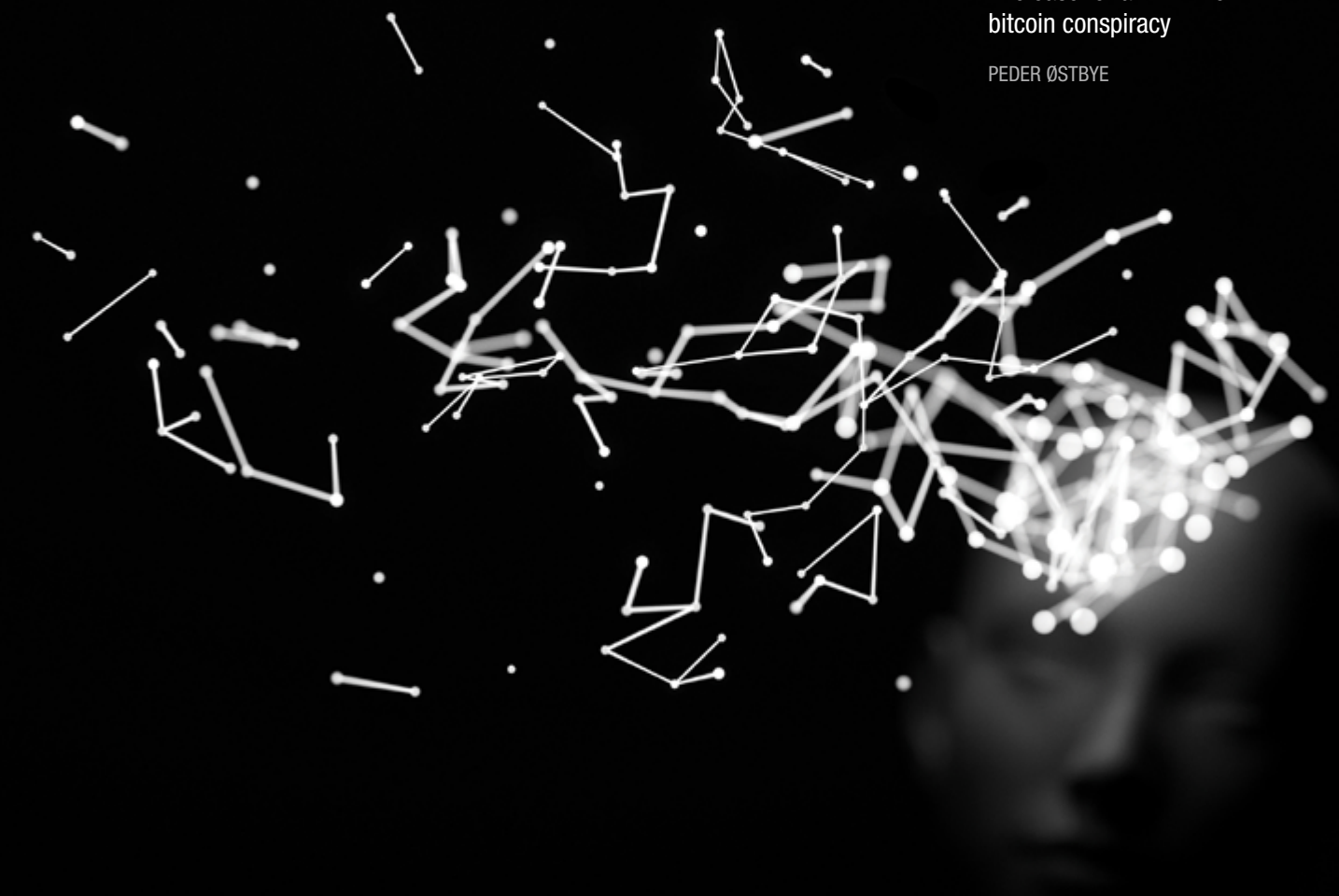
THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TRANSFORMATION

The case for a 21 million bitcoin conspiracy

PEDER ØSTBYE



DESIGN THINKING

#48 NOVEMBER 2018

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

DESIGN

TRANSFORMATION

SUPERVISION

DEAR READER,

Design thinking, a collaborative, human-focused approach to problem-solving, is no longer just for the creative industries. It has become an important management trend across many industries and has been embraced by many organizations. Its results are hard to ignore. Indeed, design-driven companies regularly outperform the S&P 500 by over 200 percent.[1]

To date, the financial services industry has not led in adopting this approach. However, leaders are recognizing that important challenges, such as engaging with millennial customers, can be best addressed by using design thinking, through the methodology's exploratory approach, human focus, and bias towards action. This edition of the Journal examines the value of design thinking in financial services.

Design thinking introduces a fundamental cultural shift that places people at the heart of problem-solving, which is critical in a technology-driven environment. If the customer's real problems are not fully understood, technological solutions may fail to deliver the desired impact. In this context, design thinking offers a faster and more effective approach to innovation and strategic transformation.

The case studies and success stores in this edition showcase the true value of design thinking in the real world, and how this approach is an essential competitive tool for firms looking to outperform their peers in an increasingly innovation-driven and customer-centric future. At Mastercard, design thinking has become a part of almost all organizational initiatives, from product development, research and employee engagement to solving challenges with customers and partners. Meanwhile, at DBS Bank in Singapore, a data-informed design model has been firmly embedded into the bank's culture, enabling them to successfully move from being ranked last among peers for customer service in 2009, to being named the Best Bank in the World by Global Finance in 2018.

I hope that you enjoy the quality of the expertise and points of view on offer in this edition, and I wish you every success for the remainder of the year.

Lance Levy, **Capco CEO**

[1] http://fortune.com/2017/08/31/the-design-value-index-shows-what-design-thinking-is-worth/

THE CASE FOR A 21 MILLION BITCOIN CONSPIRACY

PEDER ØSTBYE | Special Adviser, Norges Bank[1]

ABSTRACT

Bitcoin and many other cryptocurrencies have currency-caps implemented in their protocols. Bitcoin is capped at approximately 21 million bitcoins. These protocols are complied by consenting operators. This paper discusses whether such currency-caps are illegal quantity-fixing conspiracies in violation of antitrust law. It is found that there is a present antitrust risk for cryptocurrency operators. This may render such operators subject to criminal and civil liabilities.

1. INTRODUCTION

Bitcoin and many other cryptocurrencies have currency-caps implemented in their protocols. Bitcoin is capped at approximately 21 million bitcoins. This protocol is complied with by the decentralized operators in the creation of consensual distributed ledgers. In an antitrust sense, this sounds like some sort of cooperation that may be subject to antitrust liability. This paper examines whether the 21 million cap implemented in the bitcoin protocol and similar caps in other cryptocurrencies are illegal quantity-fixing conspiracies in violation of antitrust law. It is found that there is a present antitrust risk for block-validators and other stakeholders involved in cryptocurrencies. This may render such stakeholders subject to criminal and civil liabilities.

Over the last few years, there has been an explosion of legal and regulatory research into cryptocurrencies and the associated technology more generally. This ranges from general assessments, as provided by Chuen (2015), Tu and Meridith (2015), and Paech (2017), to more specialized assessments, such as the legal status of so-called initial coin offerings (ICOs) provided by Zetzsche et al. (2018). Much of the literature gravitates towards financial regulation. This paper shares topics with Zetzsche et al. (2017), which assess the liability of participants in a distributed ledger. Zetzsche et al. (2017) rebuts the claim that the operators of distributed ledgers are outside the reach of the law and regulators. This paper also shares topics with Østbye (2017), which discusses competition policy for the cryptocurrency markets in general, also emphasizing the possible liability of the operators. In this paper we will, however, explore the narrow issue of whether the currency caps in cryptocurrencies are antitrust conspiracies. To the author's knowledge, this is not well explored in the literature. To make an adequate assessment of this issue, it is necessary to delve into the "nuts and bolts" of cryptocurrencies as provided by, inter alia, Narayanan et al. (2016).

[1] This paper should not be reported as representing the views of Norges Bank. The views expressed are those of the author and do not necessarily reflect those of Norges Bank.

2. CRYPTOCURRENCY TECHNOLOGY AND THE ROLE OF CURRENCY-CAPS

Bitcoin was launched in 2009, but documentation was already available in 2008. The creator or creators of bitcoin are unknown to the general public. The bitcoin white paper, Nakamoto (2008), was written under the pseudonym Satoshi Nakamoto. The intention behind bitcoin expressed in the white paper is that "[w]hat is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party." As a disruptive innovation and from the perspective of competition, it is a welcome potential challenger to banks and other financial service providers.

Many of the cryptocurrencies introduced in the aftermath of bitcoin seek to improve upon its shortcomings. For instance, scale and increased anonymity have been popular features to improve upon.[2] Some cryptocurrencies have been created by known natural or legal persons, and some even have mechanisms including more or less centralized governance and permission-based access. For instance, Ripple is intended to improve the efficiency of settlements between financial institutions.[3] Many new cryptocurrencies serve as utility-tokens to fuel service platforms. Ethereum is such a platform, providing a complete programming language on the platform, which can be used for, inter alia, smart contracts.

Cryptocurrencies are based on two main principles: cryptography-based asset disposal and distributed ledgers. Cryptography-based asset disposal means that cryptographic keys are used to sign transactions and verify ownership.[4] The transaction sender signs a transaction with a secret private key, and a corresponding public key can be used to validate that the transaction has been signed by the corresponding private key.[5] The cryptographic-asset disposal also allows for various mechanisms for conditional disposal, allowing for the execution of smart contracts. As it is private keys and not personal identities that determine control of assets, and there is no need to link real-world identities with private keys, the systems are pseudo-anonymous.[6]

However, digital assets are easy to copy, entailing a double-spending risk. A traditional solution is to rely on trusted third parties to maintain registers. The prime invention associated with cryptocurrencies is the elimination of the need for a trusted third party by letting the users validate transactions and maintain the integrity of the register. This is called distributed ledger technology (DLT). DLT protocols are designed to maximize the incentives of the users to maintain the integrity of the ledger in compliance with the protocol governing the cryptocurrency. The DLTs in various cryptocurrencies are designed such that they facilitate:

- **Detection:** the transparency of the ledger facilitates detection of dishonest behavior.
- **Punishment:** dishonest behavior is costly. The reward for validating transactions is given in the actual cryptocurrency, which will probably be lost in case of dishonest behavior. For many cryptocurrencies, the protocol allows for a reward for validation in terms of newly minted coins.

By such a design, users given the authority to validate transactions have incentives to do so honestly to maintain the value of the reward.[7]

The blockchain technology invented with bitcoin can be used to illustrate the implementation of such a design.[8] In bitcoin, put simply, each single transaction is broadcasted to the user-network and propagated according to peer-to-peer technology.[9] Participants in the system generate addresses from their public keys for transactions between them. The private key corresponding to each public key used to generate an address is needed to dispose of the bitcoins at that address. Competitive block validators collect transactions to add into a block to be added to the

[2] For instance, Litecoin seeks to improve scale and speed relative to Bitcoin. Dash, Cloakcoin, and Zcash, among others, seek to improve privacy. See Duffield and Diaz (2014) and Cloak (2018) for documentation of Dash and Cloakcoin, respectively. Both also improve scalability. Sasson et al. (2014) is the original whitepaper for Zcash. Improved anonymity is achieved in all three by coin-mixing arrangements that prevent transparency with respect to the sender and receiver of coins.

[3] See https://ripple.com/.

[4] Cryptography-based asset disposal is not an invention to be credited to cryptocurrencies. Public-key cryptography has been available for decades and has been suggested in variants of digital cash since the 1980s.

[5] The public key is generated from the private key with a non-invertible function, which is supposed to make this system secure. Non-invertibility is meant in a practical, not mathematical, sense. Advancements in technology may affect the security of the cryptographic functions applied today.

[6] However, as so-called network analysis can be used to infer identities from limited real-world information, several cryptocurrencies seek to improve anonymity by variants of mixing to hide the senders and receivers of transactions. See, for instance, Conti et al. (2017).

[7] This shares parallels with repeated prisoner's dilemma games, which are often utilized to analyze stability of cartels. See Belleflamme and Peitz (2015), Chapter 14.

[8] Although the description is aimed at being as precise as possible, some simplifications are necessary to avoid a too-lengthy description. For a more detailed description, see, for instance, Narayanan et al. (2016); for technical details, see Antonopoulos (2017). Alternative implementations of DLT, not based on blockchains, have also been developed as means to maintain the integrity of a distributed ledger. One alternative is to represent the ledger as a directed acyclic graph (DAG). IOTA is an example of a cryptocurrency using DAG for maintaining the distributed ledger as described in Popov (2017).

[9] Most software implements a rule that only valid transactions are propagated further to the network. However, this is not a hard rule, but dependent on users following the protocol.

blockchain. In bitcoin, the block size imposes limits on the number of transactions to be included.[10]

Each new block is pointing to a hash[11] of the previous block.[12] Hence, the blocks are chained together in a blockchain. A consequence of this is that if a validator wants to include transactions not consistent with the previous blocks in a new block, the validator would then need to alter the whole chain, back to a block consistent with the fraud, possibly the genesis block, to get hashes consistent with the present block of transactions. This could, in theory, be a simple task, but the bitcoin blockchain is designed such that this would be very costly. This will be explained next.

To be allowed to add a candidate block to the blockchain, the validator must be the first to solve a computationally costly puzzle. This puzzle consists of assembling the hash of the previous block, a hash of the transactions in the candidate block, some other inputs, and a freely chosen nonce into a hash-function, such that the resulting hash falls below a certain threshold. Hence, the validator must find a nonce that produces a valid hash consistent with the blockchain that the subsequent blocks will point back to. To solve this puzzle, the candidate block validator must perform many trials, as the hash function is not invertible and each trial contains minimal information about the solution. The lower the threshold, the harder it is to find a solution. To maintain the difficulty as the technological computational capacity increases, reductions in thresholds are implemented in the protocol.[13] The difficulty is set such that a new block is found on average every 10 minutes. The first finder of a valid nonce gets the privilege of adding its candidate block to the blockchain. However, it is not guaranteed to be a part of the blockchain. This depends on future block validators building their blocks on this particular block – that is, whether it becomes part of the consensus chain. Assuming that future block validators are honest and only build upon honest blocks, a validator has strong incentives to be honest and follow the protocol. Attempts to violate the protocol rules will render the block abandoned and the potential reward lost. This incentive scheme, based on the miners' use of computing-resources to validate blocks to receive a reward, is referred to as proof-of-work (PoW).[14] After the nonce is found, its validity is easy to verify, which facilitates the detection of dishonest behavior.

The incentive to be a block-validator is that the validator can include a fixed amount of newly minted bitcoins to a chosen address (normally of the validator itself or a mining pool in which the block validator participates) and transaction fees set at the discretion of the senders. According to the bitcoin-protocol, the reward of newly minted coins is halved at intervals of about four years.[15] This causes the total supply of bitcoins to converge from below at approximately 21 million.[16] The justification for this specific scheme is not provided by Nakamoto (2008).[17] The 21 million cap is not a technological limit; it is a consequence of the consented protocol followed by the validators. In theory, miners could be rewarded with newly minted coins forever, rendering the total supply non-capped. Actually, many cryptocurrencies do not have currency-caps, such as Ethereum[18] and Monero.[19] Some cryptocurrencies, such as the cryptocurrency Basis, aim to have stability reinforcing mechanisms built into the protocol to maintain a peg to another metric, such as the U.S. dollar. In such a case, the coin-supply will be floating to whatever is necessary to maintain the peg.[20] As the mining reward in terms of newly minted bitcoins declines, transaction fees are expected to increase in importance to encourage validation.[21] Since the block-validator is rewarded newly minted coins, the block-validators are commonly referred to as miners. The newly minted coin reward and the transaction fees are lost if the block does not become part of the consensus chain.

Cryptocurrencies are supposed to be decentralized. However, certain stakeholders may have more influential roles than others. As just explained, validators potentially

[10] The block-size is 1MB. A transaction contains on average 495 bytes, which makes the average number of transactions per block slightly below 2000.
[11] A hash function generates a non-invertible fixed-length output from an input in the same manner as a public key is generated from a private key
[12] To be precise: the header of the previous block.
[13] Although the main rule so far has been that the difficulty increases, it is also possible that the difficulty level reduces if the average time taken to find a new block increases.
[14] Various alternatives to PoW exist that may be used in combination with PoW. One commonly applied scheme is proof-of-stake (PoS). PoS means, simplified, that the block-validator is determined probabilistically according to the stake in the actual currency. For a detailed analysis of PoS schemes, see Bentov et al. (2016).
[15] The reward started at 50 bitcoins per block and halves every 210,000 blocks, which happens approximately every four years.
[16] Using a geometric series as an approximation, the upper limit is given by $21000 * 50 * \sum_{k=0}^{\infty} \left(\frac{1}{2}\right)^k = 210000 * 50 * 2 = 21\text{m}$. Because bitcoins are not infinitely divisible, the maximum is slightly below 21 million.
[17] See https://bit.ly/1pQPBGe.
[18] To be more precise, this applies to the token Ether, see https://bit.ly/2zCJgVS.
[19] See https://bit.ly/2OfSVJB.
[20] See Al-Naji et al. (2018) for the Basis whitepaper. See also Østbye (2018b) for a critique of the mechanisms relied upon by Al-Naji et al. (2018).
[21] The limited capacity of bitcoin blocks can affect whether a miner includes the transaction in the block or not, or at least how fast the transaction will be processed. Huberman et al. (2017) studied equilibrium transaction fees in a simplified model. Tsabary and Eyal (2018) use simulations to show that validation only based on transaction fees can impede the security of bitcoin.

wield great influence. There is a risk of concentration among such validators, which would increase their influence.[22] If changes in the protocols are to be implemented, it is ultimately the validators that must execute these changes. Other influential stakeholders include so-called core developers. The formalized role of such core developers varies from cryptocurrency to cryptocurrency. Some protocols include mechanisms for awarding core-developers directly with newly created coins. In some permission-based schemes, the core-developers are fixed. The core-developers also have a role as the face of the cryptocurrency, resembling the administration of a corporation. Just as an administration might be replaced by a board, validators might replace the core-developers. Such influential stakeholders can be referred to as operators. However, due to the decentralized characteristics of cryptocurrencies, normal users holding a node may take part in the operation by propagating transactions and performing other functions, such as mixing coins to facilitate anonymity. The term normal users refers here to persons mainly using cryptocurrencies for the benefit they provide. The distinction between operators and normal users is not binary.

> "Cryptocurrencies are based on two main principles: cryptography-based asset disposal and distributed ledgers."

There are several ways users can acquire cryptocurrencies from their owners. Such acquirement can, inter alia, follow from bilateral private exchange, brokers, professional exchanges, and as payment for goods, services, and labor. In addition to those involved in the direct trade with cryptocurrencies, there is an ecosystem of third-party service providers, such as wallet providers for users to administer their cryptocurrencies, payment service providers, consulting services, and investment services. Such services allow for users not participating as nodes in the system, as such providers can appear as custodians for the users with their own nodes. Such custodians share similarities with banks and, in fact, some traditional banks are providing such services.

3. ARE CRYPTOCURRENCIES' CURRENCY-CAPS ANTITRUST CONSPIRACIES?

3.1 Antitrust conspiracies

The antitrust laws are legal rules regulating actions that restrict competition between businesses in the marketplace. Broadly speaking, the antitrust laws cover cooperation between businesses that restricts the competitive pressure among them, practices that might prevent competitors from competing fiercely in the marketplace, and mergers and acquisitions that restrict competition. Many jurisdictions follow the same template of competition law: prohibiting anti-competitive cooperation, prohibiting unilateral abuse of market power, and merger regulation that provides the legal basis for controlling mergers that restrict competition.

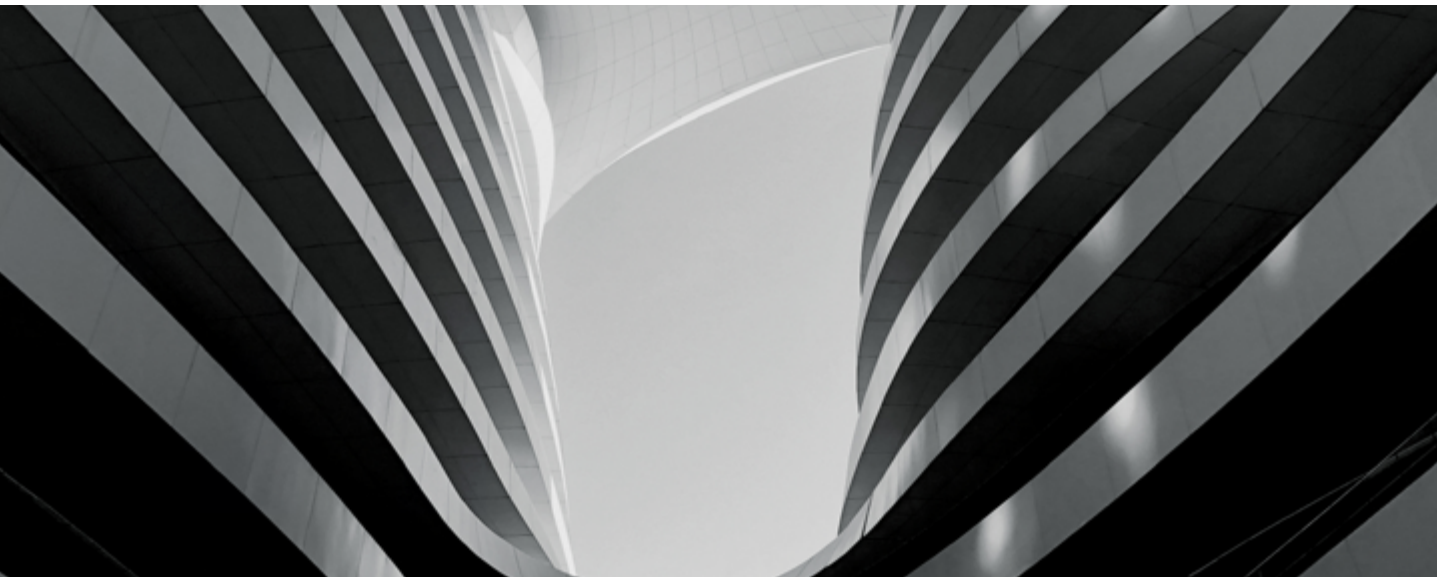
In this paper, we are concerned with the prohibition of anti-competitive cooperation, which also can be referred to as antitrust conspiracy. This paper will not delve into the details of any particular jurisdiction. However, the U.S. and the E.U. serve as examples. In the U.S., the Sherman Act, Section 1, prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade." In the E.U., the TFEU Article 101 prohibits "agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market."[23]

No formal agreement is necessary to establish an illegal cooperation. However, some sort of "meeting of minds" is necessary to distinguish cooperation from unilateral behavior.[24] Cooperation can, inter alia, follow from some communication to facilitate the coordinated behavior. Individual rational adoption to the market

[22] A concern with decentralized validation is that validators or a coordinated group of validators could gain sufficient validation power to render a decentralized network de facto centralized. A so-called 51-percent attack refers to the situation where a dishonest validator or cartel of validators gains sufficient power to manipulate the ledger. A 51-percent attack is usually associated with so-called double-spending attacks. This involves a validator mining secret blocks to replace with the consensus blocks as the longest chain, facilitating the ability to spend the same coins twice. Much research has been devoted to the robustness of cryptocurrency protocols, in particular bitcoin, against attacks by validators with sufficient validation power. See, for instance, Conti et al. (2017) for a survey of possible attacks on the bitcoin blockchain. See also Narayanan et al. (2016), Chapter 5.

[23] For a more detailed description of competition law, see Østbye (2013).

[24] Unilateral conduct may also be subject to antitrust liability. This will not be discussed in this paper. For a general discussion on antitrust liability in the cryptocurrency markets, see Østbye (2017).



is not cooperation, even if the outcome is a mutually beneficial equilibrium among other "worse" equilibria in a game theoretical sense. For instance, two competitors maintaining an artificially high price (relative to cost) because both know that if one of them reduces their price the other will follow suit is not as such cooperation in an antitrust sense.

Cooperation that prima facie restricts competition may still escape illegality if it can be justified by legitimate grounds. For instance, in the U.S., cooperation not considered harmful per se, such as outright price fixing is judged according to a rule of reason standard, which means that it must be individually assessed as to whether the restraint is reasonable to make the society better off – that is, if consumer welfare is improved. In the E.U., the question is whether the restraint is necessary to realize social gains and the consumers receive a fair share of this gain. Another way to state legitimate grounds, which will be used in this paper, is whether the cooperation is ancillary to realizing gains that benefit society and consumers are not hurt. In this paper, we will consider consumers as those users using the cryptocurrencies for their intended purpose – that is, for transactions – without profiting from the operation as such.

Below, we will assess the conditions for currency-caps in cryptocurrencies to be considered as cooperations in an antitrust sense. The question as to whether such cooperation has legitimate grounds will be returned to in Section 4.

3.2 Are the operators liable entities?

The first question that must be addressed before we can take a stand on antitrust liability is whether operators of a cryptocurrency are liable entities according to antitrust law. In many antitrust regimes, such as that of the U.S., both natural and legal persons can be held liable. In some jurisdictions, like the E.U., only entities performing some economic activity can be held liable.[25] Such a restraint would, for instance, mean that those using cryptocurrencies only for private purposes, such as purchasing services for consumption, cannot be held liable. In such circumstances, the liability of operators such as block-validators, doing this as a hobby or for idealistic purposes, is unclear. However, for certain cryptocurrencies, such as bitcoin, many validators are clearly commercial, with business plans, employees, and investor backing. They will not escape antitrust liability on the grounds that they do not perform economic activity.

[25] However, at the national level, the member states may hold any person liable.

Cryptocurrency operators are normally scattered among jurisdictions. Hence, another question is whether the operators may escape liability because they are outside the jurisdiction of the countries wishing to apply their antitrust laws. Normally, antitrust liability is based on effects in the relevant jurisdiction and not the geographical location of the offenders. This means that if a conspiracy is established outside a country, but with effects in that country, possibly by persons with alien citizenship, this does not prevent the persons being held liable. This is rather an enforcement problem. As a country does not have enforcement powers outside its jurisdiction, the country is dependent on extradition agreements or if the person enters the country of jurisdiction voluntarily.

Consequently, it seems that restrictions on liable entities do not constitute any obstacle for antitrust liability. Lack of jurisdiction may, however, constitute a practical problem for enforcement.

3.3 Are the operators behaving unilaterally or in coordination?

For there to be an antitrust conspiracy, there must be coordination on the currency caps. Hence, the behavior of the operators cannot be a unilateral rational adoption. Despite common referrals to terms like “consensus protocol” and “consensus mechanism” in the cryptocurrency world, it is not obvious that the operators cannot be said to behave unilaterally. Rather, the governance structure of distributed ledgers is designed such that it is individually rational for each participant to follow the protocol without the need for communication or other coordination, as described in Section 2.

There are, however, several arguments that can be provided that indicate coordination. The original creators of a cryptocurrency may be a group of several persons. In this sense, there is coordination initially, and then new participants join this coordination. Furthermore, the protocol can be seen as an invitation by the original creators to participate, which is accepted by participants, thereby establishing coordination. Furthermore, as miners in PoW schemes join mining pools, each pool is a case of coordination. However, maybe the clearest indication of widespread coordinated behavior is the community communication between the operators in the operation of a cryptocurrencies. Operators communicate with each other for the coordination on protocol changes. This involves, inter alia, communications among core developers and validators, among validators, and among mining pools. This is done in community chat forums, and such communications are often a part of the protocol itself. For instance, in the bitcoin protocol, so-called bitcoin improvement proposals (BIPs) are a part of the protocol, and block-validators can use the blocks to signal their position [Narayanan et al. (2016), Chapter 7].

Consequently, it seems reasonable to conclude that there is coordination between the operators of a cryptocurrency in an antitrust sense, distinguishable from unilateral behavior.

3.4 Are the operators a company or structural joint venture?

A diametric opposite to unilateral conduct would be having the participants in a cryptocurrency be considered as a single entity, like a company. Normally, operations within a company will not be considered as illegal coordination. For instance, an owner of several shops may set common prices for all the shops without being subject antitrust liability. Furthermore, so-called structural joint ventures entered into by several parties operated as an individual unit with stable control-conditions, can be considered as a single unit not subject to antitrust liability for the operation of the unit.

A requirement of stable control conditions would render most cryptocurrencies outside the scope of being a unit under stable control conditions. Rather, the intention behind cryptocurrencies is that no one is supposed to be in control, although an oligopolistic structure of operators may prevent this intention in practice. Hence, most cryptocurrencies, such as bitcoin, cannot be considered a structural joint venture. This may, of course, change if a single validator or mining pool obtains sufficient computational power to de facto control bitcoin block-validation. If a mining-pool obtains de facto control over bitcoin on a stable basis, this mining pool may be considered as a structural joint venture. However, so far there is no evidence that this is the case.

As pointed out by Zetzsche et al. (2017), the conclusion might be different for permissioned special purpose cryptocurrencies, such as Ripple. Such cryptocurrencies often satisfy the condition of a stable control structure. This must be considered from cryptocurrency to cryptocurrency. For further discussion in this paper, it is assumed that we are not dealing with cryptocurrencies organized as structural join ventures.

3.5 Are cryptocurrencies' currency-caps restricting trade?

For a cryptocurrency currency-cap to be an antitrust conspiracy, it must restrict trade by somehow restricting the competitive process. It is well established that cooperation on quantity restrictions restricts competition. This is obvious in the "normal" economy of goods and services, as cooperation among suppliers to restrict output deprives the consumers of the benefit from suppliers competing with each other to capture market shares by, inter alia, lowering prices.

Cryptocurrency validators do not compete in terms of capturing market shares. In fact, users cannot choose their validators. Still, prima facie, it seems that coordination on a currency-cap restricting the amount of currency issued has the same effect. A cap on the currency increases its price in the same way as restricting output on normal goods and services increases prices. If competing validators could freely choose the reward for validating transactions, they may choose another reward than that set in the protocol, which would violate the cap. Hence, it is not unreasonable to assume that currency caps would be considered to restrict trade. This does not automatically mean that such caps are unlawful. This depends on the presence of legitimate reasons, as will be discussed in Section 4.

4. DO THE CRYPTOCURRENCIES' CURRENCY-CAPS HAVE LEGITIMATE JUSTIFICATIONS?

If we assume that cryptocurrencies' currency-caps compromise coordinations that restrict trade, the question is whether such currency caps can be legitimately justified. The exact legal assessment of such legitimate justifications varies between both contexts and jurisdictions. Such legal details are avoided here. In the present assessment, an agnostic approach is taken to the benefit of cryptocurrencies as such. If one takes the position that cryptocurrencies are bad for the society as such, no legitimate justifications may be found. Hence, the approach taken is that as long as there is demand for cryptocurrencies, they provide some sort of benefits to those who are involved with them. The question is whether currency caps are necessary to realize those benefits without harming the users, as described in Section 3.1.

4.1 Cryptocurrencies as money

Bitcoin and many other cryptocurrencies were introduced as alternative money and payment systems. Nakamoto (2008) makes several references to bitcoin as money and a payment system. At first sight it might appear obvious that the currency cap on cryptocurrencies is a prerequisite for their existence. Without any cap on the issuance, there is a chance that validators would issue too much, causing a value-loss and preventing the cryptocurrency from functioning as money – that is, from providing functions as mediums of exchange, units of account, and stores of value [Ali et al. (2014)]. Central bankers tend to argue that cryptocurrencies do not satisfy any of these properties today and, thus, are not money [Carney (2018) and Soderberg (2018)]. Such arguments may in some cases appear inconsistent, as it is at the same time argued that cryptocurrencies should be regulated for some of their money properties. Indeed, cryptocurrency exchanges are subject to money services regulations in several jurisdictions. Besides, central bankers' assessments of the moneyness of cryptocurrencies may not provide useful guidance on how they should be assessed under antitrust law. Furthermore, cryptocurrencies' capability to fulfill money functions may change in the future.

In the theory of private money supply, economists have argued that issuers' commitment to restricting issuance is essential for success [Klein (1974) and Fernández-Villaverde and Sanches (2016)]. Otherwise, the issuer would be tempted to issue too much, eventually causing the collapse of the value of the issued money. Numerous historical examples of privately issued money seem to confirm this thesis [Schnabel and Shin (2018)].

For cryptocurrencies, there would be an over-issuance risk with no restriction on validation rewards. For competing block-validators, there would be an externality present if they were free to mint whatever block-reward they wished, which would exacerbate the over-issuance risk. However, as block-validators need approval of their blocks by later block-validators to have their block included in the consensus chain, some discipline would be enforced. Later block-validators would probably be reluctant to include blocks with very high validation rewards. Such discipline would not be coordination as long as the block-validators make this decision unilaterally.

In developed economies, national fiat currencies are subject to inflation targets as well as constitutional checks and balances for money to remain credibly stable. Hyper-inflation seldom ends well in the countries where it happens. Hence, it seems that for cryptocurrencies to function as money, the issuance must be under some control.

However, controlling over-issuance is not equivalent to currency-caps. Inflation-targets for national fiat-currencies not only serve the purpose of protecting the currency from inflation, but also of protecting it from deflation. Deflation is not considered beneficial, as people may end up hoarding money instead of fueling the economy with consumption and investment. Consumption would be delayed, as holding the money would increase purchasing power. Investment would need to exceed the value-increase in money to be attractive. In macro-economic research, there have been various golden rules suggested for inflation targeting to protect a currency both from the evils of inflation and deflation [Langdana (2016), Chapter 11].

Consequently, it seems that if we are going to consider cryptocurrencies as money, some sort of money growth would be preferred to an absolute currency-cap to prevent harmful deflation. A concern would be that a coordinated rule on money growth would just be another coordinating antitrust violation. Such a concern has no merits, however, as a justified money growth rule more easily satisfy a legitimate justification requirement. The question then is whether a rule on money growth is achievable, or if currency caps are a technical necessity to restrict issuance. As several cryptocurrencies do not have currency caps, it seems they are not a necessity for cryptocurrencies.

As a currency cap seems neither optimal nor necessary for a cryptocurrency scheme, it seems plausible to conclude that the money character of cryptocurrencies is not a clear legitimate justification for a currency cap. This puts operators of such cryptocurrencies into antitrust risk. The short analysis provided here may of course be refuted by valid legitimate justifications, but according to standard burden-of-proof principles, it is the operators that must provide such justifications in an antitrust trial.

4.2 Cryptocurrencies as securities

Another way to look at cryptocurrencies is to apply the analogy to securities. Securities are typically bonds and equity stocks in companies. This analogy typically applies well to so-called initial coin offerings (ICOs) of tokens, where the tokens are a claim on a potential future value similar to securities. Many securities regulators have assessed whether securities regulation applies to ICOs [Zetzsche et al. (2018) and Fein (2018)]. There is no practice for considering caps on securities or company stocks as antitrust conspiracies. Such caps are usually essential for investors. Securities are claims on specific assets, such as a company. For instance, company stocks are residual claims on the value of a company. If new company stocks are issued, the value of the existing stocks is, according to theory, correspondingly diluted. A cap on the stocks, and the requirement of consent by the stock holders for diluting the stock by the issuance, is necessary for investors to acquire the stocks in the first place. Similarly, for bond issuers, if a debtor issues new bonds, the prospects of repayment in case of default reduces, as there are more creditors to share the remaining assets in case of bankruptcy. Hence, bond investors will normally require some control or commitments with respect to a debtor's issuance of new bonds.

Consequently, to the degree that cryptocurrencies are considered securities or share the characteristics of securities, there seem to be a weak case for considering currency-caps as antitrust conspiracies.

4.3 Cryptocurrencies as commodities

Cryptocurrencies could be considered commodities. The U.S. Commodity Futures Trading Commission (CFTC) has under certain circumstances considered cryptocurrencies as commodities [Adimi (2018)]. Comparing cryptocurrencies to digital gold is common, and is, in fact, used in Nakamoto (2008) to characterize bitcoin: "By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

Coordinations restricting the supply of commodities are at the core of what are considered antitrust conspiracies restricting trade. An international cartel restricting the supply of gold would be a strong antitrust case. The question is then whether bitcoin and other cryptocurrencies are so different from other commodities that a cap-coordination is justified. A particular feature of cryptocurrencies is that they are often pure digital goods not backed by any tangible assets. As opposed to gold, the scarcity of bitcoin and other cryptocurrencies is a pure social construct. Hence, they could potentially be supplied in an infinite amount. As discussed in Section 4.1, some scarcity is necessary for them to have value as money, which also applies if they are considered as commodities. Hence, it might seem that the operators would have some merits in arguing for a restricted supply where the cryptocurrencies are considered as commodities. However, this does not necessarily justify a currency cap.

This issue will not be concluded here. Rather, it will be asked instead what the theory of harm is. What theories of harm would the operators overcome in arguing for the legitimacy of the cap? The obvious theory of harm would be that the conspirators create something artificial in limited supply, and earn market power profits from any gains exceeding normal returns. There are, however, several problems associated with such an assessment. The first is the benchmark for normal returns. Some critical commentators would say that as cryptocurrencies have no fundamental value, all profits will be gains from the illegal coordination. However, this will be too-hasty a conclusion considering the possible benefits to society of cryptocurrencies. Another problem is that in PoW schemes, competing operators are not likely to obtain above-normal returns, as most of the income from mining is required to cover the costs associated with the PoW (such as electricity costs). The harm would then be the alternative cost to the society as the resources could have been spent better.

The quote from Nakamoto (2008) above also reveals another more sophisticated possible theory of harm. The newly minted coins work as an incentive scheme to validate transactions to later be replaced by transaction fees. This means that the users' transactions are subsidized in the beginning as validators finance their transactions by newly generated coins. However, as the cap is approached, and later reached, transaction fees must finance the operations. According to the theory of network effects and platform competition [Belleflamme and Peitz (2015)], this might be effective in obtaining sufficient scale. However, such mechanisms might also create lock-in effects, making it possible to exploit users in the future. A full analysis is beyond the scope of this paper [See Huberman et al. (2017) for a study of equilibrium fees in a bitcoin-like scheme].

Consequently, considering cryptocurrencies as commodities might initially provide a clear case of coordinated currency-caps as conspiracies violating antitrust law, which may render a burden of proof upon the operators to justify legitimate reasons. With that in mind, it also seems like the traditional theory of harm of antitrust conspiracies – excessive prices – does not follow the same mechanism in the operation of a cryptocurrencies. Competition among operators is likely to eliminate market power profits of operators. The theory of harm would be more justified if one thought of the entire cryptocurrency scheme as social waste, or if concentration of operators paved the way for excessive profits.

5. CONCLUDING REMARKS

This paper provides arguments and counter-arguments for currency-caps in bitcoin and other cryptocurrencies to be considered as antitrust conspiracies. If they are considered antitrust conspiracies, operators may be subject to both criminal and civil liabilities. Antitrust liability is probably just one of the many legal liabilities rendering it prudent for the creator(s) of bitcoin to remain anonymous. In the context of antitrust, Satoshi Nakamoto could be considered as the ultimate cartel ringleader. Legal liabilities are only theoretical without enforcement. For cryptocurrencies where the operators are pseudo-anonymously spread over a manifold of jurisdictions, enforcement is impractical. Hence, the real risk to the operators is probably marginal for now. This might change as operators become more concentrated and institutionalized, and as analytical tools improve in revealing the real identities of the operators.

REFERENCES

Adimi, A., 2018, "Regulating decentralized cryptocurrencies under payment services law: lessons from the European Union," Journal of Law, Technology, & the Internet 9:1, 1-1st.

Ali, R., J. Barrdear, R. Clews, and J. Southgate, 2014, "The economics of digital currencies," Bank of England Quarterly Bulletin 54:3, 276-286

Al-Naji, N., J. Chen, and L. Diao, 2018, Basis: a price-stable cryptocurrency with an algorithmic central bank," white paper, https://bit.ly/2NH00Wu

Antonopoulos, A. M., 2017, Mastering bitcoin: programming the open blockchain, O'Reilly Media, Inc.

Belleflamme, P., and M. Peitz, 2015, Industrial organization: markets and strategies, Cambridge University Press

Bentov, I., A. Gabizon, and A. Mizrahi, 2016, "Cryptocurrencies without proof of work," in International Conference on Financial Cryptography and Data Security, Springer, 142-157

Carney, M., 2018, "The future of money," speech to the inaugural Scottish Economics Conference, Edinburgh University, March 2, Bank of England

Chuen, D. L. K. (ed.), 2015, Handbook of digital currency: bitcoin, innovation, financial instruments, and big data, Academic Press

Cloakteam, 2018, "Enigma v2.1 A private, secure and untraceable transaction system for CloakCoin," white paper, https://bit.ly/2uJF5Xc

Conti, M., C. Lal, and S. Ruj, 2017, "A survey on security and privacy issues of bitcoin," arXiv preprint arXiv:1706.00916.

Duffield, E., and D. Diaz, 2014, "Dash: A privacy-centric crypto-currency," white paper, https://bit.ly/2p3gABX

Fein, M. L., 2018, "Bitcoin: how is it regulated?" white paper, https://bit.ly/2Mq9KQv

Fernández-Villaverde, J., and D. Sanches, 2016, "Can currency competition work?" working paper no. w22157, National Bureau of Economic Research

Huberman, G., J. D. Leshno, and C. C. Moallemi, 2017, "Monopoly without a monopolist: an economic analysis of the bitcoin payment system," working paper, https://bit.ly/2OhHLnA

Klein, B., 1974, "The competitive supply of money," Journal of Money, Credit and Banking 6:4, 423-453

Langdana, F. K., 2016, Macroeconomic policy: demystifying monetary and fiscal policy, Springer Texts in Business and Economics

Nakamoto, S., 2008, Bitcoin: a peer-to-peer electronic cash system, https://bit.ly/LjkXCv

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and G. Goldfeder, 2016, Bitcoin and cryptocurrency technologies: a comprehensive introduction, Princeton University Press

Østbye, P., 2013, "Rational antitrust analysis: an inquiry into antitrust assessment principles and procedures," doctoral dissertation, Series of dissertations submitted to the Faculty of Law, University of Oslo no. 59

Østbye, P., 2017, "The adequacy of competition policy for cryptocurrency markets," working paper, https://bit.ly/2xaGgj0

Østbye, P., 2018a, "Will regulation change cryptocurrency protocols?" working paper, https://bit.ly/2p4OJBE

Østbye, P., 2018b, "Model risk in cryptocurrency governance reliability assessments," working paper, https://bit.ly/2N893QR

Paech, P., 2017, "The governance of blockchain financial networks," The Modern Law Review 80:6, 1073-1110

Popov, S., 2017, "The Tangle," white paper, https://bit.ly/2KXUlqQ

Sasson, E. B., A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, 2014, "Zerocash: decentralized anonymous payments from bitcoin," in 2014 IEEE Symposium on Security and Privacy (SP), 459-474

Schnabel, I., and H. S. Shin, 2018, "Money and trust: lessons from the 1620s for money in the digital age," Bank for International Settlements No. 698

Soderberg, G., 2018, "Are bitcoin and other crypto-assets money?" Economic Commentaries No. 5, Sveriges Riksbank

Tsabary, I., and I. Eyal, 2018, "The gap game," working paper, https://bit.ly/2Oftd8a

Tu, K. V., and M. W. Meredith, 2015, "Rethinking virtual currency regulation in the bitcoin age," Washington Law Review 90, 271-347.

Zetzsche, D. A., R. P. Buckley, and D. W. Arner, 2017, "The distributed liability of distributed ledgers: legal risks of blockchain," University of Illinois Law Review, https://bit.ly/2OdnDT0

Zetzsche, D. A., R. P. Buckley, D. W. Arner, and L. Föhr, 2018, "The ICO gold rush: it's a scam, it's a bubble, it's a super challenge for regulators," University of Luxembourg Law Working Paper no. 11/2017

CAPCO

THE FUTURE. NOW.

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube and LinkedIn.**

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM