ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Institut für Informatik und Gesellschaft – Abteilung Telematik
Prof. Dr. Dr. h.c. Günter Müller

Seminar Wirtschaftswissenschaften
Digitale Währungen, Risiko & Privacy
Wintersemester 2014/15

Zentrale Daten im Überblick

Anmelde-Zeitraum: 31. Juli – 12. Oktober 2014

Bekanntgabe Zulassung: 13. Oktober 2014

Einführungsveranstaltung: Mo, 20. Oktober 2014, 16:00-17:00, IIG 5.OG, Raum 5003

Zuteilung der Themen: 24. Oktober 2014

Abgabe der Seminararbeiten: 23. Januar 2015, 12:00 Uhr

Präsentations-Termine: Voraussichtlich Woche vom 02. Februar 2015 (genaue Daten werden noch bekanntgegeben)

Hinweis: Bitte beachten Sie, dass bei der Einführungs-Veranstaltung und den Präsentationsterminen eine **Anwesenheitspflicht** besteht.

Allgemeine Informationen

- Das Seminar ist eine **Vorbereitung auf die Erstellung einer Masterarbeit**.
- Die Seminararbeit wird als Einzelarbeit angefertigt.
- Bei erfolgreicher Teilnahme können durch das Seminar **6 ECTS** (in englischer oder deutscher Sprache) erworben werden.

Anmeldung zum Seminar

- Die Anmeldung zum Seminar erfolgt **im Zeitraum vom 31. Juli - 12. Oktober 2014** durch eine Bewerbung **per E-Mail** und ist verbindlich. Spätere Anmeldungen können leider nicht berücksichtigt werden.
- Zur Anmeldung sind bitte die folgenden **Unterlagen** einzureichen:
  - Vordiplomszeugnis bzw. Bachelor-Abschlusszeugnis
  - alle bisherigen Noten im Rahmen des Masterstudiums
  - Lebenslauf *(optional)*
- Des Weiteren benötigen wir die folgenden **weiteren Informationen** von Ihnen:
  - Ihre Matrikelnummer
  - Ihre RZ-Kennung (bsp. XY1234)
  - eine kurze Angabe Ihrer Motivation zur Teilnahme an dem Seminar
- Bitte senden Sie Ihre digitale Bewerbung zu Händen von Prof. Müller und bitte **ausschließlich** an die folgende E-Mail-Adresse: **seminar2014@iig.uni-freiburg.de**
  (Wenn möglich, senden Sie uns Ihre Bewerbung bitte in einem Dokument und nicht in vielen Einzeldokumenten).
- Sie erhalten eine **Eingangsbestätigung** bzgl. des Erhalts Ihrer Unterlagen.

Ablauf und Betreuung

- Die Bekanntgabe über die Zulassung erfolgt per E-Mail **am 13. Oktober 2014**.
- **In der ersten** Vorlesungswoche im Wintersemester 2014/15 findet eine **Einführungsveranstaltung** statt. Die Seminarteilnehmer sind verpflichtet, hieran teilzunehmen. Im Rahmen der Veranstaltung werden die Erwartungen an die Seminararbeit kommuniziert, Tipps und Hinweise zur Erstellung der Seminararbeit gegeben und die Themen vorgestellt.
- Während der Einführungsveranstaltung geben die Seminarteilnehmer (bis zu drei) Präferenzen bezüglich ihres gewünschten Themas ab. Die Mittelung der Themenzuordnung erfolgt per E-Mail, woraufhin sich die Studenten an die zugeteilten Betreuer am Lehrstuhl wenden und ein Literatur-Startpaket erhalten.
- Zum **Bestehen des Seminars** sind das Anfertigen einer Seminararbeit (**6-8 Seiten** bei Nutzung der Lehrstuhl-Vorlage), einer Präsentation der Seminararbeit, sowie die Teilnahme an den Präsentationen der anderen Teilnehmer erforderlich. Die Note für die Seminararbeit geht mit 70%, die Note für die Präsentation geht mit 30% in die Gesamtnote für das Seminar ein. Als Mindestnote muss jede Leistung mit der Note "ausreichend" (= 4,0) bewertet sein.
- Die **Abgabe** der Seminararbeiten muss bis zum **23. Januar 2015, 12:00 Uhr,** erfolgen.
- Die Seminararbeit ist beim Sekretariat des Lehrstuhls in **doppelter** schriftlicher Ausfertigung abzugeben.
- Zusätzlich ist eine digitale Version Ihrer Arbeit als *Word*- oder *LaTeX*-Datei **auf einer CD** abzugeben.
- Die **Präsentation** der Arbeiten erfolgt im Rahmen von **Blockveranstaltungen in der Woche vom 02. Februar 2015.** die Zeitblöcke werden in der Einführungs-Veranstaltung bekanntgegeben.
- Bei diesen Blockveranstaltungen gilt für alle Teilnehmer **Anwesenheitspflicht**. Jeder Teilnehmer hat 20 Minuten Zeit, seine Seminararbeit zu präsentieren, hinzu kommen jeweils 10 Minuten der Diskussion.
- Die digitale Version der Präsentationen ist bis spätestens zwei Tage vor der ersten Seminarpräsentation an seminar2014@iig.uni-freiburg.de zu senden.
- Sollten sich Änderungen an dem genannten Ablauf ergeben, erhalten Sie diese rechtzeitig per E-Mail.
- Richtlinien für die Erstellung von Seminararbeiten sind über ILIAS erhältlich.

Formalia zur Ausarbeitung

- Arbeiten sollten grundsätzlich gut lesbar und übersichtlich strukturiert sein.
- Die schriftliche Ausarbeitung muss in *LaTeX* und unter Verwendung von *BibTeX* erfolgen. Um eine einheitliche Form der Arbeiten zu gewährleisten, ist die Verwendung des ACM-Templates vorgeschrieben, welches Ihnen auf ILIAS zum Download bereitgestellt wird. Abzuliefern ist ein PDF-Dokument sowie die zugehörigen Quelldateien.
- Abbildungen müssen lesbar und beschriftet sein.
- Das Deckblatt ist mit dem Namen der Universität, dem Vermerk "Vorgelegt bei Prof. Dr. Dr. h.c. Günter Müller" gefolgt vom Institutsnamen nebst Anschrift sowie der Bezeichnung "Seminararbeit" zu versehen. Außer dem Titel der Arbeit muss weiter der Name des Verfassers, dessen postalische und elektronische Anschrift und Matrikelnummer sowie die Anzahl der Fachsemester und der Abgabetermin aufgeführt werden.

Themen/Seminar-Beschreibung

Das Seminar versetzt die Studierenden in die Situation sich mit wirtschaftsinformatischen Problemen differenziert auseinander setzen zu müssen.

Spätestens seit den enormen Kurssprüngen der Bitcoins sind digitale Währungen nicht länger nur technologiebegeisterten Internetznutzern ein Begriff. Die einen sehen digitales Bargeld als das Zahlungsmittel der Zukunft. Unterstützung erfahren die Anhänger dieser These unter anderem dadurch, dass mittlerweile sogar schon Unternehmen wie Dell Bitcoins akzeptieren. Gleichzeitig werden virtuelle Währungen jedoch auch mit Strafdelikten wie Steuerbetrug, Geldwäsche und Drogengeschäften in Verbindung gebracht. Das Seminar widmet sich zum einen den ökonomischen Implikationen digitaler Währungen. Ferner soll der Frage nachgegangen werden, welche Risiken und Auswirkungen auf die Privacy mit ihrer Einführung einhergehen.

Das Seminar umfasst die **folgenden Themenkomplexe.** Während der Einführungsveranstaltung werden die konkreten Themenstellungen vorgestellt, auf die Sie sich dann bewerben können (bei der Angabe der Themenwünsche bitte maximal *drei Themen* nach Präferenz zuordnen):

Themenblock: Risiken digitaler Währungen

Die herausragenden Eigenschaften digitaler Währungen sind ihre Dezentralität und eine zumindest theoretisch sichergestellte Anonymität der Transaktionspartner. Daraus resultiert jedoch gleichzeitig eine Vielzahl an neuen Herausforderungen. Digitale Währungen unterliegen keinerlei Kontrolle durch zentrale Instanzen, was sie zu hochspekulativen Finanzinstrumenten macht. Die Anonymität schafft außerdem ein besonderes Interesse organisierter Kriminalitätsformen zur Verschleierung illegaler Transaktionen. Der Themenblock untersucht die mit zunehmender Verbreitung digitaler Währungen verbundenen Risiken und deren ökonomische Implikationen.

1) Disintermediation und Transaktionskosten

Motiviert wird die Vision hinter digitalen Währungen durch die Möglichkeit des vollständigen Verzichts auf Intermediäre (z.B. Kreditkartenanbieter, Paypal) die als vertrauenswürdige Dritte bei Online-Transaktionen auftreten. Ökonomisch wird das mit dem Argument geringerer Transaktionskosten der direkten Zahlungsabwicklung begründet.

Diese Aussage gilt es mit besonderem Fokus auf die Transaktionsphasen zu analysieren. Insbesondere ist in diesem Kontext der Beitrag von Intermediären zur Risikominderung einzubeziehen.

Empfohlene Einstiegsliteratur:

Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System.

Jaag, C.; Bach, C. (2014): The Effect of Payment Reversibility on E-commerce and Postal Quality. Swiss Economics Working Paper 0046. Online verfügbar unter http://www.swiss-economics.ch/RePEc/files/0046JaagBach.pdf.

Becker, Jörg; Breuker, Dominic; Heide, Tobias; Holler, Justus; Rauer, Hans Peter; Böhme, Rainer (2013): Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. In: Rainer Böhme (Hg.): The Economics of Information Security and Privacy. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 135–156.

2) Ausgestaltung regulatorischer Rahmenbedingungen

Ein Risiko digitaler Währungen ist in den vorherrschenden Unsicherheiten ihres regulatorischen Umfelds begründet. Es fehlt bisher an verbindlichen Regelungen bezüglich essentieller Bereiche wie der Besteuerung, des Rechnungswesens sowie der Bekämpfung von Geldwäsche. Aber nur durch klare Vorschriften kann die Stabilität und das Vertrauen gesteigert werden, was gleichzeitig für Akzeptanz sorgt.

Ziel der Arbeit ist herauszuarbeiten, welche Ansätze von Regulatoren unterschiedlicher Staaten für den Umgang mit digitalen Währungen verfolgt werden. Wenn Inkonsistenzen vorliegen gilt es diese zu analysieren.

Empfohlene Einstiegsliteratur:

Brito, J.; Castillo, A. (2013): Bitcoin: A Primer for Policymakers. Mercatus Center - George Mason University.

ECB (2012): Virtual currency schemes. Frankfurt-on-Main: European Central Bank.

Descôteaux, D. (2014): How should Bitcoin be regulated? Montreal Economic Institute.

3) Technische Risiken - Cyberangriffe

Häufig werden Sicherheitsbedenken bezüglich der zugrundeliegenden Technologie digitaler Währungen ins Feld geführt. Die Angriffe von Hackern auf die Wechselbörse Mt. Gox, welche zum Verlust erheblicher Guthabenbeträge geführt haben, verdeutlichen das Risiko durch Cyberattacken. Erschwerend kommt hinzu, dass einmal getätigte Transaktionen unwiderruflich und verlorene Wallets nicht wiederherstellbar sind.

Ziel der Arbeit ist es die Schwachstellen digitaler Währungen zu identifizieren. Welche Methoden, Mechanismen und Instrumente existieren für den Umgang mit diesen Verwundbarkeiten?

Empfohlene Einstiegsliteratur:

Kroll, J.A.; Davey, I.C.; Felten, E.W. (2013): The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In: The Twelfth Workshop on the Economics of Information Security (WEIS 2013). Washington, DC, June 11-12, 2013.

Hutchison, David; Kanade, Takeo; Kittler, Josef; Kleinberg, Jon M.; Mattern, Friedemann; Mitchell, John C. et al. (Hg.) (2012): Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science).

4) Stabilität und finanzielle Risiken

Die Kurse digitaler Währungen sind gegenwärtig starken Schwankungen unterworfen. Der Wechselkurs für Bitcoins stieg von 100$ auf über 1.200$ an seinem Höchststand im Dezember 2013 und bewegt sich derzeit um die 400$. Das legt die Vermutung nahe, dass solche Währungen derzeit eher als Spekulationsobjekt denn als Zahlungsmittel genutzt werden.

Zur Bearbeitung der Themenstellung sollen Faktoren für die starke Volatilität digitaler Währungen identifiziert werden. Weiterhin ist zu analysieren, inwiefern sich digitale Währungen bezüglich verfügbarer Mechanismen zur Sicherstellung der Preisstabilität von staatlichen Währungssystemen unterscheiden und welche Implikationen sich daraus für deren Akzeptanz als Zahlungsmittel ergeben.

Empfohlene Einstiegsliteratur:

Goldman Sachs (2014): All about bitcoin. Issue 21. Hg. v. Goldman Sachs Global Investment Research. Online verfügbar unter http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf.

Brezo, F.; Bringas, P. G. (2012): Issues and Risks Associated with Cryptocurrencies such as Bitcoin. In: Lasse Berntzen und Petre Dini (Hg.): SOTICS 2012. The second international conference on social eco-informatics, october 21-26, Venice, Italy. [S. l.]: IARIA, S. 20–26.

Kristoufek, L. (2014): What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis. Online verfügbar unter http://arxiv.org/pdf/1406.0268v1.pdf.

5) Terrorismusfinanzierung & Geldwäsche

Es ist unstrittig dass kriminelle Organisationen elektronische Bezahlsysteme und digitale Währungen zur Geldwäsche und Terrorismusfinanzierung nutzen. Die Besonderheit digitaler Währungen die auf kryptografischen Verfahren basieren ist jedoch, dass keine einfache Möglichkeit zur Identifikation von Nutzern sowie verdächtiger Transaktionen existiert.

In einem ersten Schritt soll daher herausgearbeitet werden, welche Mechanismen und Instrumente zur Aufdeckung von Geldwäsche existieren. Im zweiten Schritt ist zu analysieren, ob bzw. inwiefern sich diese Mechanismen und Instrumente auf digitale Kryptowährungen übertragen lassen. Außerdem sind eigene Lösungsvorschläge einzubringen.

Empfohlene Einstiegsliteratur:

Villasenor, J.; Monk, C.; Bronk, C. (2011): Shadow Figures: Tracking Illicit Financial Transactions in the Murky Word of Digital Correncies, Peer-to-Peer Networks, and Mobile Device Payments. Online verfügbar unter http://bakerinstitute.org/media/files/Research/d9048418/ITP-pub-FinancialTransactions-082911.pdf.

Moser, Malte; Bohme, Rainer; Breuker, Dominic: An inquiry into money laundering tools in the Bitcoin ecosystem. In: 2013 eCrime Researchers Summit (eCRS). San Francisco, CA, USA, S. 1–14.

Themenblock: Privacy-Aspekte digitaler Währungen

In der öffentlichen Berichterstattung werden digitale Währungen als anonym beschrieben. Ein erster Blick bestätigt diese Vermutung, da zur Teilnahme keine persönlichen Daten der Nutzer erhoben werden und Transaktionen nur zwischen vorher erstellten Adressen stattfinden. Durch die technisch bedingte Veröffentlichung jeder Transaktion an alle Teilnehmer ermöglichen digitale Währungen allerdings die totale Rückverfolgbarkeit von Zahlungsströmen. Wenn nun beim Kauf von Waren oder Dienstleistungen offengelegte persönliche Daten mit den in der Transaktionshistorie zugänglichen Adressen in Verbindung gebracht werden können, lassen sich dadurch einzelne Nutzer und ihre Transaktionen identifizieren. Daraus ergeben sich ganz neue Problematiken im Sinne der Privacy.

6) Deanonymisierung und Manipulation

Bitcoin wird nicht zuletzt aufgrund der angeblichen Anonymität bei Zahlungsvorgängen im Vergleich zu Banküberweisungen und Kreditkartenzahlungen angepriesen. Diese Anonymität wird jedoch nur dadurch gewährleistet, dass sich hinter einem Zahlungsvorgang eine anonyme Bitcoin Wallet anstatt eines vollen Namens verbirgt. Allerdings wird von immer neue Methoden berichtet, die es möglich machen über verschiedene Angriffswege Muster zu entschlüsseln welche IP Adresse sich hinter welcher Bitcoin Wallet verbirgt und mittels gezielter Attacken auf Rechner-Pools Transaktionen zu manipulieren.

Ziel dieser Seminararbeit soll es sein eine erklärende Übersicht über die entsprechenden Methoden zur Deanonymisierung der Bitcoin Zahlungsströme und deren Manipulation zu erstellen, sowie diese entsprechend ihrer Vorgehensweisen zu kategorisieren. In einem zweiten Schritt soll analysiert werden, welche ökonomischen Einflüsse solcherlei Attacken auf die digitale Währung hatten und das bestehende Risiko weiterer Attacken hat.

Empfohlene Einstiegsliteratur:

Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in Bitcoin P2P network. *arXiv preprint arXiv:1405.7418*.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. In *Financial Cryptography and Data Security* (pp. 34-51). Springer Berlin Heidelberg.

Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). Springer New York.

7) Bitcoin Blockchain & Big Data

Mit jeder Bitcoin Transaktion wird die alle bisherigen Transaktionen umfassende Blockchain errechnet. Unter der Verwendung weiterer Informationsquellen, wie z.B. Sozialen Online Netzwerken oder Kommentaren auf Bewertungsportalen und Shopsystemen, besteht die Gefahr, dass Bitcoin Wallets einzelnen Personen zugeordnet werden können und ihr Kaufverhalten so analysiert werden kann.

Ziel der Arbeit soll es sein die Vorgehensweise dieser Art der Client Deanonymisierung zu erklären und in einem zweiten Schritt zu erläutern, welche weiteren Privacy Risiken sich für die User ergeben, wenn große Kommerzielle Anbieter wie eBay oder Amazon in Zukunft Käufe via Bitcoin erlauben und welche ökonomischen Risiken und Anreize bei den Unternehmen bzgl. der Einbindung des Bitcoin-Systems bestehen.

Empfohlene Einstiegsliteratur:

Sorge, C., & Krohn-Grimberghe, A. (2012). Bitcoin: Eine erste Einordnung. *Datenschutz und Datensicherheit-DuD*, *36*(7), 479-484.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. In *Financial Cryptography and Data Security* (pp. 34-51). Springer Berlin Heidelberg.

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In *Financial Cryptography and Data Security* (pp. 6-24). Springer Berlin Heidelberg.

8) Gewährleistung von Privacy

Aufgrund der bereits beschriebenen Risiken zur Deanonymisierung von Bitcoin-Clients gibt es inzwischen zahlreiche Dienste und Methoden um die Privacy bei der Nutzung von Bitcoin zu sichern.

Das Ziel dieser Seminararbeit ist es eine Übersicht über diese Dienste und Hilfsmittel zu erstellen, sie entsprechend ihrer Funktionsweise zu kategorisieren und ihre Schwächen und Stärken herauszuarbeiten. Dabei soll auch miteinbezogen werden, welche Anreize bestehen auf Privacy sichernde Hilfsmittel zurückzugreifen und welchen ökonomischen Einfluss sie auf das Bitcoin-System und dessen Nutzung haben.

Empfohlene Einstiegsliteratur:

Ober, M., Katzenbeisser, S., & Hamacher, K. (2013). Structure and anonymity of the bitcoin transaction graph. *Future internet*, *5*(2), 237-250.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on* (pp. 397-411). IEEE.

Möser, M. (2013). Anonymity of Bitcoin Transactions. In *Münster Bitcoin Conference*.