**The New Centre for Research and Practice**

# Disassembling the Trust Machine:

# An introduction to a political economy of blockchain

**Running August 19th – October 22nd 2018**

**By Jaya Klara Brekke**

## Week 1: Introduction to Disassembling the Trust Machine

We will begin the seminar series by carefully disassembling the components of the Bitcoin proof-of-work algorithm in order to get a first glimpse of the technical, economic and political concepts, techniques, assumptions and ethics that are mobilized in order to make the protocol work. The seminar introduces the core aspects of blockchain and cryptoeconomics from a radically interdisciplinary angle, and so is an essential introduction – for both newbies as well as those who are already working in the fields of, or familiar with, blockchain, cryptocurrencies and cryptoeconomics.

*In the seminar we will explore and discuss the following questions:*
How are blockchain and consensus algorithms "political"? How are they "economic"? What is cryptography? What is cryptoeconomics? What is *political* cryptoeconomics? How and why does blockchain address "trust"?

*Readings:*

Brekke, Jaya Klara. 2018. Disassembling the Truth Machine. In: de Vega, M. Mazon
    Gardoqui, V. & Silvestrin, D. */META. Tracing unknown kno//wns/.* ñ
    (Mexico City & Berlin)

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.*
    https://bitcoin.org/bitcoin.pdf.

Merkle, Ralph Charles. 1979. *Secrecy, Authentication and Public Key Systems.* Information
    Systems Laboratory.

## Week 2: Technology, politically

*Extrastatecraft* / *cyborg* / *stack* / *apparatus* / *assemblage* / *delegation* / *translation* / *automation* / *sedimentation*. These concepts are ways in which theorists have sought to relate and understand networks, infrastructure, technology and computation as existing within and as part of the social, political and natural world. Despite these efforts science and technology is still often understood as existing in an "objective" outside of the "subjective" messiness of human social and political life. In this seminar we will get familiar with conceptual tools that allow us to understand the nature of technology as part of the world. We will explore the techno-political implications of different conceptual understandings, in particular the work of Karen Barad, trying out the concepts on our case and discuss what they might have to offer for an understanding of blockchain and cryptoeconomics.

*In the seminar we will explore and discuss the following questions:*
In what ways is technology "political"? How is it "social" and "historical"? How do these explanations account for scientific objectivity? Why do some things, devices, protocols simply "work" and others not? What are the effects of difference conceptual understandings?

*Readings:*

*Set 1: (How) is it possible to know the politics of emergent, network systems?*

Amoore, L. (2016) 'Cloud geographies: computing, data, sovereignty.', Progress in human geography.

Bratton, Benjamin E. 2014. "The Black Stack." *E-Flux*. http://www.e-flux.com/journal/the-black-stack/.

Hayles, N. Katherine. 2010. "How We Became Posthuman: Ten Years On." *Paragraph* 33 (3): 318–30. https://doi.org/10.3366/E0264833410000933.

*Set 2: How do we understand science and technology as part of the social and political world?*

Barad, Karen. 2003. "Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter." *Signs: Journal of Women in Culture and Society* 28 (3): 801–31. https://doi.org/10.1086/345321 .

Edwards, Paul N. 2003. "Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems." In *Modernity and Technology*, edited by Thomas J. Misa, Philip Brey, and Andrew Feenberg, 185–225. Cambridge, MA: MIT Press.

Rogaway, Phillip. 2015. "The Moral Character of Cryptographic Work." *Asiacrypt 2015*, 48.

## Week 3: Blockchain, politically

The Bitcoin whitepaper was published just as the financial crisis began to ripple across the world, eventually turning into a sovereign debt crisis. For many, then, Bitcoin came to represent the possibility of a different kind of money and a different kind of economic system. The main proposition of Nakamoto's consensus algorithm (and most blockchain projects) is to solve the problem of authority and control through a trustless, decentralized protocol. This has led to several understandings of the potential of the technology, from the possibility of communities taking control over their own economic and monetary policies, developing a plethora of different protocols with visions of plural monetary eco-systems, to a "systems primacy" in which the problem of corrupt systems is considered solved by replacing human governance with what are considered a more neutral, unbiased and objective techno-economic means. In this seminar we will look at some of the critiques of debt-based money creation and fractional reserve banking that attracted people from across the political spectrum to Bitcoin and the potential of cryptocurrencies, and discuss some of the ways in which these hopes are sought realized. "Systems primacy" as a tendency will be discussed in relation to the problem of "primacy" more generally  - ways in which understandings of objectivity and subjectivity used in order to mobilize economic theory and mathematics as a deterministic and indisputable ground on which to build new techno-political systems.

*In the seminar we will explore and discuss the following questions:*

What were the main criticisms of fractional reserve banking and the financial system? Are "primacy" and "plurality" useful political distinctions to make sense of these critiques? How are markets and technology understood as objective and neutral? How are they not?

*Readings:*

*Set 1: What was the political economic climate and cultures that gave rise to Bitcoin?*

Anonymous. 2016. "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments." *De Gruyter Open*.

Hughes, Eric. 1993. "A Cypherpunk Manifesto." Activism.Net. 1993. https://www.activism.net/cypherpunk/manifesto.html.

Duran, Enric. Crisi. 2008 https://enricduran.cat/en/crise-2008pdf-in-english/

Golumbia, David. 2015. "Bitcoin as Politics: Distributed Right-Wing Extremism." In *An Intervention in Digital Economy*, eds. Geert Lovink, Nathaniel Tkacz, and Patricia De Vries. Amsterdam: Institute of Network Cultures.

*Set 2: What are some of the political economic assumptions encoded into blockchain and Bitcoin?*

Brekke, Jaya Klara. Forthcoming. *Systems primacy*.

Hayek, Friedrich August Von. 1945. "The Use of Knowledge in Society." *American Economic Review, XXXV* 4(September): 519–30. http://oll.libertyfund.org/title/92.

Scott, Brett. 2014. Visions of a Techno-Leviathan: The politics of the Bitcoin Blockchain. Available at: https://www.e-ir.info/2014/06/01/visions-of-a-techno-leviathan-the-politics-of-the-bitcoin-blockchain/

Wood, Gavin. 2014. "Ethereum: A Secure Decentralised Generalised Transaction Ledger."

# Week 4: Money, politically

*Visiting lecture by financial/ fintech author Brett Scott*

In this seminar we will take a closer look at the economic and monetary theories that are encoded and operationalized in cryptoeconomics – and the possibilities for and potential effects of incorporating heterodox economic theories into these systems. Author and financial activist Brett Scott will give an overview of some of the main economic and monetary assumptions that tend to be encoded in cryptocurrencies today. We will discuss their historical origin and the political and conceptual assumptions that they draw on. We will also look at projects that incorporate other economic ideas and discuss the possibilities and potential effects of these.

*In the seminar we will explore and discuss the following questions:*
How does cryptocurrencies have "value"? What are the monetary and economic assumptions encoded in blockchain? What scope is there for encoding different monetary ideas and values? Is it a mistake to understand cryptocurrencies as "money"?

Readings:

Innes, AM. 1914. "The Credit Theory of Money." *The Banking Law Journal* 31 (January): 151–68.

Innes, A. Mitchell. 1913. "What Is Money?" *The Banking Law Journal*, no. May: 22–51.

Gibson-Graham, J. K. 2008. "Diverse Economies: Performative Practices for ' Other Worlds .'" *Progress in Human Geography* 32(5): 613–32.

Scott, Brett. 2013. "Riches beyond Belief." *Aeon*. https://aeon.co/essays/so-you-want-to-invent-your-own-currency.

What, why and how Economic Space Agency
https://medium.com/new-economic-spaces/what-why-how-ecsa-60e95ee31324

Cryptocurrency and its discontents
https://www.e-flux.com/program/155336/economic-space-agency-presents-cryptocurrency-and-its-discontents/

## Week 5: Cryptoeconomic governance – tracing how things come to matter

In this seminar, the shifting understanding of what matters in blockchain will be discussed and explored. Encoding and enforcing a set of monetary and economic ideas through an immutable protocol was supposed to have made governance and politics obsolete. Only after deep-seated disputes about protocol changes, major hacks, exploits took place in the blockchain community did the governance of protocols come center-stage in the design of decentralized systems. We will discuss how code is written, deployed, governed and run in decentralized systems, and questions around what is considered important or not in that process.

*In the seminar we will explore and discuss the following questions:*
How are protocols governed in decentralized systems? Who gets to determine what and who is important and what matters in a decentralized system? What is considered to "not matter" and what are the effects of this?

*Readings:*

*Set 1: Forking as dissensus - how things come to matter in blockchain communities*

Wirdum, Aaron van. 2016. "On Consensus, or Why Bitcoin's Block-Size Presents a Political Trade-Off." *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/on-consensus-or-why-bitcoin-s-block-size-presents-a-political-trade-off-1452887468.

Wirdum, Aaron van. 2015.Segregated Witness, Part 3: How a Soft Fork Might Establish a Block-Size Truce (or Not) https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-soft-fork-might-establish-a-block-size-truce-or-not-1451423607/

Wirdum, Aaron van. 2017. The Long Road to SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality https://bitcoinmagazine.com/articles/long-road-segwit-how-bitcoins-

biggest-protocol-upgrade-became-reality/

Vollmer, Jan. 2016. The Biggest Hacker Whodunnit of the summer.
https://motherboard.vice.com/en_us/article/pgkzqm/the-biggest-hacker-whodunnit-of-the-summer

Zamfir, Vlad. 2016. The DAO Hard Fork, and the Negotiation that Couldn't Happen
https://medium.com/@Vlad_Zamfir/the-dao-hard-fork-and-the-negotiation-that-couldnt-happen-bdd2aedefe84

Ethereum EIP process, Github https://github.com/ethereum/EIPs

Ethereum Classic ECIP process, Github https://github.com/ethereumproject/ECIPs

*Set 2: Decentralized Governance?*

Azouvi, Sarah; Maller, Mary and Meiklejohn, Sarah "Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance," in *22nd International Conference on Financial Cryptography and Data Security*, March 2018.
Available: https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final13.pdf

Kreutler, Kei. 2018. The Byzantine Generalization Problem: Subtle strategy in the context of Blockchain Governance. https://technosphere-magazine.hkw.de/p/The-Byzantine-Generalization-Problem-Subtle-Strategy-in-the-Context-of-Blockchain-Governance-8UNNcM8VShTpBGWRuob1GP

Wirdum, Aaron van. 2016. "A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol." *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427/.

Zamfir, Vlad. Against on chain governance.
https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

Taaki, Amir. 2011. BIP Purpose and guidelines.
https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki

Luke Dashjr 2016. BIP2.
https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki#Rationale-3

Vitalik Buterin tweet storm about proof-of-stake, Ethereum Casper debates:
https://twitter.com/VitalikButerin/status/1029900695925706753

*General readings:*
Satoshi Oath
http://ipfs.b9lab.com:8080/ipfs/QmXysWEAexXQqYZhTGpECvksnaBkSEWHdGhM7vNeHxue2g/

Bitcoin developers mailing list https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev

## Week 6: Consensus algorithms politics and design

*Visiting lecture - Rachel Rose O'Leary, writer for CoinDesk*

The Bitcoin proof-of-work algorithm inspired the emerging interdisciplinary field of cryptoeconomics along with a plethora of new blockchain applications and consensus protocols. In this seminar, Rachel O'Leary will give an overview of consensus algorithms and the forms of disputes, governance issues and concerns that have given rise to them. We will discuss how different protocol designs give clues about what matters to the communities that have developed them – for example energy consumption, centralizing tendencies in mining, distribution of wealth, and how these implicitly point towards emerging political and ethical perspectives. And most importantly we will map out what matters in consensus algorithm design and the major implications of deciding what is or is not part of the design space.

*The seminar will address and discuss the following questions:*

What are the main consensus protocols? What main issues do they seek to address? What does this tell us about what matters to the communities that developed them? What is consensus protocol design? What are the limits to the design space?

*Readings:*

Political insight into cypherpunk and technical precursor to ethereum: Wei Dai, 'b-money,' 1998
http://www.weidai.com/bmoney.txt

Origins of proof-of-work: Adam Back, 'HashCash', 1998
http://www.hashcash.org/papers/hashcash.pdf

Cynthia Dwork and Moni Naor, Pricing via Processing or Combatting Junk Mail, 1992
http://www.wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf

Consequences of runaway economic growth in proof-of-work: David Vorick, 'The State of Cryptocurrency Mining,' 2018 https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b

Political origins of proof-of-stake: Vitalik Buterin, 'A Proof of Stake Design Philosophy,' 2018

https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

Vitalik Buterin, 'Slasher: A Punitive Proof-of-Stake Algorithm,' 2014

https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm/

Vitalik Buterin in conversation with Sunny King, 2013

https://talk.peercoin.net/t/transcript-of-sunny-king-interview-with-vitalik-buterin-from-bitcoinmagazine/463

Precious stones in cyberspace (bitcoin precursor): Nick Szabo, "Bit-gold," 2005
https://nakamotoinstitute.org/bit-gold/

Budish, Eric. 2018. "The Economic Limits of Bitcoin and the Blockchain."
https://doi.org/10.3386/w24717

Bano, Shehar et al. 2017. "Consensus in the Age of Blockchains."
http://arxiv.org/abs/1711.03936

# Week 7: Reconfiguring the digital, the physical, scarcity and abundance

Network culture, piracy, hacker ethics, cypherpunk, open source and the political history of peer-to-peer promoted ideas of digital space as making possible a politics of abundance, sharing and fluid identities. Blockchain technology, having emerged from these cultures, nevertheless seeks to establish scarcity in the digital realm, determine and secure private property, define identities, in many ways seeking to reproduce techniques of the state in new technical forms. In this seminar we will trace back the main principles in blockchain through the history of peer-to-peer, and look closer at concepts like decentralization, trustlessness, disintermediation, autonomy, privacy and transparency as they have shifted through the history of peer-to-peer and in particular in their interaction with economic theory in which property and the individual is the basis of a system and systems interactions.

*In the seminar we will explore and discuss the following questions:*
How and why did peer-to-peer culture and practice develop from a critique of digital scarcity and property to the creation of scarcity and security of property? And what are the effects of this? What are some of the design challenges and political contradictions in the field?

*Readings:*
Arvanitakis, James, and Martin Fredriksson. 2016. "Commons, Piracy, and the Crisis of Property." TripleC 14 (1): 132–44.
Coleman, Gabriella. 2009. "Code Is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers." Cultural Anthropology 24(3): 420–54.

Käll, Jannice. 2018. "Blockchain Control." Law and Critique 29(2): 133–40.
https://doi.org/10.1007/s10978-018-9227-x.

Oram. A. Peer-to-Peer: Harnessing the power of disruptive technologies. O'Reilly, 2001. (Section 2.5 pp26- 28)

Papadimitropoulos, Vangelis. 2018. "Reflections on the Contradictions of the Commons." Review of Radical Political Economics, 1–15. https://doi.org/10.1177/0486613417735660.

Söderberg, Johan, and Adel Daoud. 2012. "Atoms Want to Be Free Too! Expanding the Critique of intellectual Property to Physical Goods." TripleC 10 (1): 66–76.

Slock.it. 2016. UG proposal. "For a Universal Sharing Network, the Ethereum Computer Reference Design and Its Ecosystem of Applications."

## Week 8: Emerging political ideas

In this final seminar we will look at some of the emerging political and economic fractions in the space, seeking out contradictions and commonalities and strategic positioning. From futarchy to holocracy, open source/ commons based ideas these political economies will be explored in practice, as they are strategically deployed as function, promise, or strategy across different layers of "the stack". We will seek to disentangle political cryptoeconomics as it is practiced in three ways, namely the *operationalization* of political economic ideas for computational purposes; the political economic *promises* that are made about the function and applications of cryptoeconomic projects; and finally the *maneuvering* of existing political economic contexts in order to achieve strategic and practical goals. The aim of the final seminar will be to collectively articulate a field of political cryptoeconomics and articulate its main questions and scope.

*In the seminar we will explore and discuss the following questions:*
What are some of the new political economic ideas emerging in the space? What are the main political economic aims of cryptoeconomics? What should the field of political cryptoeconomics look like?

*Readings:*

*Set 1: "Futarchy" and new configurations of democracy and markets*

> Hanson, Robin. "Shall We Vote on Values, But Bet on Beliefs ? *.
> http://mason.gmu.edu/~rhanson/futarchy.pdf

> S. P. Lalley and E. G. Weyl, "Quadratic Voting," *Am. Econ. Assoc. Pap. Proc.*, vol. 1, no. 1, 2018. https://www.sss.ias.edu/files/pdfs/Rodrik/workshop%2014-15/Weyl-Quadratic_Voting.pdf

> V. Buterin, Z. Hitzig, and E. Glen Weyl, "Liberal Radicalism: Formal Rules for a Society Neutral among Communities *," no. September, pp. 1–41, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3243656

> Brekke, J. K. Three Postcards from the World of Decentralised Money. In: Gloerich, I., Lovink, G. & de Vries, P. *MoneyLab Reader#2: Overcoming the hype*. Institute of Network Cultures; 2018. http://networkcultures.org/wp-content/uploads/2018/01/06-jayaklarabrekke.pdf

*Set 2: "Current sees" and the sensibility of the political*

> Ulieru, By Mihaela. "Organic Governance Through the Logic of Holonic Systems." **[Pdf attached]**

> Interview with Arthur Brock from metacurrency project and Holo
> https://www.patreon.com/posts/19911963

Holochain whitepaper
https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf

Holo currency whitepaper
https://files.holo.host/2017/11/Holo-Currency-White-Paper_2017-11-28.pdf

J. K. Brekke, "The decentralization 'fix' and the persistence of the political," in *INSCI*, 2018, pp. 1–17. **[pdf attached]**

Thank you to all the students who participated and engaged with the seminar and the New Centre for Research and Practice, in particular Patrick Schabus and Mohammad Salemy for facilitation and the invitation to run the series.

Thank you also to Brett Scott and Rachel Rose O'Leary for generous presentations and discussions in sessions 4 and 6.

## Jaya Klara Brekke

Contact: j.k.brekke@durham.ac.uk

Website: http://distributingchains.info/

## The New Centre for Research and Practice

Contact: https://thenewcentre.org/connect/

Website: https://thenewcentre.org/