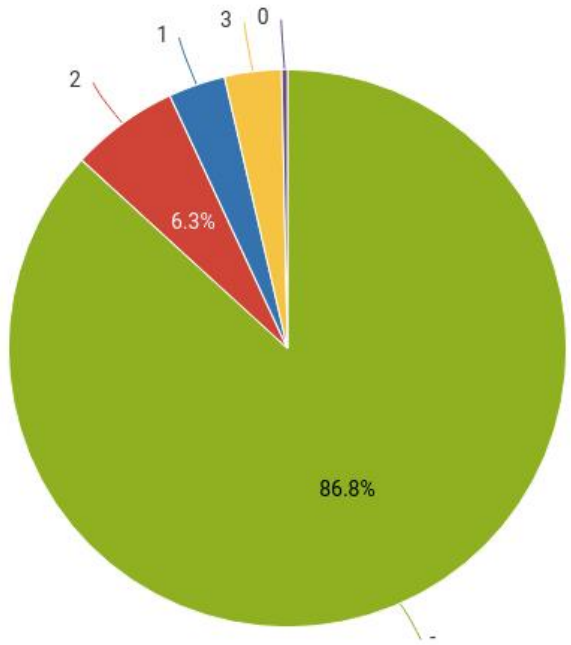

Abbildung 22: Bekannte Sicherheitsvorfälle aller untersuchten Produkte gemäß den in Abschnitt 2.2.8 festgelegten Kriterien.

Hinsichtlich der Sicherheitsmechanismen und der Softwarequalität ist zunächst auffällig, dass diese Kategorie bei über einem Drittel aller untersuchten Angebote nicht zu bewerten ist (Abbildung 23). Der Grund hierfür scheint insbesondere in dem insgesamt geringen Reifegrad der untersuchten Blockchain-Anwendungen zu liegen, was in Abbildung 24 auch bestätigt wird. Weiterhin ist bemerkenswert, dass nur bei einem sehr kleinen Teil aller Produkte (gleichmäßig verteilt über alle Produktklassen) die eingesetzten Mechanismen oder die Qualität der Software offensichtlich unzureichend sind.

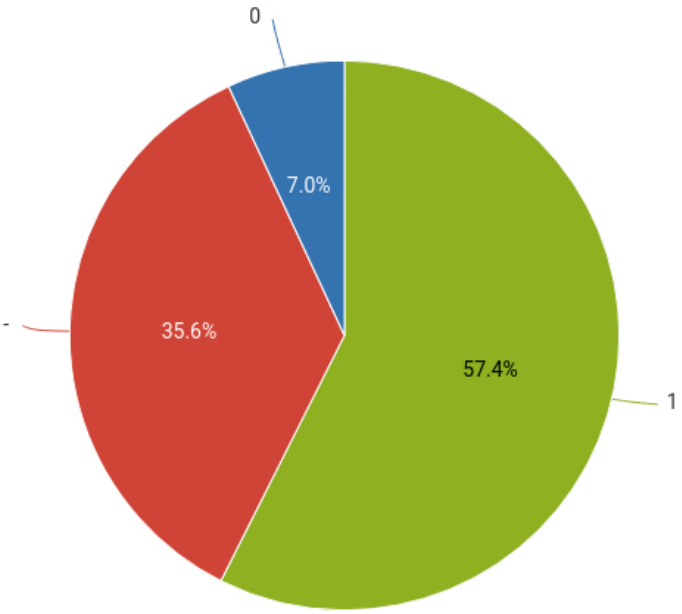

Abbildung 23: Sicherheitsmechanismen und Softwarequalität aller untersuchten Produkte gemäß den in Abschnitt 2.2.3 festgelegten Kriterien.

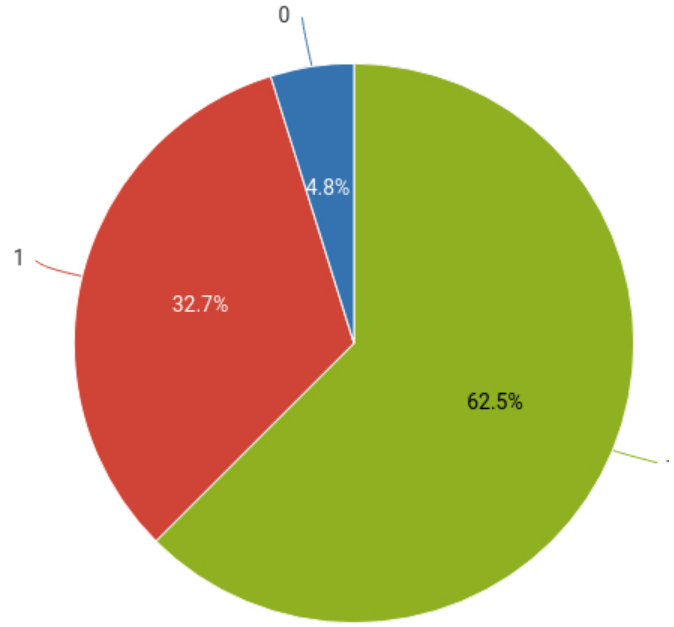

Abbildung 24: Sicherheitsmechanismen und Softwarequalität der untersuchten Blockchain-Anwendungen gemäß den in Abschnitt 2.2.3 festgelegten Kriterien.

Beim richtigen Einsatz von kryptographischen Mechanismen verhält es sich – über alle Arten von Angeboten hinweg – nahezu identisch (siehe Abbildung 25). Auch hier stellen Blockchain-Anwendungen den größten Teil derjenigen Angebote, die bezüglich dieser Kategorie nicht bewertet werden konnten (ca. 68%). Kryptographische Mechanismen sind insbesondere bei Software-Wallets überproportional häufig bereits in einer vorläufigen Analyse schlecht bewertet, während andere Arten von Angeboten hinsichtlich dieses Merkmals unauffällig sind.

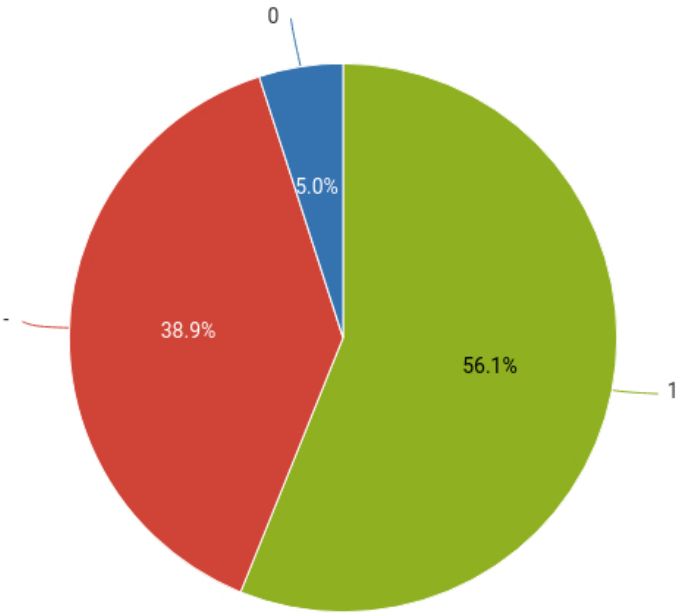

Abbildung 25: Einsatz kryptographischer Mechanismen aller untersuchten Produkte gemäß den in Abschnitt 2.2.5 festgelegten Kriterien.

Formale Sicherheitsnachweise existieren nur für sehr wenige Angebote, wie in Abbildung 26 zu sehen ist.

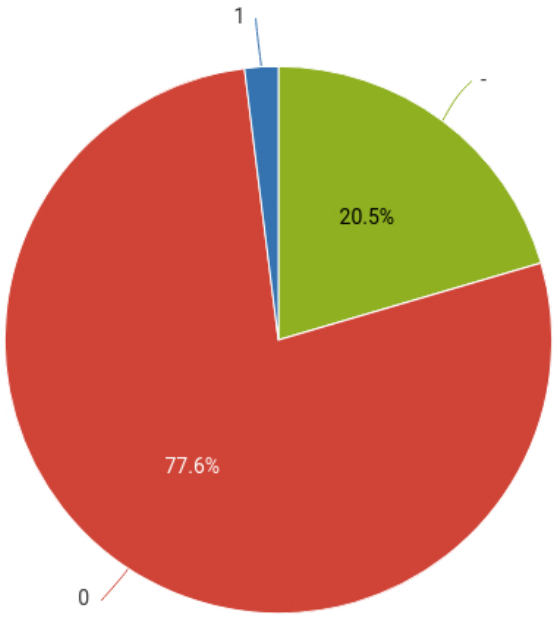

Abbildung 26: Existenz formaler Sicherheitsnachweise für die untersuchten Produkte gemäß den in Abschnitt 2.2.10 festgelegten Kriterien.

4 Schlussfolgerungen

Basierend auf der erfolgten Analyse und Bewertung halten wir die folgenden allgemeinen Schlussfolgerungen für vertretbar:

- **Es existieren so gut wie keine Angebote mit formalen Sicherheitsnachweisen, die wesentliche Teile des Angebots betreffen.**
  Formale Sicherheitsnachweise existieren zwar für die eingesetzten kryptographischen Bausteine wie Verschlüsselungsverfahren oder Signaturfunktionen, viele Blockchain-Angebote versprechen jedoch weit darüber hinausgehende Sicherheitseigenschaften, wie Unveränderlichkeit oder Resistenz gegen Sybil-Angriffe. Für diese Aussagen bestehen in der Regel keine formalen Nachweise oder wissenschaftliche Untersuchungen. Obwohl die meisten Angebote Sicherheit zum zentralen Thema ihrer Werbebotschaft machen, existiert auch für die eingesetzten Softwarekomponenten (oder für Teile davon) in aller Regel keine formale Verifikation.
- **Blockchain-Anwendungen spielen auf dem Markt kaum eine Rolle.**
  Fast 80% aller untersuchten Anwendungen haben eine kleine oder sehr kleine Marktrelevanz. Auch hinsichtlich des Reifegrades bleiben Blockchain-Anwendungen hinter anderen Arten von Angeboten zurück: Nur knapp 20% aller Anwendungen haben einem hohen oder sehr hohen Reifegrad, über ein Drittel aller Anwendungen sind bisher nicht über das Stadium einer Marketingwebseite hinausgekommen. Mit einem durchschnittlichen Reifegrad von 2,38 sind Blockchain-Anwendungen die am wenigsten entwickelte Art von Blockchain-Angeboten auf dem Markt. Es entsteht insgesamt der Eindruck, dass es bisher noch so gut wie keine im Einsatz befindlichen Anwendungen für die Blockchain-Technologie gibt.
- **Existierende Angebote wurden bisher kaum öffentlichen Sicherheitsanalysen oder „Penetration Tests“ unterzogen.**
  Obwohl das Hauptverkaufsargument der meisten Blockchain-Angebote die Sicherheit ist, wurden nur in wenigen Einzelfällen von den Herstellern der Produkte unabhängige Sicherheitsuntersuchungen in Auftrag gegeben und deren Ergebnisse veröffentlicht. In einigen weiteren Fällen wurden Sicherheitslücken von unabhängigen Forschern entdeckt. Diese wurden in fast allen Fällen schnell behoben. Eine Ausnahme bilden hier Hardware-Wallets und Blockchain-Clients, die überdurchschnittlich gut untersucht sind, jedoch zusammen weniger als 10% der Gesamtanzahl der untersuchten Angebote ausmachen.
- **Blockchain-Clients und Hardware-Wallets sind diejenigen Angebote mit dem höchsten Entwicklungsstand.**
  Für über 40% der untersuchten Hardware-Wallets und für 50% der untersuchten Blockchain-Clients existiert ein dokumentierter Prozess zur Meldung von Sicherheitslücken. Eine große Anzahl der kommerziell verfügbaren Wallets und Clients wurde bereits einer Sicherheitsanalyse unterzogen. Diese Zahlen sind besonders vor dem Hintergrund zu erklären, dass Sicherheitslücken in diesen Angeboten schnell zum Verlust einer großen Menge Geld führen können.
- **Mining-Hardware kommt aus China und Mining-Software von Privatpersonen.**
  Über 70% der untersuchten Mining-Software wird von Privatpersonen entwickelt – der Hauptvertriebskanal ist ein öffentliches Forum. Die Hälfte der kommerziell verfügbaren Mining-Hardware kommt aus China; aus Israel, Schweden, Japan und den USA kommen jeweils nur ein oder zwei Produkte.
- **Zahlungsverkehr und Spiele sind die Hauptanwendungsfelder von existierenden Blockchain-Anwendungen.**
  Der größte Teil der untersuchten Blockchain-Anwendungen (ca. 20%) ist für den Einsatz im Finanzsektor gedacht, bei dem zweitgrößten Teil handelt es sich um Spiele, die ihre Spieldaten in der

Blockchain verwalten. Insbesondere die Anwendungsfelder Verwaltung, IoT, Identitätsmanagement, Gesundheit und Energie, welche häufig als Hauptverkaufsargument für Blockchain-Technologie genannt werden, werden bisher kaum von existierenden Blockchain-Anwendungen abgedeckt. Ein signifikanter Teil der Anwendungen (ca. 22%) ist keinem der klassischen Anwendungsfelder zuzuordnen.

5 Auswahl der zu untersuchenden Produkte

Auf Basis des Marktüberblicks wurden in Abstimmung mit dem BSI 8 Produkte als Kandidaten für eine tiefergehende Untersuchung festgelegt. Neben dem Ziel, möglichst viele Anwendungsfelder und Angebotsarten abzudecken, hatten weiterhin die folgenden Bewertungskriterien auf diese Auswahl Einfluss:

- **Marktrelevanz und Bekanntheit**: Je höher die Marktrelevanz eines Angebots, desto höher wurde das Potential für AP5 gesehen, da sich Sicherheitslücken in einem bekannten Angebot potenziell auf einen größeren Nutzerkreis auswirken. Angebote, die aktuell zwar eine eher geringe Marktrelevant haben, bei denen aber davon auszugehen ist, dass sich das in Zukunft ändert, wurden ebenfalls eher mit einem hohen Potenzial für AP5 eingeschätzt.
- **Sicherheitsvorfälle**: Bekannte Sicherheitsvorfälle haben auf unterschiedliche Arten Einfluss auf die Bewertung des Potenzials für AP5 genommen. Zum einen wurden Angebote, bei denen schon viele Sicherheitsanalysen durchgeführt wurden und die dementsprechend auch viele bekannte Sicherheitsvorfälle aufweisen (die jedoch überwiegend schnell und professionell behandelt und gelöst werden konnten) in der Regel nicht für eine weiterführende Untersuchung berücksichtigt. Bei solchen Angeboten haben wir es als unwahrscheinlich angesehen, dass im Rahmen des begrenzten Untersuchungsaufwands dieser Studie, weitere Sicherheitslücken gefunden werden. Berücksichtigt wurden insbesondere solche Angebote, zu denen bisher keine bekannten Sicherheitsuntersuchungen erfolgt waren oder bei denen bereits durchgeführte Sicherheitsanalysen darauf schließen lassen, dass das Angebot weitere Lücken aufweist.
- **Sicherheitsmechanismen/Softwarequalität und kryptographische Mechanismen:** Die Angebote, bei denen die Sicherheitsmechanismen, die Softwarequalität oder die kryptographischen Mechanismen offensichtlich unzureichend waren, wurden tendenziell eher für eine weiterführende Untersuchung berücksichtigt.
- **Evaluierbarkeit:** Bei der Auswahl wurde darauf geachtet, nicht zu viele Angebote auszuwählen, die schwierig zu evaluieren sind (beispielsweise, weil es keinen öffentlichen Quellcode gibt), um den Gesamtaufwand der Studie in einem realistischen Rahmen zu halten. Gleichzeitig sollten jedoch nicht nur Angebote ausgewählt werden, die leicht zu evaluieren sind, um auch andere Angriffstechniken (wie beispielsweise „Reverse Engineering“) demonstrieren zu können.

Die Kriterien „Formale Sicherheitsnachweise“ und „Performance“ hatten auf diese Bewertung keinen Einfluss, da sie, unserer Ansicht nach, keine Aussage über die Eignung eines Angebots für eine Untersuchung im Rahmen von AP5 erlauben. Insbesondere die Existenz von formalen Sicherheitsnachweisen kann einerseits ein Hinweis darauf sein, dass der Anbieter einen großen Wert auf Sicherheit legt und eine weitere Untersuchung daher nicht notwendig ist. Andererseits sagt beispielsweise eine formale Analyse auf Konzeptebene nichts über die tatsächliche Implementierung aus und eine weiterführende Untersuchung kann daher sehr interessant sein. Die für AP5 relevanten Aspekte der Kriterien „Lizenzierung“ und „Nutzerfreundlichkeit“ (wie beispielsweise das Vorhandensein von Dokumentation oder öffentlichem Quellcode) wurden unter „Evaluierbarkeit“ zusammengefasst und in diesem Sinne bei der Bewertung berücksichtigt.

Im Ergebnis wurden die folgenden 8 Angebote ausgewählt:

- Corda: Bei Corda handelt es sich um eine Basistechnologie, die speziell für den Einsatz im Unternehmenskontext konzipiert wurde (ähnlich wie beispielsweise Hyperledger). Obwohl Corda nicht primär auf den Einsatz im Gesundheitswesen ausgerichtet ist, wird die Technologie doch intensiv für

eine Anwendung im Gesundheitskontext beworben. Corda genießt auch bereits einige Aufmerksamkeit in Fachmedien. In Ermangelung besser geeigneter Alternativen wird mit der Untersuchung von Corda das Anwendungsfeld „Gesundheit“ abgedeckt.

- OriginTrail: OriginTrail ist eine Blockchain-Anwendung, die speziell für das Anwendungsfeld Supply-Chain-Management gedacht ist. Das Produkt befindet sich aktuell in einer Testphase und ist dementsprechend bisher noch gering kapitalisiert. In einschlägigen Medien genießt es jedoch bereits große Aufmerksamkeit. Es ist davon auszugehen, dass OriginTrail in Zukunft einen größeren Teil des Marktes für sich beanspruchen wird. Es ist daher besonders naheliegend, eine Sicherheitsuntersuchung durchzuführen, bevor das Angebot flächendeckend eingesetzt wird.
- VeChain: VeChain ist, ähnlich wie Ethereum, eine Mischung aus Basistechnologie und Digitaler Währung. In der VeChain-Blockchain sollen Informationen über bestimmte Produkte gespeichert werden. Im Gegensatz zu OriginTrail ist VeChain deutlich stärker kapitalisiert und wird von einer Vielzahl von großen Unternehmen unterstützt. Mit der Untersuchung von VeChain und OriginTrail wird das Anwendungsfeld „Supply-Chain-Management“ abgedeckt.
- Sia: Sia ist ein Blockchain-basierter Cloud-Datenspeicher, bei dem Nutzer anderen Nutzern freien Speicherplatz bereitstellen können. Durch dieses Konzept ergeben sich signifikante Sicherheitsrisiken für die Nutzer, da sie im Wesentlichen fremden Personen Zugriff auf ihre Festplatte ermöglichen. Wie auch OriginTrail ist Sia aktuell zwar noch gering kapitalisiert, erfährt jedoch eine große mediale Aufmerksamkeit. Es ist also davon auszugehen, dass Sia in Zukunft einen großen Teil des Marktes besetzen wird. Mit der Untersuchung von Sia wird das Anwendungsfeld „Datenspeicher“ abgedeckt.
- Exodus: Bei Exodus handelt es sich um eine Software-Wallet. Exodus ist für eine Untersuchung besonders interessant, da die Software, nach Aussagen des Herstellers, Unterstützung für über 80 verschiedene Coins und Token mitbringt und eine Sicherheitslücke dementsprechend ein hohes Schadenspotential hat. Exodus wird in einigen Fachmedien als eine der wichtigsten Software-Wallets genannt und ist daher auf dem Markt bekannt.
- Trust Wallet: Trust Wallet ist eine Software-Wallet für Android und iOS. Sie unterstützt eine Vielzahl von verschiedenen Währungen und genießt eine mittlere Bekanntheit. Die Untersuchung von Trust Wallet und Exodus folgt der Einschätzung, dass Software-Wallets ein hohes Risiko für Nutzer bergen. Daher liegt die Untersuchung einer Desktop-Anwendung und einer App nahe.
- EOS: EOS ist eine Basistechnologie, die insbesondere für die Realisierung von dezentralisierten Anwendungen (sogenannten „dApps“) gedacht ist. Nach Aussagen des Herstellers ist EOS als eine Art „Blockchain-basiertes Betriebssystem“ gedacht. EOS hat eine Marktkapitalisierung von über 3 Mrd. Euro. Eine Untersuchung ist vor allem vor dem Hintergrund dieser hohen Marktrelevanz sowie aufgrund der eingesetzten neuartigen Konzepte, wie beispielsweise des eigens entwickelten Konsensmodells, interessant.
- BitBox: Bitbox ist eine Hardware-Wallet, die gleichzeitig als zweiter Faktor für Authentifizierungsprotokolle verwendet werden kann. Besonders bei Bitbox ist, dass die geheimen Informationen, die zur Authentifizierung von Transaktionen verwendet werden, auf einer SD-Karte gespeichert werden können und das Gerät kein Display besitzt, um Transaktionsdetails anzuzeigen. Daraus ergeben sich besondere Anforderungen an die Umsetzung von Sicherheitsmaßnahmen, die im Rahmen einer detaillierten Untersuchung analysiert werden können. Des Weiteren handelt es sich bei dem Hersteller von BitBox um einen der wenigen europäischen Hersteller von Hardware-Wallets. Die Untersuchung von BitBox deckt insbesondere den geforderten Einsatz von Analysetechniken für Hardware ab.

Zum Zeitpunkt der Auswahl der Angebote waren uns keine öffentlich bekannten oder öffentlich einsehbaren professionellen Sicherheitsanalysen bekannt. Der Quelltext von Corda, OriginTrail, VeChain und EOS ist jeweils öffentlich verfügbar und eine Untersuchung ist daher verhältnismäßig einfach. Für diese

drei Angebote verwendeten wir daher automatisierte Analysewerkzeuge, wie statische Codeanalyse und Fuzzing und führten eine manuelle Überprüfung der sicherheitsrelevanten Code-Teile (insbesondere hinsichtlich der Erzeugung von Zufallszahlen und der korrekten Verwendung von kryptographischen Primitiven) durch. Der Quelltext von Exodus und Trust Wallet ist nicht öffentlich, daher setzten wir hier Werkzeuge für Reverse Engineering und Debugging ein.

6 Generelle Untersuchungsmethodik

Im Folgenden beschreiben wir eine allgemeine Vorgehensweise, die generell bei der Untersuchung von Produkten aus dem Blockchain-Ökosystem verwendet werden kann. Nicht alle Methoden können auf jedes Produkt angewandt werden, zum Beispiel ist eine statische Codeanalyse nur bei vorliegendem Quellcode möglich. Zumeist wird aber damit begonnen, ein Verständnis vom Produkt zu entwickeln, wofür sich insbesondere ein Review des technischen Konzepts eignet.

6.1 Review des technischen Konzepts

Ein Review des technischen Konzepts erfolgt im Regelfall auf Grundlage der vom Hersteller veröffentlichten Konzeptpapiere und anderer Dokumentation. Liegen diese nicht vor, so kann das Konzept erst nach umfangreichem Reverse Engineering beurteilt werden, soweit dies überhaupt möglich ist. Je nach Umfang und Detailtiefe der vorliegenden Dokumentation kann das technische Konzept nur teilweise oder nur auf einem höheren Abstraktionslevel beurteilt werden. Aufgrund der vorliegenden Dokumentation wird zunächst die Grundidee extrahiert und dann in mehreren Schritten das gesamte Konzept geprüft, um ein Verständnis für das Produkt zu entwickeln. Auf Basis der Grundidee werden insbesondere die zu schützenden Werte (z.B. monetäre Werte, persönliche Daten) identifiziert, damit deren angemessener Schutz im weiteren Verlauf geprüft werden kann, sowie darüber hinaus die Akteure und deren Motivation identifiziert.

Nach der Identifikation der Grundidee wird das Konzept darauf aufbauend detaillierter untersucht. Hierbei wird für die verwendeten Komponenten untersucht, welche Sicherheitseigenschaften sie erfüllen müssen, um ihrer jeweiligen Aufgabe gerecht zu werden. Zudem wird eingeschätzt, ob dies unter den vorliegenden Bedingungen plausibel ist. Bei selbst entwickelten Komponenten wird dieser Prozess ggf. rekursiv wiederholt, bis bekannte Standardkomponenten oder (kryptographische) Primitiven identifiziert werden, für die eine solche Einschätzung möglich ist. Da insbesondere die korrekte Nutzung von kryptographischen Primitiven nicht trivial ist, wird ggf. notiert, worauf bei der Prüfung der Umsetzung besonderes Augenmerk gelegt werden muss. Falls der Hersteller eine (Sub-)Komponente selbst entwickelt hat, statt auf eine Standardlösung zurückzugreifen, obwohl das an dieser Stelle aufgrund der Anforderungen an die Komponenten sinnvoll erscheint, wird besonderes Augenmerk auf die Begründung hierfür gelegt.

Nachdem der Aufbau des Produkts bzw. der Zusammenhang der Komponenten aufgearbeitet ist, wird geprüft, ob das vorgelegte Konzept dazu geeignet ist, ein angemessenes Schutzniveau für die zuvor identifizierten Schutzgüter sicherzustellen.

6.2 Einrichtung einer Testumgebung

Um die Funktion von Produkten in verschiedenen Betriebszuständen zu analysieren, muss eine Testumgebung aufgesetzt werden, in der diese Zustände simuliert werden können. Die Art der Testumgebung ist stark vom Produkt abhängig, im Allgemeinen ist es aber üblich, zunächst eine möglichst einfache Umgebung aufzusetzen. Für Software-Produkte kann dies z.B. durch eine virtuelle Maschine mit einem frisch installierten, aktuellen Betriebssystem ohne Spezialkonfiguration realisiert werden. Die Verwendung von virtuellen Maschinen vereinfacht auch die Reproduktion von Tests, da es die Snapshot Funktion erlaubt, den Zustand einer Maschine zu speichern und die Maschine später wieder auf diesen Zustand zurückzusetzen. Zusätzlich ist es häufig erforderlich, eine individuelle Entwicklungsumgebung, je nach Programmiersprache, für ein Produkt einzurichten, um möglichst effektiv den Quelltext während der Laufzeit zu untersuchen und gegebenenfalls zusätzliche Analysefeatures aktivieren zu können.

Je nachdem welches Verhalten des zu untersuchenden Produkts analysiert werden soll, muss die Testumgebung unterschiedlich konfiguriert werden. Für die Analyse des Netzwerkverkehrs kann beispielsweise eine andere Umgebung erforderlich sein als für das Debuggen des Produkts. Die

Testumgebung ist daher stark vom Produkt, vom durchzuführenden Test und von den Präferenzen des Prüfers abhängig und kann nicht generell beschrieben werden.

6.3 Statische Codeanalyse / Static Application Security Testing (SAST)

Hierzu werden Programme eingesetzt, welche den reinen Quelltext ohne Laufzeitinformationen vor dem Kompilieren auf Fehler und Qualität überprüfen. Die Qualität des Quelltextes ist für die Anwendungssicherheit als wichtig einzustufen. Der Grund liegt darin, dass sich in unübersichtlichem und unverständlichem Quelltext leichter Fehler einschleichen und unbemerkt bleiben können. Für die meisten verbreiteten Programmiersprachen existieren bereits eine Reihe an Werkzeugen für solche Analysen. Die Funktionsweise dieser Werkzeuge sieht häufig vor, den Quelltext oder dessen abstrakten Syntaxbaum sowie andere statische Zwischenformate nach bekannten Fehlermustern zu durchsuchen. Diese Werkzeuge produzieren häufig eine große Menge an Informationen wie Warnungen, Qualitätsmaße und Verbesserungsvorschläge. Aufgrund der großen Informationsflut und häufigen „False-Positives“ eignen sich diese Werkzeuge alleine nicht für eine Sicherheitsanalyse des Programmcodes. Nichtsdestotrotz sind diese Werkzeuge besonders einfach aufzusetzen und auszuführen und eignen sich dafür, einen Gesamtüberblick über die Qualität des Codes zu erlangen. Sie geben somit erste Hinweise für Programmpfade, die manuell oder dynamisch untersucht werden können. Voraussetzung hierfür ist Zugang zum Quelltext.

6.4 Abhängigkeiten-Analyse / Software Composition Analysis (SCA)

Diese Werkzeuge analysieren die Abhängigkeiten der Software von Drittquellen. Solche Abhängigkeiten gehören heutzutage zum Tagesgeschäft und werden vor allem im Bereich der Programmiersprachen Java, Javascript und Kotlin exzessiv eingesetzt, um die gewünschte Funktionalität zu erreichen. Aus Entwicklungssicht ist ein solcher modularer Aufbau sinnvoll. Aus Sicherheitsperspektive empfiehlt sich jedoch ein zurückhaltender Einsatz, da Verantwortlichkeiten und Vertrauen auf Dritte ausgelagert werden. Häufig enthalten eingebundene Programmbibliotheken selbst Sicherheitslücken, die die Sicherheit der Gesamtanwendung gefährden.

Die Funktionsweise dieser Tools ist denkbar einfach. Jede der Abhängigkeiten besitzt eine eindeutige Zeichenkette, die „Common Product Enumeration“ (CPE). Zusätzlich wird die gesamte CVE-Datenbank heruntergeladen und nach den gefundenen CPEs durchsucht. Die SCA ist ebenfalls alleine nicht ausreichend. Eine mit SCA gefundene Schwachstelle ist noch keine Garantie, dass diese Schwachstelle auch ausnutzbar ist. Beim Einbinden einer Abhängigkeit wird häufig nur eine minimale Funktionalität eingesetzt, über die die Schwachstelle der Programmbibliothek möglicherweise nicht ausnutzbar ist. Eine manuelle Analyse der gefundenen Schwachstellen ist daher zwingend notwendig. Der Nutzen von SCA ist damit ähnlich dem Nutzen des SAST. Für SCA ist der Zugang zum Quelltext in der Regel nicht notwendig, da Abhängigkeiten häufig auch aus einer kompilierten Anwendung extrahierbar sind.

6.5 Manuelles Review des Quelltextes

Ist das technische Konzept verstanden, ist eine manuelle Analyse des Quelltextes der sinnvolle nächste Schritt. Eine solche Analyse dient der Zuordnung der Komponenten des technischen Konzepts auf die Code-Architektur, z.B. auf Module und Pakete. Als Hilfestellung wird zeitgleich der Code zur Laufzeit im Debug-Modus untersucht und die Zuordnung bestätigt. Eine funktionierende Testumgebung ist dafür Voraussetzung. Ist die Code-Architektur verstanden, kann man damit beginnen, Teile des Quelltextes einer Sicherheitsanalyse zu unterziehen. Die manuelle Analyse eignet sich nur für die Analyse kleinerer Teile des Codes und skaliert bei komplexen Programmstrukturen nicht. Die folgende Liste soll hervorheben, nach welchen Kriterien Teile des Codes für ein manuelles Review ausgesucht werden können.

- Im Idealfall haben Analysen aus SAST und SCA bereits erste Hinweise für Schwachstellen hervorgebracht, sodass man sich anfangs auf die betroffenen Teile des Quelltextes konzentrieren kann.

- Neben den Hinweisen aus SCA und SAST sind kryptographische Komponenten – insbesondere die selbst implementieren und daher nicht untersuchten – geeignete Kandidaten für ein manuelles Review. Um jedoch die Implementierung eines kryptographischen Bausteins vollständig auf Sicherheit zu untersuchen, ist eine breit angelegte, eigenständige Analyse notwendig, die den Rahmen einer allgemeinen Untersuchung der Anwendungssicherheit sprengen würde. Nichtsdestotrotz ist eine Untersuchung auf Konformität der Implementierung mit akzeptierten Standards, z.B. „Request for Comments“ (RFC), ein geeignetes Mittel, um die Sicherheit von kryptographischen Implementierungen im Rahmen einer allgemeinen Analyse der Anwendungssicherheit mithilfe des manuellen Code-Reviews auszuloten. Des Weiteren gibt es mehrere Eigenschaften, welche auf eine unsachgemäße Implementierung der Kryptographie hinweisen. Zum einen ist die Verwendung von Zufall, je nach Verfahren, eine sicherheitskritische Stelle. Hier ist insbesondere darauf zu achten, dass ausreichende Mengen an Entropie für Schlüssel und Zufallsgenerierung genutzt werden. Wird weniger Entropie als für die Schlüssellänge notwendig verwendet, bestehen die Sicherheitsgarantien des kryptographischen Verfahrens nicht mehr. Die Verwendung von mehr Entropie als für die Schlüssellänge notwendig ist spricht dagegen für einen unsachgemäßen Einsatz von Kryptographie und ein genauerer Blick könnte Fehler zu Tage fördern. Einen besonderen Stellenwert in den Blockchain-Implementierungen nimmt die deterministische Verwendung des Signaturverfahres ECDSA (Elliptic Curve Digital Signature Algorithm) ein. Deterministische Signaturen sind besonders anfällig für die sogenannten „Fault Injection Attacks“, welche z.B. mithilfe der Methode „Rowhammer“ durchgeführt werden können. Erste Zeichen für Anfälligkeiten sind aufeinanderfolgende Signaturen für identische Nachrichten. Können solche Signaturen sogar extern ausgelöst werden, ist Vorsicht geboten.
- API-Implementierungen stellen häufig die größte Angriffsoberfläche dar, da sie mit potenziell böswilligen Eingaben arbeiten müssen. Die Untersuchung der Validierungsmechanismen solcher Eingaben geben einen Einblick in die Qualität der Implementierung. Des Weiteren ist es notwendig, festzustellen, für welche Benutzer oder Systeme die API-Funktion zugreifbar ist. Eine allumfassende Einsicht in die Sicherheit einer API-Funktion lässt sich allerdings mit manuellem Code-Review nur in seltenen Fällen erreichen. Mit der Methode des „Fuzzing“ lassen sich solche Schnittstellen genauer testen.

6.6 Reverse Engineering

Liegt eine Anwendung nicht im Quelltext vor, ist ein Review des Programmcodes mit mehr Aufwand verbunden. Durch Reverse Engineering können dennoch einige Einsichten über die Anwendung gewonnen werden. Je nach verwendeter Programmiersprache gibt es unterschiedliche Tools, die den Programmcode in ein für Menschen lesbares Format übersetzen. Unterschieden werden dabei Disassembler und Decompiler. Ein Disassembler übersetzt Binärcode in Assemblercode, während ein Decompiler die Rekonstruktion des Binärcodes in eine Hochsprache wie C oder Java zum Ziel hat und dadurch die Lesbarkeit weiter erhöht. Hat man den Code in einer Assembler- oder Hochsprache vorliegen, kann man analog zum Review des Quelltextes vorgehen. Das Review ist jedoch generell zeitaufwändiger, da im Code Kommentare und häufig auch sprechende Variablen- und Methodennamen fehlen.

Auch bei Anwendungen, die im Quelltext vorliegen, kann Reverse Engineering notwendig sein. Beispielsweise werden in proprietärer Software Code-Obfuszierungstechniken verwendet, um die Analyse des Programmcodes zu erschweren. Das bedeutet, der Programmcode wird derart abgeändert, dass er für Menschen schlechter lesbar ist. Beispielsweise werden sprechende Variablennamen durch zufällig generierte Namen ersetzt, oder der Kontrollfluss des Programms durch Dummy-Funktionen verkompliziert. Auch hier existieren je nach Sprache Tools, die versuchen, die Obfuszierung automatisiert rückgängig und den Programmcode dadurch lesbarer zu machen. Die Qualität derartiger Tools variiert jedoch stark. Als letzter Ausweg stehen dem Tester dynamische Methoden wie Debugging zur Verfügung. Das Beobachten des Programms zur Laufzeit gewährt häufig trotz Obfuszierung hilfreiche Einblicke in die Funktionsweise der Anwendung. Diese Methode ist jedoch ebenfalls mit einem sehr hohen Zeitaufwand verbunden und kann daher meist nur für ausgewählte Teile des Programmcodes durchgeführt werden.

6.7 Dynamic Application Security Testing (DAST)

Ist der Quelltext zu komplex, z.B. durch viele Verzweigungen und Datentypen, dann skaliert das manuelle Code-Review nicht mehr. Dies ist häufig bei größeren APIs der Fall. In diesem Fall empfiehlt sich der Einsatz von sogenannten „Fuzzern“. Diese Werkzeuge sind darauf ausgelegt, möglichst viele Programmpfade automatisiert auf Sicherheit zu testen. Das Testen der Programmpfade wird je nach Fuzzer mal mehr mal weniger intelligent durchgeführt. Ein Programmpfad wird in der Regel getestet, indem eine bestimmte Eingabe durch die Anwendung verarbeitet wird. Fuzzer erzeugen eine große Menge an Eingaben und liefern diese an die angegebene Schnittstelle in der Anwendung, während im Hintergrund das Verhalten der Anwendung aufgezeichnet wird, um Fehler zu rekonstruieren. Zusammengefasst ist die Hauptaufgabe des Fuzzers, Fehler in der Anwendung zu provozieren.

6.7.1 Fuzzing

Es existiert eine Vielzahl an Fuzzern und die Auswahl muss für eine effektive Analyse der Anwendungssicherheit wohlüberlegt sein. Dabei wird zwischen zwei verschiedenen Arten von Fuzzing unterschieden:

- Blackbox Fuzzing: Hier wird eine Software untersucht, die z.B. nur als ausführbare Datei vorliegt. Der Quellcode der Software steht für diesen Test nicht zur Verfügung. Das heißt, dass die Software ausgeführt und dann auf alle möglichen Eingaben untersucht werden muss. So lassen sich Fehler durch unvorhergesehene Benutzereingaben und API-Aufrufe finden. Für die Tests können „Dumb Fuzzer“ oder „Grammar Fuzzer“ verwendet werden. Ersterer verändert eine Eingabe zufällig. So wird zum Beispiel ein gegebener Benutzername „Test123“ zu „Teet55555“. Wird die Eingabe nicht richtig verarbeitet, kann zum Beispiel eine zu kurze, eine zu lange oder eine Eingabe mit Sonderzeichen zu einem Fehler führen. Bei einem „Grammar Fuzzer“ wird die Eingabe in Form einer Grammatik vorgegeben. Zum Beispiel kann die Grammatik eine HTML-Datei beschreiben, sodass jede Seite ein „html“, „head“ und „body“ Tag in einer bestimmten Reihenfolge enthalten muss. Der Fuzzer generiert verschiedene Eingaben und verwirft automatisch alle Ergebnisse, die nicht der Grammatik entsprechen. So kann sichergestellt werden, dass nur Eingaben überprüft werden, die vom System zugelassen sind und so effizienter nach komplexen Fehlern gesucht werden.
- Whitebox Fuzzing: Neben der Software, die auf Fehler untersucht werden soll, steht beim Whitebox Fuzzing auch der Quellcode der Anwendung zur Verfügung. Dies hat den Vorteil, dass im Programmcode überprüft werden kann, welche Stellen im Ablauf des Programms mit einer bestimmten Eingabe erreicht werden. Die Eingabe kann im nächsten Schritt so verändert werden, dass eine andere Abzweigung im Programmablauf durchlaufen wird. Ziel ist es, dass am Ende alle Zeilen im Programmcode mindestens einmal erreicht werden, um so tief im Programmcode versteckte Bugs zu finden.

6.7.2 Fehlererkennung

Im einfachsten Fall stürzt die Anwendung durch einen induzierten Fehler einfach ab, was sehr leicht zu erkennen ist. Kompliziertere Fehler, wie z.B. Speicherlecks, sind subtiler und können nur durch zusätzliche Werkzeuge entdeckt werden. Solche Werkzeuge sind in der Regel bereits in Compilern eingebaut und können bei Bedarf während des Kompilierungsprozesses in Form von Flags aktiviert werden. Besonders fortgeschritten ist der Compiler clang für C++ mit seinen Sanitizer-Werkzeugen. Die Funktionsweise der Sanitizer sieht vor, das Programm-Layout während des Kompilierens mit zusätzlichen Kontrollmechanismen zu versehen, z.B. mithilfe von „Shadow Memory“. Diese Kontrollmechanismen überwachen z.B. das Speicherlayout der Anwendung während der Ausführung und erstellt detaillierte Fehlermeldungen bei erfolgreicher Detektion.

6.8 Analyse des Netzwerkverkehrs

Durch die Analyse des Netzwerkverkehrs eines Produkts lässt sich bestimmen, wie gut Daten bei der Übertragung geschützt sind und an welche Systeme überhaupt Daten übertragen werden. Dazu wird der Netzwerkverkehr eines Produkts über ein Testsystem geleitet. Auf dem Testsystem kann der Verkehr passiv mit wireshark untersucht werden. Unverschlüsselter Netzwerkverkehr, beispielsweise über HTTP, lässt sich damit mit wenig Aufwand identifizieren. Verwendet das Produkt TLS, sollten zusätzlich aktive Tests durchgeführt werden, da bei der Zertifikatsprüfung immer wieder Fehler gemacht werden. Tools wie mitmproxy können genutzt werden, um die Zertifikatsprüfung zu testen. Zur Identifizierung der übertragenen Daten kann zudem manuell die Zertifikatsüberprüfung des Produkts deaktiviert werden. Der Netzwerkverkehr sollte über einen langen Zeitraum und unter Verwendung möglichst vieler Funktionen des Produkts untersucht werden.

7 Grundsätzliche Beobachtungen und typische Schwächen

Die im Rahmen dieses Projektes durchgeführten Untersuchungen deuten auf zwei wesentliche strukturelle Probleme hin, die eine breite Anzahl von Blockchain-Produkten und -Technologien betreffen: die große Anzahl an Abhängigkeiten zu fremden Programmbibliotheken und identische Code-Bausteine, die von einer Vielzahl von Implementierungen geteilt werden.

Wie in den folgenden Abschnitten noch dargelegt wird, nutzen Implementierungen im Blockchain-Ökosystem häufig eine Vielzahl von fremden Programmbibliotheken, die, insbesondere im Fall von nodeJS, häufig direkt aus einem Github-Projekt importiert werden. Obwohl Anwendungen, die nicht aus dem Blockchain-Ökosystem stammen, sicherlich auch auf einer großen Menge von Programmbibliotheken basieren, stellen sich hier im Kontext der Blockchain besondere Herausforderungen. Insbesondere Basis-Technologien, Digitale Währungen und Blockchain-Anwendungen basieren darauf, dass unter allen Nutzern Einigkeit darüber besteht, was die aktuelle Version der Client-Software ist, die zur Teilnahme an dem Netzwerk genutzt werden soll. Eine Änderung an der Client-Software vorzunehmen, ist daher sehr aufwändig und immer mit dem Risiko verbunden, dass nicht alle Nutzer auf die neue Version umsteigen und es zu einem Fork in der Blockchain kommt. Das ist anders als beispielsweise bei Windows, wo Microsoft theoretisch alle Nutzer dazu zwingen kann, ein bestimmtes Sicherheitsupdate zu installieren. Die Abhängigkeit von einer großen Menge von Programmbibliotheken verursacht daher im Blockchain-Kontext spezielle Herausforderungen im Sicherheits- und Patch-Management, die bisher nur unzureichend adressiert werden. Das direkte Einbinden von Programmcode aus einem Github-Projekt birgt außerdem die Gefahr, dass Besitzer des Projekts unbemerkt Schadcode in fremde Anwendungen einschleusen können – wie jüngst im Fall der Bitcoin-Wallet „Copay“ geschehen[9].

Darüber hinaus nutzen Blockchain-basierte Produkte und Technologien in der Regel kryptographische Primitive, um bestimmte Sicherheitseigenschaften zu erzielen. Die Implementierung dieser Primitive basiert jedoch häufig auf einer geteilten Code-Basis. Besonders auffällig ist dies bei der Implementierung der elliptischen Kurve „secp256k1“, die für die Erstellung und Prüfung von Signaturen verwendet wird. Eine Vielzahl von Produkten nutzen hierfür die öffentlich verfügbare Implementierung von Bitcoin. Zwar ist es grundsätzlich eine gute Empfehlung, kryptographische Primitive nicht selbst zu implementieren, sondern ausreichend getestete Standardimplementierungen zu verwenden, jedoch ist es fraglich, ob die Bitcoin-Implementierung von „secp256k1“ diese Anforderung erfüllt. Abbildung 27 zeigt die Github-Seite der Implementierung und lässt erkennen, dass auch die Entwickler Zweifel an der Eignung der „secp256k1“-Bibliothek für einen produktiven Einsatz haben.

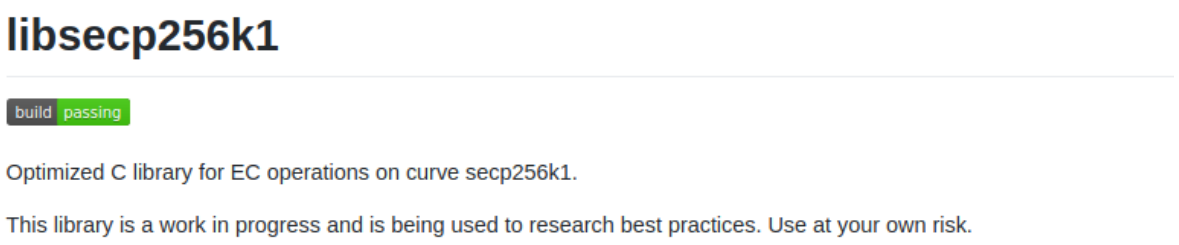

Abbildung 27: Öffentlich verfügbare Implementierung der Kurve „secp256k1“ aus dem Github-Repository von Bitcoin.

[9]https://www.heise.de/security/meldung/NPM-Paket-EventStream-mit-Schadcode-zum-Stehlen-von-Bitcoins-infiziert-4233171.html

Falls ein sicherheitskritischer Implementierungsfehler in dieser Forschungsimplementierung gefunden werden sollte, stellt sich die Frage, wie damit umgegangen werden kann. Wenn der Fehler allen betroffenen Herstellern gleichzeitig gemeldet wird, besteht die Gefahr, dass einzelne Hersteller den Fehler in Konkurrenzprodukten ausnutzen, bevor er behoben wurde. Die Lösung dieses Dilemmas bleibt eine zu lösende Herausforderung für eine Vielzahl von Blockchain-Produkten und -Technologien.

8 Schlussfolgerungen

Zusammenfassend lässt sich sagen, dass Produkte und Technologien aus dem Blockchain-Ökosystem einen ungewöhnlich hohen Security-Reifegrad haben – insbesondere, wenn man das geringe Alter des Technologiefelds bedenkt. Hier scheint sich eine grundlegend andere Entwicklung vollzogen zu haben als beim „Internet of Things“. Während bei Produkten aus dem Internet of Things häufig bereits ganz grundlegende Sicherheitsmaßnahmen, wie Authentifizierung oder Transportverschlüsselung, fehlen oder falsch angewendet wurden, scheinen die Entwickler von Blockchain-Produkten nicht den gleichen Fehler begangen zu haben. Die Gründe dafür lassen sich in der starken Fokussierung auf IT-Sicherheit und in dem hohen Finanzvolumen im Blockchain-Markt vermuten. Beide Faktoren machen es für IT-Sicherheitsexperten attraktiv, in dem Umfeld von Blockchain tätig zu werden.

Es ist allerdings auffällig, dass nur sehr wenige Konzepte und Lösungen aus dem Blockchain-Ökosystem wissenschaftlich fundiert untersucht wurden. Das lässt sich insbesondere an der geringen Anzahl an veröffentlichten wissenschaftlichen Publikationen, die ein Peer-Review-Verfahren durchlaufen haben, erkennen. Das ist vor allem deswegen problematisch, weil die Sicherheitsgarantien, die von verschiedenen Produkten gegeben werden, neuartig und häufig nicht vollständig verstanden sind. Sie sollen in der Regel durch eine Kombination von verschiedenen kryptographischen Maßnahmen erreicht werden. Würde man sich an der aus der Kryptographieforschung bekannten Standardmethodik orientieren, wäre die Anfertigung eines formalen Sicherheitsnachweises erforderlich, womit keine der bekannten Blockchain-Technologien aktuell dienen kann.

Bei der Untersuchung von ausgewählten Produkten und Technologien hat sich gezeigt, dass bekannte Methodiken aus dem klassischen Penetration Testing (wie z.B. statische Codeanalyse, Fuzzing und Reverse Engineering) auch für Blockchain-Produkte anwendbar sind. Eine Herausforderung ist dabei allerdings der hohe initiale Aufwand der bereits zum Aufsetzen eines Testsystems notwendig ist. Da die Blockchain-spezifischen Code-Teile (z.B. die Implementierung der elliptischen Kurve) in vielen Produkten identisch sind, ist es fraglich, ob die Erstellung einer eigenen Testmethodik für Blockchain-Produkte notwendig ist. Es scheint zielführender, eine zielgerichtete Untersuchung der in dieser Form geteilten Code-Bausteine durchzuführen, da die Ergebnisse eine Vielzahl von Produkten betreffen werden. Das betrifft insbesondere die unter vielen Produkten geteilte Implementierung der kryptographischen Primitiven, aber auch die „Bitcoin Improvement Proposals“ (BIP), die eine zu RFCs ähnliche Funktion im Blockchain-Ökosystem übernehmen.