Cryptocurrencies and Blockchain: Promise and Challenges

Master Seminar WS2019

Peter Hamm, M.Sc.

(Frédéric Tronnier, M.Sc.)

Chair of Mobile Business & Multilateral Security

Goethe University Frankfurt

mobile business

Agenda

I. Organization
II. Grading and Formal Rules
III. Expectations and Support
IV. Introduction to Blockchain and CC
V. Topics
VI. Distribution of Topics

Frédéric Tronnier

Education

- M.Sc. Business and Information Systems
- B.Sc. Economics and Business Administration
- Worked in VC and Start-Ups

Research Interests:

- Cryptocurrencies
- Behavioural Finance
- Security and Privacy in Distributed Ledger Technology

Frédéric Tronnier

Master Thesis:
"The Initial Coin Offering (ICO) as an investment opportunity - Empirical study on the investment behaviour of retail investors in ICOs of crypto assets„

Topic:

- Behavioral finance
- Initial Coin Offering → no research being done before

Results:

- First association of behavioral biases and ICO investors
- Unique set of personality traits in investors

I. Organization

- Registration
  - Signing will be done after distribution of topics
  - After today, resignation leads to a fail of the whole seminar

I. Organization

- Contact
  - All questions to peter.hamm@m-chair.de
  - You will always get a personal appointment ASAP, since a regular exchange is important for a very good work (arranged by mail)
  - All relevant information will be published on www.m-chair.de

I. Organization

Date	What	Where/How
28.10.2019	Introduction and Distribution of Topics	RuW 2.202
13.01.2020	Seminar paper submission	Sekretariat, RuW 2.257 **and** digitally via e-mail
14.01.2020	Presentation submission	E-mail
15.01.2019	Presentations (Day 1)	RuW 2.202
- 17.01.2019	Presentations (Day 2-3)	RuW 2.202

- Agenda will be sent to all participants prior to the presentation days.

II. Grading and Formal Rules

- Course assessment
  - Based on your seminar paper (60%) and presentation (40%) (+ discussion)
  - Each partial requirement needs to be passed with a grade of 4.0 or better

II. Grading and Formal Rules

- Seminar paper
  - Either alone, in groups of 2-3
  - ~20 pages (for two)
  - Use the template on https://m-chair.de/index.php/teaching/theses, but with citations formatted with the APA style
    - (Tipp: Use Mendeley for citation)
- Deadline for submission: 13.01.2020
  - Provide the printed version to Elvira Koch, RuW 2.257
  - Send the digital version to peter.hamm@m-chair.de

II. Grading and Formal Rules

- Seminar presentation:
  - Duration: 15 min. at most
  - Following discussion: 15 min.
- Submission until 14.01.2020
  - Powerpoint format
  - E-mail to peter.hamm@m-chair.de

III. Expectations and Support

- We expect from you:
  - Motivation, dedication and rigor when working on your seminar
  - Engage in discussions when preparing your paper and especially during the presentations days
  - Ask questions and be curious
  - Understand the used methodology and try to become an expert for it

III. Expectations and Support

- How we want to support you:
  - Opportunity to exchange ideas on a regular basis
  - Honest feedback and strong interest in your work
  - Possibility to publish it in the future together

III. Expectations and Support

- Workshops
  1. How to conduct a literature review
  2. How to present
  3. How to structure a paper

  →Workshops outline important concepts and guidelines and provide a first insight to the topic, **without** claiming to be exhaustive

  →Will all be done today and are **optional**

IV. Introduction to Cryptocurrencies and Blockchain

- Blockchain:

  “... shared, trusted, public ledger of transactions, that everyone can inspect but which no single user controls.” ("What is Blockchain?", n.d.)

  - Can be used for more than cryptocurrency
  - Main technologies behind it: *Distributed network, Advanced cryptography, Data architecture, Decentralized consensus*

- Cryptocurrency: Definition by Oxford Dictionary

  „... digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.“

IV. Introduction to Cryptocurrencies and Blockchain

Results of a Systematic Literature Review on CC in IS research (Tronnier, tbd)
→ shows promising research gaps to investigate in future work →

	Journal / Conference	Search	Coverage	Hits	Final Hits
1	ISR	"anywhere"	since 2017	3	1
2	MISQ	"all fields"	-	0	0
3	JMIS	"all fields"	since 2016	13	2
4	JAIS	"all fields"	since 2018	3	0
5	JIT	"all fields"	since 2017	1	0
6	ISJ	"all fields"	since 2018	5	1
7	JSIS	"all fields"	since 2019	1	0
8	EJIS	"all fields"	since 2017	1	0
9	CACM	"any field"	since 2016	14	8
10	CSUR	„all fields“	since 2018	1	1
11	Decision Sciences	"all fields"	since 2019	1	0
12	Decision Support Systems	"all fields"	since 2017	3	3
13	AMCIS	"all fields"	Since 2015	69	11
14	ECIS	"all fields"	Since 2014	45	13
15	HICSS	"all fields"	Since 2014	28	4
16	ICIS	"all fields"	Since 2014	46	16
17	PACIS	"all fields"	--	9	2
18	Backward Search	--		--	275
19	Total	--		243	62
20	**Total incl. Backward Search**				**337**

V. Topics

- Can be roughly divided by methodologies used and naturally by topics
  - Literature reviews
  - Quantitative research
  - Qualitative research

Literature Reviews – Topic 1

- The modern cryptocurrency ecosystem involves a magnitude of actors with complex interrelationships, from miners, over exchanges to end users.
- Create an overview over the current ecosystem, it's actors and mechanisms.
  - Böhme, R., Christin, N., Edelman, B. and Moore, T., 2015. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), pp.213-38.

Literature Reviews – Topic 2

- Blockchain has found use cases in industries beyond currencies, be it solutions for supply chain management, financial services or IT.
- Create an overview over current uses of distributed ledger technologies, as well as the characteristics of the deployed blockchains (like public vs. permissioned).
  - Glaser, F., 2017. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Literature Reviews – Topic 3

- Smart Contracts offer the implementation and automatic execution of code on a blockchain.
- Create an overview over smart contracts and their uses, including a short introduction into the Ethereum Virtual Machine.
  - Bartoletti, M. and Pompianu, L., 2017, April. An empirical analysis of smart contracts: platforms, applications, and design patterns. In *International conference on financial cryptography and data security* (pp. 494-509). Springer, Cham.

Literature Reviews – Topic 4

- Bitcoin and most cryptocurrencies rely on proof of work (PoW) to ensure consensus and protect against attacks. However, potential attacks and scalability challenges have led to the exploration of alternative mechanisms such as proof-of-stake.
- How do these procedures aim to fix perceived issues with PoW while offering similar benefits?
  - Eyal, I. and Sirer, E.G., 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), pp.95-102.
  - Kiayias, A., Russell, A., David, B. and Oliynykov, R., 2017, August. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual International Cryptology Conference* (pp. 357-388). Springer, Cham.

Literature Reviews – Topic 5

- The regulatory landscape for cryptocurrencies and cryptotokens is constantly shifting, be it in the question whether tokens are financial securities of whether an immutable blockchain is compatible with the “right to be forgotten” established by the General Data Protection Regulation.
- Create an overview over the current regulatory environment.
  - Guadamuz, Andres, and Christopher Marsden. "Blockchains and Bitcoin: Regulatory responses to cryptocurrencies." *First Monday* 20.12-7 (2015).
  - De Filippi, P., 2014. Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review*, *3*(2).

Literature Reviews – Topic 6

- The rise and fall of the Silk Road marketplace highlighted the popularity of using bitcoin for black market activity due to it’s perceived anonymity compared to other electronic currencies and greater convenience over cash.
- What is the current state of research into the use of cryptocurrencies for illicit activities?
  - Kethineni, S., Cao, Y. and Dodge, C., 2018. Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American Journal of Criminal Justice*, *43*(2), pp.141-157.
  - Slattery, T., 2014. Taking a bit out of crime: Bitcoin and cross-border tax evasion. *Brook. J. Int'l L.*, *39*, p.829.

Literature Reviews – Topic 7

- One of the initial pulls of Bitcoin as well as it’s predecessors was anonymity & privacy. While pseudonymity enables users to hide their identity behind addresses, analyses of the transaction graph have shown information leakages that may lead to the unintended unmasking of users.
- Discuss the privacy-protecting mechanisms implemented into Bitcoin and other cryptocurrencies, such as Zerocash.
  - Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T. and Capkun, S., 2013, April. Evaluating user privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 34-51). Springer, Berlin, Heidelberg.
  - Ron, D. and Shamir, A., 2013, April. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security* (pp. 6-24). Springer, Berlin, Heidelberg.

Literature Reviews – Topic 8

- The correctness and stability of Bitcoin is heavily dependent on the mining process. Recent research has looked at this process through the lens of game theory and discussed attacks and potential incentive-incompatibilities.
- Give an overview over the current state of game theoretical discussions of the mining process.
  - Eyal, I. and Sirer, E.G., 2018. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), pp.95-102.
  - Kroll, J.A., Davey, I.C. and Felten, E.W., 2013, June. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS* (Vol. 2013, p. 11).

Quantitative Research – Topic 9

- Since exploding in valuation and market cap in 2017, bitcoin has made headways in the financial industry as an asset, with the CME trading BTC futures and planning to introduce options.
- What are the characteristics of Bitcoin as an asset class, in terms of risk-return spectrum and cross-correlation with other asset classes?
  - Baur, D.G., Hong, K. and Lee, A.D., 2018. Bitcoin: Medium of exchange or speculative assets?. *Journal of International Financial Markets, Institutions and Money, 54*, pp.177-189.
  - Wu, C.Y. and Pandey, V.K., 2014. The value of Bitcoin in enhancing the efficiency of an investor's portfolio. *Journal of financial planning, 27*(9), pp.44-52.

Qualitative Research – Topic 10

- While most research focuses on technical aspects, there is a growing body of work on the "client side" of the equation. Who buys cryptocurrencies, and why?
- Create a literature review on the characteristics of cryptocurrency users, OR design a questionnaire and conduct a user study focusing on new facets such as the decision making style of crypto investors.
  - Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C. and Siering, M., 2014. Bitcoin-asset or currency? revealing users' hidden intentions. *Revealing Users' Hidden Intentions (April 15, 2014). ECIS*.
  - Yelowitz, A. and Wilson, M., 2015. Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, *22*(13), pp.1030-1036.

Topic 11+

- Do you already have own ideas?
- What areas are you interested in?

Topics

Number	Topic	Methodology	Name
1	CC ecosystem	Literature Review	
2	Blockchain technology and use cases	Literature Review	
3	Introduction to smart contracts	Literature Review	
4	PoW and alternative consensus mechanisms – technical/ economical	Literature Review	
5	GDPR and CC - legal / privacy	Literature Review	
6	Illicit activities with CC	Literature Review	
7	Privacy in CC - technical	Literature Review	
8	Mining – game theory	Literature Review	
9	BTC as an asset class – financial analysis	Quantitative	
10	CC user study - survey	Qualitative (Literature)	
11	? Own ideas ?		

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Peter Hamm
(Frédéric Tronnier)
Goethe University Frankfurt
E-Mail: peter.hamm@m-chair.de
WWW: www.m-chair.de