M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 137

Für bare Münze? NutzerInnenerfahrungen mit Sicherheit und Datenschutz bei Bitcoin[1]

Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, Edgar Weippl[2]

Abstract:

Im vorliegenden Paper wird die erste großangelegte NutzerInnenstudie zu Bitcoin vorgestellt. Dabei wird untersucht, wie die NutzerInnen das Bitcoin-Ökosystem im Hinblick auf Sicherheit, Datenschutz und Anonymität bewerten. 990 Bitcoin-NutzerInnen wurden mittels Online-Fragebogen befragt, um Strategien der Bitcoin-Verwaltung zu identifizieren und festzustellen, welche Sicherheitsmaßnahmen NutzerInnen zum Schutz ihrer Schlüssel und Bitcoins ergreifen. Dabei stellte sich heraus, dass 46 % der TeilnehmerInnen webbasierte Lösungen zur Verwaltung von Bitcoins verwenden und etwa die Hälfte davon ausschließlich solche Lösungen verwendet. Es zeigte sich auch, dass viele NutzerInnen die Sicherheitsmaßnahmen ihres Bitcoin-Verwaltungstools nicht voll ausschöpfen und falsch informiert sind, was die Anonymität und den Schutz ihrer Daten im Bitcoin-Netzwerk angeht. 22 % der TeilnehmerInnen haben bereits durch Sicherheitsvorfälle oder eigenes Verschulden einen finanziellen Verlust erlitten. Zum besseren Verständnis der beobachteten Phänomene wurden zusätzlich qualitative Interviews geführt. Außerdem wird eine umfassende Methode zur Kategorisierung von Bitcoin-Clients vorgestellt, mit der NutzerInnen rasch einen Überblick über die technischen Eigenschaften verschiedener Tools erhalten und leicht abschätzen können, was das für die Kontrolle und Verifizierbarkeit durch die NutzerIn bedeutet.

1 Einleitung

Mit einer Marktkapitalisierung von über 3,5 Milliarden US-Dollar ist Bitcoin die derzeit erfolgreichste Kryptowährung. Bitcoin wird für ca. 130.000 Transaktionen täglich verwendet [Bl14] und ist immer wieder in den Medien präsent. Nach dem Erfolg von Bitcoin sind mehrere weitere Kryptowährungen entstanden, sowohl basierend auf Bitcoin als auch Neuentwicklungen.

Obwohl Kryptowährungen zunehmend an Beliebtheit gewinnen, sind sie noch kein Massenphänomen. Einer der Gründe dafür ist, dass sich Bitcoin-NutzerInnen gezwungenermaßen mit kryptografischen Grundlagen und Schlüsselverwaltung auseinandersetzen müssen, wodurch die Verantwortung für den Großteil der Sicherheitsmaßnahmen im Gegensatz zu Zentralwährungssystemen auf den Endnutzer übergeht. Obwohl verschiedenste Software zur Verwaltung von Bitcoins verfügbar ist, müssen die NutzerInnen sich dennoch mit den technischen Grundlagen auseinandersetzen und Backups erstellen, um im Fall eines Verlustes ihr virtuelles Geld wiederherstellen zu können. Daher weisen diese Systeme

[1] Das Paper ist eine deutsche Version des Papers: Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. In Proceedings of Financial Cryptography 2016, Barbados, February 2016.

[2] SBA Research, 1040 Wien, Österreich, (firstletterfirstname)(lastname)@sba-research.org

keine Resilienz im Bezug auf menschliches Versagen auf. Berichte aus Onlineforen und von Mailinglisten zeigen, dass viele Bitcoin-NutzerInnen bereits aufgrund der mangelnden Benutzerfreundlichkeit des Schlüsselmanagements sowie durch Sicherheitsvorfälle, etwa betrügerische Online-Börsen oder Wallets, Verluste erlitten haben. Daher ist es notwendig, das Interaktionsverhalten von NutzerInnen mit dem Bitcoin-Ökosystem zu untersuchen.

Bitcoin-NutzerInnen steht eine große Bandbreite an Werkzeugen zur Verwaltung ihres virtuellen Vermögens zur Verfügung. Diese werden üblicherweise als 'Wallets' bezeichnet. Ein Wallet wurde ursprünglich als Sammlung privater Schlüssel definiert [Es15]. Insofern könnte auch ein Stück Papier, auf dem der Schlüssel steht, oder sogar eine mentale Repräsentation desselben als Wallet bezeichnet werden. Die meisten dieser Tools verfügen aber neben der Schlüsselverwaltung auch über weitere Funktionalitäten, z.B. das Durchführen von Transaktionen. Im Gegensatz zu anderen kryptographischen Systemen, die auf öffentlichen Schlüsseln beruhen, z.B. PGP/GPG, ist Bitcoin nicht völlig kanalagnostisch. Die Interaktion mit dem Bitcoin-Netzwerk ist zwingend notwendig, um im verteilten System arbeiten zu können. Im Gegensatz zu anderen Signatursystemen müssen Bitcoin-Werkzeuge die Statusinformation durchgeführter Transaktionen bzw. Kontostände speichern.

Um Missverständnisse bei der Definition des Bitcoin-Wallets zu vermeiden, soll hier der weitreichendere Begriff *Coin Management Tool (CMT)* eingeführt werden. Ein CMT werde als Werkzeug oder Paket von Werkzeugen definiert, die es NutzerInnen erlauben, eine oder mehrere der Kernaufgaben von Kryptowährungen zu verwalten. In diesem Artikel soll daher der Begriff *Bitcoin-Verwaltung* verwendet werden, da er eine bessere Beschreibung der Aktivitäten von NutzerInnen bei der Interaktion mit dem Bitcoin-Ökosystem darstellt. Sicherheits- und Datenschutzaspekte von Bitcoin wurden bereits in der Vergangenheit untersucht [Bo15, GKL15, He15, Ge, Go]. Eine erste Untersuchung der Schlüsselverwaltung bei Bitcoin wurde in [Es15] vorgestellt. Der vorliegende Artikel beschreibt jedoch die erste umfassende NutzerInnenstudie, bei der Erfahrungen von NutzerInnen mit der Sicherheit und dem Datenschutz von Bitcoin erhoben werden.

Es handelt sich dabei um eine umfassende NutzerInnenstudie ($n = 990$) zur Interaktion von Mensch und Computer im Bitcoin-Ökosystem. Ziel der Untersuchung war es, zu verstehen, wie NutzerInnen mit Bitcoin interagieren und wie sie ihr virtuelles Vermögen verwalten. Außerdem wurden Erfahrungen und Wahrnehmungen zu Sicherheit, Datenschutz und Anonymität im Bitcoin-Netzwerk gesammelt. Die Datenerhebung wurde mittels einer Online-Umfrage mit 990 TeilnehmerInnen durchgeführt. Zusätzlich wurden mit 10 davon qualitative Interviews durchgeführt.

Im Zuge der Studie wurden interessante Erkenntnisse zur Interaktion von NutzerInnen mit dem Bitcoin-Netzwerk sowie zu den Datenschutz- und Sicherheitsmechanismen, die sie zum Schutz ihrer Schlüssel und ihres Vermögens nutzen, gewonnen. Dabei zeigte sich, dass sich an Platz 1 und 3 der meistverwendeten CMTs mit Coinbase und Xapo webbasierte Tools befinden, bei denen die NutzerInnen die Verantwortung für die Sicherheit an eine dritte Partei abgeben. Es stellte sich auch heraus, dass etwa ein Drittel der NutzerInnen dieser Tools nicht wusste, ob ihre CMT-Daten verschlüsselt und Sicherungskopien erstellt werden. Von den TeilnehmerInnen, die eine webbasierte Lösung verwendeten, ga-

ben 50 % an, dass sie ausschließlich dieses Tool verwendeten, während die andere Hälfte zusätzlich lokale Clients zur Verwaltung ihrer Bitcoins einsetzte. In Bezug auf Risikoszenarien und deren Eintrittswahrscheinlichkeit wurde das zweithöchste Risiko Schwachstellen in webbasierten CMTs zugeschrieben (nach Wertschwankungen und vor Diebstahl durch Malware).

Es zeigte sich auch, dass viele NutzerInnen eine falsche Vorstellung davon haben, wie sie anonym bleiben können. Ca. 25 % der TeilnehmerInnen gaben an, auf Bitcoin über das Tor-Netzwerk zuzugreifen, was sich in bestimmten Fällen ein Sicherheitsproblem darstellen kann [BP14, Al14]. 22,5 % der TeilnehmerInnen gaben an, Bitcoins durch Sicherheitsvorfälle verloren zu haben. Etwa die Hälfte davon sehen diesen Verlust als ihre eigene Schuld an und die meisten von ihnen konnten ihre Bitcoins nicht wiederherstellen und machten so einen permanenten Verlust. Die vorliegende Studie ist ein Beitrag zum Wissen über nutzerInnenzentrierte Bedenken beim Bitcoin-Management, da laut Bonneau [Bo15] im Falle von Bitcoin die Praxis der Theorie voraus ist.

2 Stand der Forschung

Unsere Studie baut auf früheren Forschungsarbeiten auf. Eskandari et al. [Es15] präsentierten einen ersten Blick auf die Schlüsselverwaltung bei Bitcoin durch eine Reihe von Evaluierungskriterien für Bitcoin-Wallets. Außerdem werden Usability-Aspekte der Software von Bitcoin-Wallets in einem Cognitive Walkthrough [Wh94] evaluiert. Die Studie von Eskandari et al. [Es15] kann als erste Untersuchung der Usability von Bitcoin angesehen werden. Bisher wurde keine empirische Studie mit Bitcoin-NutzerInnen zu Aspekten wie Sicherheit und Nutzbarkeit vorgestellt. Für Kryptowährungen wie Bitcoin ist eine Chiffrierung mit öffentlichem Schlüssel notwendig. Im Bereich von E-Mail haben hier zahlreiche Studien gezeigt, dass es bei der Usability von Schlüsselverwaltung und Verschlüsselung noch viele Probleme gibt [WT99, GM05, Ga05, Sh06]. Bislang gibt es für keinen dieser zwei Bereiche ein komplett anwendbares erfolgreiches Konzept. Die menschlichen Faktoren bei der Schlüsselverwaltung wurden bereits in anderen Bereichen untersucht [WT99, Ga05, GM05, Sh06, GFFK06]). Im Bitcoin-Ökosystem ist allerdings die sichere Schlüsselverwaltung allein nicht ausreichend, da die Kommunikation nicht kanalunabhängig ist, sondern einen elementaren Bestandteil des Sicherheitskonzepts darstellt.

3 NutzerInnenstudie: Methodologie

Ziel der Studie ist eine empirische Untersuchung der Sichtweise von EndnutzerInnen und deren Verhalten im Bitcoin-Ökosystem mit einem Schwerpunkt auf Sicherheitsmaßnahmen sowie die Verwaltung von Bitcoins und Schlüsseln mit den damit verbundenen Sicherheitsrisiken. Dazu wurde ein Online-Fragebogen erstellt, der durch qualitative Interviews ergänzt wurde. Die Forschungsfragen wurden auf Grundlage der bestehenden Literatur zu Bitcoin (s. 2) sowie einer qualitativen Inhaltsanalyse von Threads in Onlineforen und Mailinglisten formuliert. Außerdem wurden die verfügbaren Bitcoin-Wallets

und deren Leistungsumfang untersucht und als Inspiration für die Fragen sowie zur Entwicklung der Risikoszenarien verwendet. Der Fokus der Studie liegt auf Bitcoin, da dies zum Durchführungszeitpunkt (Juli 2015) die mit Abstand beliebteste Kryptowährung war. Während der Online-Fragebogen die Angaben der NutzerInnen zu Bitcoin-Verwaltungsverhalten und Risikowahrnehmung erheben sollte, wurden die zusätzlichen Interviews mit Bitcoin-NutzerInnen zum tiefergehenden Verständnis der wichtigsten Usability-Probleme und der Gründe für übliche Sicherheitsvorfälle geführt sowie auch, um zu eruieren, ob und wie verlorene Schlüssel wiederhergestellt werden konnten.

Mit der Studie sollten die folgenden Forschungsfragen zur NutzerInnenwahrnehmung in den Themenbereichen Verwaltung von Bitcoins und mit Bitcoins verbundene Sicherheitsrisiken beantwortet werden:

- *Q1: Was sind die wichtigsten Verwendungsszenarien für Bitcoins?*
- *Q2: Wie verwalten die TeilnehmerInnen ihre Bitcoins? Wie verhalten sich TeilnehmerInnen im Hinblick auf Sicherheit, Datenschutz und Anonymität?*
- *Q3: Wie nehmen die TeilnehmerInnen mit Bitcoin verbundene Sicherheitsrisiken wahr?*
- *Q4: Von welchen Sicherheitsvorfällen waren NutzerInnen in der Vergangenheit betroffen und wie bekamen sie ihre Bitcoin-Schlüssel und Bitcoins wieder?*
- *Q5: Was sind die größten Herausforderungen an Usability, denen sich NutzerInnen bei der Verwendung von Bitcoin stellen müssen?*

Detaillierte Information zu den Online-Umfragen,den Qualitativen Interviews sowie die genauen Fragestellungen des Fragebogens finden sich im englischen Originalpapier.

4 Ergebnisse

In diesem Abschnitt werden die erhobenen Antworten analysiert, um die in Abschnitt 3. definierten Forschungsfragen zu beantworten. Zu Beginn jedes Abschnittes werden zunächst die Ergebnisse der Online-Umfrage analysiert und dann den Ergebnissen aus den qualitativen Interviews gegenübergestellt, um die Erkenntnisse miteinander in Bezug zu setzen und zu erklären.

4.1 Allgemeine Verwendung von Bitcoin (Q1)

Die meisten TeilnehmerInnen gaben an, Bitcoin für Spenden zu verwenden (38,0 %), gefolgt von virtuellen Gütern und Dienstleistungen wie Webhosting oder Online-Zeitungen (33,3 %) Online-Shopping (27,5 %), alternative Kryptowährungen (altcoins) (26,5 %), Glücksspiel (26,5 %) und Bitcoin-Geschenkgutscheine (19,9 %). Etwa 5 % gaben an, mit Bitcoins Drogen zu kaufen oder dies in der Vergangenheit getan zu haben. 30,2 % gaben an, Bitcoin mindestens einmal pro Woche zu verwenden, 25 % verwenden Bitcoin mindestens einmal pro Monat und 19 % mindestens einmal täglich. Die übrigen TeilnehmerInnen gaben an, Bitcoin mindestens einmal pro Jahr oder noch seltener zu verwenden.

Die Ergebnisse lassen den Schluss zu, dass die Mehrheit der StudienteilnehmerInnen Bitcoin häufig verwendet. Die TeilnehmerInnen wurden auch nach ihrem aktuellen Bitcoin-Kontostand gefragt. Etwa die Hälfte der TeilnehmerInnen wollte hier keine Angabe machen. Die TeilnehmerInnen, die diese Frage beantworteten, haben ein Gesamtvermögen von etwa 8000BTC. Die Mehrzahl der TeilnehmerInnen (70 %) begann zwischen 2013 und 2015 mit der Verwendung von Bitcoin. 17 % begannen zwischen 2011 und 2012. 58,0 % gaben an, neben Bitcoin auch andere Kryptowährungen zu nutzen, allen voran Dogecoin und Litecoin. Die beliebtesten Bitcoin-Börsen waren BTCE (20,9 %), Bittrex (14,0 %) und Bitstamp (13,0 %). 11,4 % der TeilnehmerInnen sind derzeit am Mining von Bitcoins beteiligt. Die meisten begannen damit nach 2014. Vielen von denen, die früher mit dem Mining begannen, haben damit inzwischen wieder aufgehört, da sie der Meinung sind, dass es sich derzeit nicht lohnt. 195 TeilnehmerInnen (19,7 %) gaben an, einen vollen Bitcoin-Server zu betreiben, der über das Internet erreichbar ist. Als Hauptgrund dafür wurde angegeben, das Bitcoin-Netzwerk unterstützen zu wollen (60,5 %), gefolgt von der schnellen Verbreitung von Transaktionen (46,6 %), Netzwerkanalyse (30,3 %) und dem Erkennen von Double Spend-Attacken (26,1 %).

In den qualitativen Interviews gaben alle Teilnehmer an, Bitcoin häufig zu verwenden. Einige von ihnen sind auch im lokalen Bitcoin-Verein aktiv. Die meisten Interviewpartner nannten den dezentralen Charakter von Bitcoin als einen der Hauptgründe dafür, warum sie mit der Verwendung von Bitcoin begonnen hatten. Der zweithäufigste Grund war Neugier. Ein Teilnehmer, der zur Zeit des Ausbruchs des Konflikts zwischen der Ukraine und Russland auf der Krim lebte, nannte soziopolitische Gründe. Er arbeitete dort damals für ein US-Unternehmen und benötigte eine sichere und günstige Option, um sein Gehalt zu erhalten. Außerdem wollte er sichergehen, dass er durch die Annexion der Krim durch die Russische Föderation kein Geld verlieren würde. Für ihn war Bitcoin die beste Option und er sagte, dass zu der Zeit auf der Krim viele Menschen begonnen hätten, Bitcoin zu verwenden. Einige der TeilnehmerInnen waren vor einigen Jahren am Bitcoin-Mining beteiligt, als das Mining im kleinen Maßstab noch gewinnbringend war.

4.2 Bitcoin-Verwaltung (Q2)

4.2.1 Bitcoin-Wallets und Backup-Verhalten.

Tabelle 2 zeigt die am häufigsten verwendeten Bitcoin-Wallets. Bei dieser Frage waren Mehrfachantworten möglich, da das Verwenden von mehr als einem Wallet üblich ist. Die Tabelle zeigt die Anzahl sowie den Prozentsatz der TeilnehmerInnen, die ein bestimmtes Wallet verwenden. Außerdem zeigt Tabelle 2 sie, ob die NutzerInnen ihre Wallets mit einem Passwort schützen und ob sie verschlüsselt sind. Die Studie zeigte, dass die Mehrheit der NutzerInnen ihre Wallets mit einem Passwort schützen. Im Fall von Webclients wurde fehlendes Hintergrundwissen festgestellt. So gaben 47,7 % der Coinbase-NutzerInnen in der Umfrage an, ihr Wallet sei verschlüsselt, während 34 % sagten, sie wüssten nicht, ob es verschlüsselt sei. Bei Xapo, dem drittbeliebtesten Wallet in dieser Stichprobe, ist ein ähnlicher Trend festzustellen. Wie Coinbase ist es ein webbasiertes

Tool und ähnlich wie bei Coinbase gibt nur etwa die Hälfte der NutzerInnen an, dass es verschlüsselt sei, während ein Drittel es nicht weiß. Nur ein Drittel der Coinbase-NutzerInnen und 43 % der Xapo-NutzerInnen erstellen Sicherheitskopien von ihren Wallets. 33,9 % der Coinbase-NutzerInnen und 28,5 % der Xapo-NutzerInnen wissen nicht, ob von ihrem Wallet ein Backup besteht. Es stellte sich auch heraus, dass Bitcoin-NutzerInnen mit mehr als 0.42BTC (100 USD) von ihrem CMT nicht häufiger ein Backup erstellen als NutzerInnen mit weniger Bitcoins. Der Effekt ist statistisch signifikant ($\chi^2(1) = 5.1, p = 0.02$).

Die TeilnehmerInnen wurden auch gefragt, ob sie für den Fall eines Verlustes oder Diebstahls des primären Backups zusätzliche Backups erstellen. Bitcoin Core-NutzerInnen gaben dabei am häufigsten an, zusätzliche Backups zu erstellen - bei 64,0 % von ihnen war dies der Fall. Tabelle 1 zeigt die Angaben der NutzerInnen zu den Eigenschaften der Wallet-Backups. Den Ergebnissen der Studie zufolge speichert niemand das Backup auf einem durch Air Gap geschützten Computer. Die häufigsten genannten Eigenschaften der Backups waren Verschlüsselung und Passwortschutz. 197 Backups waren in einer Cloud gespeichert.

59,7 % der TeilnehmerInnen verwenden nur ein einziges Wallet zur Verwaltung ihrer Bitcoins, 22,7 % verwenden zwei und 10,6 % drei Wallets. Die übrigen 7 % verwenden vier oder mehr Wallets. Die höchste angegebene Zahl an Wallets war 14, wobei dieser Teilnehmer die Erklärung hinzufügte, er habe zuerst die verschiedenen Wallets ausprobieren wollen, um dann jene auszuwählen, die am besten seinen Bedürfnissen entsprachen. Etwa die Hälfte jener TeilnehmerInnen, die einen Web-Client benutzten, benutzten ausschließlich diesen zur Verwaltung ihrer Bitcoins, die andere Hälfte verwendete ihn zusätzlich zu einem lokalen Client.

Überraschenderweise zeigte sich, dass die Bitcoins der meisten TeilnehmerInnen in Armory gespeichert sind. Insgesamt hatten die Armory-NutzerInnen etwa 3818 BTC in ihren Armorys, wobei die fünf größten NutzerInnen angeben, 2000, 885, 300, 230 und 150 BTC zu haben. Die größte Summe an Bitcoins, die im Web-Client eines Teilnehmers gespeichert war, war 100 BTC. Insgesamt sind in Coinbase 238 BTC und in Xapo 157 BTC gespeichert.

Tab. 1: Eigenschaften der Backups (absolute Nennungen in absteigender Reihenfolge). Eine NutzerIn kann über mehrere Wallets und mehrere Backups verfügen.

Backup-Eigenschaften	**Nennungen**
Mein Backup ist verschlüsselt	662
Mein Backup ist passwortgeschützt	629
Mein Backup ist auf einem externen Speichermedium gespeichert (z.B. USB-Stick)	430
Mein Backup ist auf Papier gespeichert	334
Mein Backup ist in der Cloud gespeichert (z.B. Dropbox)	197
Mein Backup ist auf einem Air Gap-Gerät gespeichert	0

Tab. 2: Am häufigsten erwähnte CMTs nach Anzahl sowie Anteil der TeilnehmerInnen mit NutzerInnenangaben dazu, ob das CMT verschlüsselt ist, ob ein Backup davon erstellt wird und ob es ein zusätzliches Backup gibt (Ja (J), Nein (N), Weiß nicht (W.N.)) in Prozent der NutzerInnen. Die rechte Spalte zeigt die Gesamtsumme der Bitcoins, die die TeilnehmerInnen auf dem jeweiligen CMT gespeichert haben.

			Verschlüsselt?			Backup?			Zusätzliches Backup?			
CMT	**Anzahl**	**Prozent**	**J**	**N**	**W.N.**	**J**	**N**	**W.N.**	**J**	**N**	**W.N.**	**BTC**
Coinbase	314	31,7	47,5	18,5	34	35,5	30,6	33,9	30,3	66,9	2,8	238
Bitcoin Core	236	23,8	72,8	16,1	11,1	76,3	14,0	9,7	64,0	32,2	3,8	752
Xapo	179	18,1	51,4	19,0	29,9	43,0	28,5	28,5	41,3	57,5	1,2	157
Electrum	125	12,6	72,8	15,2	22,0	77,6	16	6,4	55,2	44	0,8	226
MyCelium	97	9,8	61,9	21,6	16,5	83,5	12,4	4,1	52,6	47,2	0,2	62

4.2.2 Anonymität.

Die Umfrage zeigte, dass 32,3 % der TeilnehmerInnen der Meinung sind, Bitcoin sei völlig anonym. Weitere 47,0 % sind der Meinung, dass Bitcoin per se zwar nicht anonym sei, aber anonym verwendet werden könnte. Allerdings sind etwa 80 % der Meinung, dass ihre Transaktionen nachverfolgt werden können. 25 % gaben an, Bitcoin zum Schutz ihrer Anonymität über Tor verwendet zu haben.

Die Frage, ob sie sich weiterer Anonymisierungsmaßnahmen bedienten, beantworteten 18 % mit “häufig”. Die meisten von ihnen gaben an, Bitcoin über Tor zu verwenden, gefolgt von mehreren Adressen, Mixing-Services, mehreren Wallets und VPN-Diensten. In der Forschung wurde bereits gezeigt, dass die Verwendung von Bitcoin über Tor einen Angriffsvektor erzeugt, der für deterministische Man-in-the-Middle Angriffe und Fingerprinting ausgenutzt werden kann. [BP14, Al14].

4.3 Risikowahrnehmung (Q3)

Ein weiteres Thema der Umfrage war die Wahrnehmung der Nutzerinnen zu Risiken von Bitcoin. Den TeilnehmerInnen wurden 11 Risikoszenarien vorgestellt, die auf Erkenntnissen aus der Literatur und Informationen aus Onlinequellen basierten. Jedes Risiko wurde leicht verständlich erklärt und die TeilnehmerInnen wurden gefragt, ob sie einen Risikoeintritt für wahrscheinlich oder unwahrscheinlich hielten. Abb. 1 zeigt die Einschätzung der TeilnehmerInnen zu den Risikoszenarien. Dabei zeigte sich, dass TeilnehmerInnen Kursschwankungen als höchstes Risiko einstufen, gefolgt von Schwachstellen in webbasierten Wallets und dem Diebstahl von Bitcoins mittels Malware. Das Risiko von Schwachstellen in der Kryptographie wurde als niedrigstes eingeschätzt, an zweitletzter Stelle standen Double Spending-Angriffe und davor DoS-Angriffe auf das Bitcoin-Netzwerk.

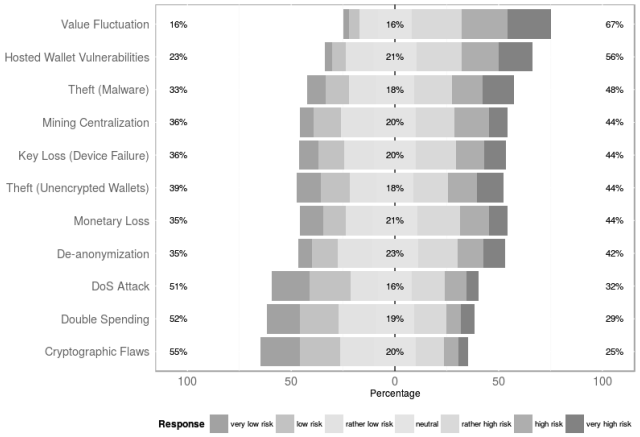

Abb. 1: NutzerInnenwahrnehmung der Risikowahrscheinlichkeit in Prozent der TeilnehmerInnen ($N = 990$).

4.4 Sicherheitsvorfälle (Q4)

Etwa 22,5 % gaben an, mindestens einmal einen Verlust von Bitcoins oder Bitcoin-Schlüsseln erlitten zu haben. Davon gaben 43,2 % als Grund einen selbstverschuldeten Fehler an, wie beispielsweise den Verlust des Geräts oder das versehentliche Löschen. Weitere genannte Risiken wurden wie folgt genannt: 26,5 % Hardware-Versagen, 24,4 % Software-Versagen. 18,0 % gaben an, ihre Schlüssel im Zuge eines größeren Sicherheitsvorfall durch Schadsoftware oder Hacker verloren zu haben. Die meisten von ihnen (77,6 %) wollten keine Angaben dazu machen, ob sie die Schlüssel wiederherstellen konnten. Von denen, die die Frage beantworteten, gelang es 65 % nicht, ihre Schlüssel wiederherzustellen. Insgesamt gaben die Teilnehmer an, etwa 660,6873 Bitcoins verloren zu haben. Dabei ist aber zu erwähnen, dass nicht nach dem Zeitpunkt des Verlustes gefragt wurde. Bei der Interpretation dieses Ergebnisses muss daher beachtet werden, dass der Bitcoin-Kurs starken Schwankungen ausgesetzt ist und es daher schwer ist, den Gesamtverlust in US-Dollar zu beziffern. Etwa 40 % der TeilnehmerInnen gaben an, Geld durch einen von ihnen als ernst eingestuften Sicherheitsvorfall verloren zu haben. 13,1 % der Gesamtstichprobe gaben an, durch HYIPS (high-yield investment programs) und Schneeballsysteme Bitcoins verloren zu haben. 7,9 % verloren auf Mt. Gox Bitcoins.

Die TeilnehmerInnen hatten auch die Möglichkeit, zu beschreiben, wie sie auf den Vorfall reagierten. Die meisten gaben an, nichts getan und den Verlust einfach akzeptiert zu haben. Einige sagten, der finanzielle Verlust sei so gering gewesen, dass es sich nicht gelohnt hätte, etwas zu unternehmen, oder dass sie sich hilflos fühlten und nicht wussten, was sie tun könnten. Jene, die etwas unternahmen, gaben meist an, Forderungen geltend gemacht und den Provider der Börse oder des Online-Wallets kontaktiert zu haben. Jene, die Geld an bösartige Online-Wallets verloren haben, gaben an, auf andere Wallet-Typen umgestiegen zu sein und keine webbasierten Wallets mehr zu verwenden. Die TeilnehmerInnen, die bei HYIPS Verluste machten, gaben meist an, dass sie aus ihren Fehlern gelernt hätten

und nun weniger risikoreiche Investitionen machten. Unabhängig von der Art des Sicherheitsvorfalls gaben viele TeilnehmerInnen an, darüber online in Foren gepostet und sich mit anderen Betroffenen ausgetauscht zu haben.

"Ich folge dem Motto 'investier nicht mehr, als du bereit bist, zu verlieren'." (P3848)

"Ich musste einfach akzeptieren, dass mein Geld gestohlen worden war ... und ich lernte daraus, Börsen niemals als Wallets zu verwenden. Man sollte alles bei sich behalten." (P3763)

"Ich habe einfach daraus gelernt. Es war unglaublich dumm von mir." (P853)

Bei den qualitativen Interviews gaben acht Personen an, bereits einmal durch einen Angriff oder einen Fehler Schlüssel und/oder Bitcoins verloren zu haben. Drei Teilnehmer waren vom Angriff auf Mt. Gox betroffen und zwei gaben an, gegen Kraken[5] Forderungen geltend gemacht zu haben. Ein Teilnehmer gab an, eine *physische* Casascius-Bitcoin-Münze[6] verloren zu haben; er habe aber aufgehört, danach zu suchen, da sie damals nur 9 US-Dollar wert gewesen sei. Andere gaben auch an, durch Geräteversagen, korrupte HDDs oder Softwareversagen Schlüsselverluste erlitten zu haben.

4.5 Bewertung der Usability (Q5)

Obwohl bei den qualitativen Interviews die meisten angaben, bei der Bitcoin-Verwaltung sehr auf Sicherheit und Datenschutz zu achten, sagten acht von ihnen, dass sie Bitcoin-AnwenderInnen ohne technisches Wissen zu webbasierten und deterministischen Wallets raten würden. Als Hauptgrund dafür wurde die einfache und praktische Handhabung genannt. Ein Teilnehmer sagte, er würde auf jeden Fall ein Wallet empfehlen, bei dem der private Schlüssel auf einem zentralen Server gespeichert ist, um den Schlüssel im Fall eines Verlustes leichter wiederherstellen zu können und so die Notwendigkeit von umfassenden Backups zu vermeiden und dass Gedächtnishilfen hilfreich wären. Sechs Teilnehmer sagten auch, dass sie MyCelium[7] als das am leichtesten verwendbare Wallet empfehlen würden. Jene, die bereits Erfahrung mit MyCelium hatten, waren der Meinung, der Papier-Backup-Prozess sei der sicherste und am nutzerfreundlichste dieser Art. Um mit MyCelium ein Papier-Backup zu machen, muss die NutzerIn ein Template ausdrucken, auf dem Teile des Schlüssels aufgedruckt sind, der dann von der NutzerIn händisch ergänzt werden muss. Einige Teilnehmer empfanden es anfangs als sehr ungewohnt, Papier-Wallets zu verwenden.

"Es fühlte sich irgendwie nicht ganz richtig an, den digitalen Raum zu verlassen." (P6 über Papier-Wallets)

Die meisten Teilnehmer strichen bei den Interviews die Notwendigkeit hervor, bereits in der Kindheit damit zu beginnen, das System zu erlernen. P2 sagte, Bitcoin sei inhärent

[5] `https://www.kraken.com/`
[6] `https://www.casascius.com/`
[7] `https://mycelium.com/`

komplex und dass die Grundidee von Verschlüsselung mit öffentlichen Schlüsseln in Schulen vermittelt werden sollte, und dass Währungssysteme Teil der Kultur seien.

"Kinder lernen schon in der Volksschule, wie unser Geldsystem funktioniert. Deswegen können wir als Gesellschaft Bargeld und Kreditkarten verwenden. Ich bin mir sicher, das könnte auch bei einer dezentralen Kryptowährung so sein." (P7)

Zwei Teilnehmer sagten außerdem, dass Anwenderoberflächen einfacher und minimalistisch sein sollten. Viele Teilnehmer sagten, dass für eine rasche Verbreitung von Bitcoin einfache und intuitiv zu bedienende Nutzeroberflächen wichtiger seien als Sicherheitsaspekte. Dies wurde damit begründet, dass auch Computer sich rasch verbreitet haben, obwohl die meisten Menschen nicht wissen, wie sie funktionieren, und dass Sicherheit bei der großflächigen Verbreitung nicht unbedingt ein Argument sei. Als Beispiele wurden Autos in den 1940er-Jahren, Computer, Kreditkarten und WhatsApp genannt. Sie sagten auch, dass die Summen, die im Bitcoin-Netzwerk zirkulieren, niedrig genug seien um das Risiko eines Verlustes eingehen zu können. Dieses Szenario wurde mit dem Verlustrisiko von Bargeld verglichen. Manche Teilnehmer schlugen auch vor, dass ein dediziertes Gerät für das Schlüsselmanagement mit einer intuitiven Nutzeroberfläche entwickelt werden könnte und waren der Meinung, dass so etwas die sicherste und nutzerfreundlichste Option wäre.

5 Diskussion

Unser Ziel war es, die in gestellten Forschungsfragen (3) zu beantworten, um zu verstehen, wie NutzerInnen mit Bitcoin interagieren. Bei dieser ersten NutzerInnenstudie mit Bitcoin-NutzerInnen wurden wertvolle Erkenntnisse gewonnen. Die Ergebnisse sollen hier in Beziehung zu bestehenden Forschungsarbeiten gestellt werden.

Bezüglich der Bitcoin-Verwaltung (Q2) zeigte sich, dass zwei der beliebtesten CMTs webbasierte Lösungen sind, bei denen die NutzerInnen sich nicht um Schlüsselverwaltung und Backups kümmern müssen. Interessanterweise wusste bei beiden Clients jeweils etwa ein Drittel nicht, ob ihr Wallet verschlüsselt ist oder ob ein Backup besteht. In diesem Szenario übertragen die NutzerInnen die Verantwortung an eine dritte Partei. Obwohl dies für nicht fachkundige NutzerInnen eine praktische und benutzerfreundliche Lösung zu sein scheint, bedeutet es, dass die NutzerIn darauf vertrauen muss, dass die dritte Partei sich um ihre Sicherheit kümmert. Etwa 50 % der Web-Client-NutzerInnen gaben an, zusätzlich einen lokalen Client zu verwenden, um ihr virtuelles Vermögen zu speichern. Die Antwort auf Q4 zeigt, dass ein bedeutender Teil der TeilnehmerInnen bereits Geld an bösartige Wallet-Provider verloren hat. Auch wurden Schwachstellen in webbasierten Wallets unter den Risikoszenarien an zweiter Stelle gereiht (Q5). Bei den qualitativen Interviews sagten einige Teilnehmer, dass sie unerfahrenen NutzerInnen empfehlen würden, zum Einstieg ein webbasiertes Wallet zu verwenden, da dies die nutzerfreundlichste Lösung sei. Bei den meisten anderen Lösungen müssen NutzerInnen zumindest die Grundlagen von Bitcoin und der Block-Chain verstehen.

Bitcoin ist ein pseudonymes System, in den Medien wird jedoch oft der Mythos verbreitet, es sei an sich anonym. Über ein Drittel der StudienteilnehmerInnen glaubt dies und gab an, zu denken, dass Bitcoin völlig anonym sei. Etwa die Hälfte der TeilnehmerInnen ist sich dessen bewusst, dass Bitcoin an sich nicht anonym ist, dass es aber anonym verwendet werden kann. Viele NutzerInnen gaben an, zur Wahrung ihrer Anonymität Bitcoin über Tor zu verwenden, wodurch aber ein Angriffsvektor für deterministische Man-in-the-Middle-Angriffe entsteht, wie in [BP14] gezeigt wurde. Die Ergebnisse deuten darauf hin, dass die StudienteilnehmerInnen auf die Kryptographie hinter Bitcoin vertrauen und sich der Risiken, die durch Kursschwankungen und Softwaresicherheitslücken entstehen können, bewusst sind. Schlechte Anwendbarkeit und mangelndes Wissen tragen stark zu Sicherheitsproblemen bei. Beinahe ein Viertel der TeilnehmerInnen gab an, bereits zumindest einmal einen Verlust von Bitcoins oder Schlüsseln erlitten zu haben (Q5). Überraschenderweise war beinahe die Hälfte dieser Verluste auf selbstverursachte Fehler zurückzuführen, was zeigt, dass moderne CMTs immer noch bisweilen schwer zu verwenden sind oder erfordern, dass NutzerInnen Sicherheitsmaßnahmen wie Backups und Verschlüsselung manuell durchführen. Die Studie zeigt, dass das Bitcoin-Ökosystem vor allem für Spenden sowie zum Erwerb digitaler Güter verwendet wird, zum Teil aber auch für kriminelle Aktivitäten und Glücksspiel.

6 Schlussfolgerungen

Im diesem Artikel wurde die erste Studie zu NutzerInnen-Interaktion mit dem Bitcoin-Ökosystem vorgestellt. Dabei wurde eine Online-Umfrage mit 990 NutzerInnen durchgeführt, die durch qualitative Interviews mit 10 Personen ergänzt wurden. Der Begriff *Coin Management Tool (CMT)* wurde eingeführt, um Tools zu beschreiben, mit denen NutzerInnen ihr virtuelles Vermögen verwalten und mit Bitcoin interagieren können. Es zeigte sich, dass die Verwaltung von Bitcoins weiterhin eine große Herausforderung darstellt, da viele von ihnen keine ausreichenden Sicherheitsmaßnahmen, wie Verschlüsselung oder Backups, durchführen. Viele der TeilnehmerInnen wussten nicht, welche Sicherheitsfeatures ihr CMT hatte. Zwei der beliebtesten CMTs unter den TeilnehmerInnen waren webbasierte Lösungen. Etwa die Hälfte der NutzerInnen dieser Lösungen gab an, nur Online-Clients zu verwenden, während die andere Hälfte sie mit lokalen Clients kombiniert. Obwohl Webclients eine nutzerfreundliche Lösung sein sollten, erfordern sie ein gewisses Maß an Vertrauen und übertragen die Verantwortung für Verschlüsselung und Backups an eine dritte Partei. Die Studie zeigte auch, dass 22,5 % der TeilnehmerInnen bereits Bitcoins verloren haben. Etwa die Hälfte davon gab als Grund eigenes Verschulden an, woraus ersichtlich ist, dass NutzerInnen es immer noch schwierig finden, ihre Bitcoins sicher zu verwalten. Wir sind davon überzeugt, dass unsere Erkenntnisse ein wichtiger erster Schritt zur Verbesserung der Sicherheit und Nutzbarkeit von Bitcoin sind. Um sichere Interaktionen mit dem Bitcoin-Ökosystem zu garantieren, müssen NutzerInnen, sowohl jene mit als auch jene ohne Fachwissen, das Konzept der Bitcoin-Verwaltung neu überdenken, da es um weit mehr geht als die Sicherung der geheimen Schlüssel. Bitcoin ist ein dezentrales System in dem die Interaktion zwischen Peers und die Verbreitung und Verifizierung von Nachrichten und Daten wichtig sind. Würde dieser Aspekt ignoriert, wären Bitcoin lediglich signierte Zahlen ohne Wert.

Literaturverzeichnis

[Al14] Alex Biryukov and Dmitry Khovratovich and Ivan Pustogarov: Deanonymisation of clients in Bitcoin P2P network. CoRR, abs/1405.7418, 2014.

[Bl14] Blockchain.info: , Bitcoin currency statistics, April 2014. Accessed: 2014-04-05.

[Bo15] Bonneau, Joseph; Miller, Andrew; Clark, Jeremy; Narayanan, Arvind; Kroll, Joshua A; Felten, Edward W: SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015.

[BP14] Biryukov, Alex; Pustogarov, Ivan: Bitcoin over Tor isn't a good idea. arXiv preprint arXiv:1410.6079, 2014.

[Es15] Eskandari, Shayan; Barrera, David; Stobert, Elizabeth; Clark, Jeremy: A first look at the usability of bitcoin key management. In: Workshop on Usable Security (USEC). 2015.

[Ga05] Garfinkel, Simson L; Margrave, David; Schiller, Jeffrey I; Nordlander, Erik; Miller, Robert C: How to make secure email easier to use. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, S. 701–710, 2005.

[Ge] Gervais, Arthur; Ritzdorf, Hubert; Karame, Ghassan O; Capkun, Srdjan: Tampering with the delivery of blocks and transactions in bitcoin. Bericht, Cryptology ePrint Archive, Report 2015/578, 2015. http://eprint. iacr. org.

[GFFK06] Gaw, Shirley; Felten, Edward W; Fernandez-Kelly, Patricia: Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In: Proceedings of the SIGCHI conference on human factors in computing systems. ACM, S. 591–600, 2006.

[GKL15] Garay, Juan; Kiayias, Aggelos; Leonardos, Nikos: The bitcoin backbone protocol: Analysis and applications. In: Advances in Cryptology-EUROCRYPT 2015, S. 281–310. Springer, 2015.

[GM05] Garfinkel, Simson L; Miller, Robert C: Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In: Proceedings of the 2005 symposium on Usable privacy and security. ACM, S. 13–24, 2005.

[Go] Goldfeder, Steven; Gennaro, Rosario; Kalodner, Harry; Bonneau, Joseph; Kroll, Joshua; Felten, Edward W.; Narayanan, Arvind: , Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. Accessed 2015-06-09.

[He15] Heilman, Ethan; Kendler, Alison; Zohar, Aviv; Goldberg, Sharon: Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In: 24th USENIX Security Symposium (USENIX Security 15). USENIX Association, Washington, D.C., S. 129–144, August 2015.

[Sh06] Sheng, Steve; Broderick, Levi; Koranda, Colleen Alison; Hyland, Jeremy J: Why johnny still can't encrypt: evaluating the usability of email encryption software. In: Symposium On Usable Privacy and Security. 2006.

[Wh94] Wharton, Cathleen; Rieman, John; Lewis, Clayton; Polson, Peter: The cognitive walkthrough method: A practitioner's guide. In: Usability inspection methods. John Wiley & Sons, Inc., S. 105–140, 1994.

[WT99] Whitten, Alma; Tygar, J Doug: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Usenix Security. Jgg. 1999, 1999.