Whither Cryptomoney?

Is cryptomoney a threat to equality and national sovereignty?

Simon Boeke, Universiteit Leiden, 19-06-2019, under supervision of Bruno Verbeek

Table of Contents

Introduction

Money used to be simple. Everybody liked the shiny yellow metal we now call gold. However, at a certain point, some so-called 'states' made the whole practice of exchanging gold rather more complicated, as they issued vouchers that were said to 'represent' an amount of gold. Even more farfetched was their later decision to cut any links between our metal of desire and the vouchers we got accustomed to. In the present day, our vouchers often lack any physical qualities, and seem to be nothing more than digits projected on a computer screen. It is perhaps remarkable that the proverbial man or woman in the street does not at all seem to be concerned with how abstract our money really is. Its omnipresence and utility have made almost every inhabitant on earth comfortable using it. We hardly reflect on its nature anymore. And so, now that an entirely novel type of money – cryptomoney – is coming to the forefront, we are quick to accept it as just another incarnation of a phenomenon that we have been familiar with ever since we started appreciating a certain shiny yellow metal. But I believe this to be a mistake.

Cryptomoney has the potential to transform our financial system just as radically as the move from gold and silver to fiat money, or the abandonment of the gold standard once did. This is because there are certain qualities to cryptomoney that are fundamentally different from the money as we know it. It seems, however, that although some people are interested in comparing different types of money from an economic standpoint, not many care about the philosophical implications of choosing one system over another. I believe this to be a second mistake. The economist Leonidas Zelmanovitz is right when he says that 'the value of any monetary policy is contingent on its adherence to a coherent set of philosophical assumptions'.[1] But this works both ways, and we should also not neglect how our philosophical assumptions are challenged by the sort of money we use. If cryptomoney would make it harder for us to adhere to our ideas about justice, equality, fairness etc. that underlie our financial system, we should try to prevent it from gaining too much prominence.

The question that lies at the origin of this investigation is the following: should we want to replace 'traditional' money with cryptomoney? The answer to this question will be negative: in this paper I will argue that it is impossible to replace traditional currencies with any form of cryptomoney and not as a direct result undermine national sovereignty and increase inequality within countries, and between them. The former is under threat because of

[1] Leonidas Zelmanovitz, *The Ontology and Function of Money. The Philosophical Fundamentals of Monetary Institutions*, (London 2016) 6.

the decentralized market-based nature of cryptomoney that leaves powerless governmental tools to execute monetary policy. The latter is the result of the disproportionate advantage more affluent people and countries will gain over their poorer equivalents as a consequence of the way cryptomoney works. If we see the consequences of these two effects through, we arrive at the conclusion that any form of replacement of traditional money by cryptomoney means a redistribution of power from (democratic) states to the market, from people to algorithms, from economically less developed countries to economically more developed countries, and from the poor to the rich. Such a redistribution, I will argue, is unjust and undermines the legitimacy of states.

To support this conclusion, I have divided this thesis in four chapters. In chapter one, I will answer the questions what money is and how cryptomoney is a separate subset of the money family. A definition of cryptomoney will also be provided, as there are many virtual phenomena called cryptomoney that are really something else. Through this definition we will come to see that cryptomoney functions quite differently from the money we use today. And because cryptomoney's ability to change our society stems in part from its technicalities, I will then give a concise explanation of how cryptomoney works. One of the really novel aspects of cryptomoney is the way it is safeguarded against fraud. The technology that does this, the 'blockchain', is the reason why cryptomoney could be the first serious competitor to national currencies since gold. Important as this all is, we will not discuss the mathematical or programmers' side of cryptomoney in detail; it has been done elsewhere. Rather, we move on to the second chapter and discuss the consequences that a financial regime based on cryptomoney would have for states and individual users. We refrain from giving too strong a normative judgment here, and merely list and explain some of the most important practical advantages and disadvantages that the introduction of cryptomoney could have, in order to better understand why cryptomoney is so attractive to some of its proponents.

In chapters three and four we shift our attention to the main question of the thesis: is cryptomoney a good idea? Now there might be many arguments that could be given either for or against using cryptomoney, and some of these will be discussed in chapter two. Many of these arguments, however, are mostly pragmatic in nature, and therefore not very interesting for a philosophical inquiry. Others do merit more thorough examination, but are contingent on the type of cryptocurrency used. However, there are two arguments against cryptomoney that are rather more substantial. In chapter three, we will explain why cryptomoney necessarily undermines national sovereignty, and why that would be bad. Chapter four does the same for equality. These arguments hold for any form of cryptomoney as defined in

chapter one, as they are the direct result of the way cryptomoney functions. Furthermore, they transcend all pragmatic arguments, because of the strong commitment many of us have to sovereignty and equality.

Naturally, not everyone believes in these values. And although I will give some arguments in favour of sovereignty and equality, this thesis does not have the explicit aim to convince those that a priori disagree with me that these two principles are desirable. There are many libertarians and anarchists who are outright opposed to the basic idea of statehood, and do not think that national sovereignty is worthwhile at all. Likewise, there are some who claim that (some sort of) inequality has utility, usually because it yields a desired effect. For some niche thinkers it could even be good in itself. This paper might not be for them.

Of course, many of cryptomoney's (dis)advantages will only become apparent in a future where cryptomoney sheds its volatile state and blossoms into a type of money on par with the money we have now. That it could come that far is an underlying assumption for this research. It is made plausible throughout, and in chapter one especially. Interest in cryptomoney surges and it has already proven to be a very popular type of artificially created money. At the same time, it would be folly to claim that we are on the brink of a true cryptomoney revolution. The trade volume of all cryptocurrencies combined is still quite small, and no single currency, not even the (in)famous bitcoin, is anywhere near a position where it could start replacing even the weakest of national currencies. So uncertain is the future in fact, that it is even possible that we are already past the peak of cryptomoney. And that would then actually be a good thing, as an ascension of cryptomoney will lead to an increase of the problems noted in chapter three and four. In a way, you could say that this inquiry aims to make itself obsolete, because in the end it argues that cryptomoney would be bad for us. Still, if we manage to keep the use of cryptomoney at bay, and all the different cryptocurrencies lose their value, that would not mean that the phenomenon could not still be valuable as a hypothetical alternative to traditional money, capable of shedding light on our current monetary institutions and the normative foundations on which these are based.

Chapter 1

What is cryptomoney?

§1. Money and cryptomoney

Let us begin the answer to the titular question with the unsurprising statement that cryptomoney is a subset of money. And as such it shares certain crucial features with other forms of money. It is, however, not identical to what I will call 'traditional' or 'national' money – the money that we think of when we talk about money in everyday life. So, let us take a step back, and first take a quick look at what money is. First off, it is useful to realize that money has never been uniform. It has taken many shapes and forms during the course of history and may be as old as agrarian society itself.[2] Gold and silver were dominant for a long time, but shells, cocoa beans, stones, teeth, paper, and many other materials have been used as money.[3]

Presently, most of these varieties have been replaced by fiat money, like coins and banknotes. What makes fiat money different from the earlier forms of money, is that the value of the resources that it is made of (paper, or cheap metals) is much lower than the value it represents. Golden and silver coins, in contrast, were as valuable as the materials they were made of. Instead, the value of fiat money is based on a central bank's assurance that it has value. Another recent phenomenon is demand deposit, the virtual kind of money stored in a bank, that is retrievable with a cheque or a debit card. Although it is often redeemable in coins or notes, with demand deposit all physical qualities of money are lost. Different as all these types of money may be, what in the end ties all of them (including cryptomoney) together, are their functions. Many scholars agree that money has at least these three distinct qualities: it can be used as a means of exchange, a storage of value, and a unit of account.[4] We will shortly discuss what those are exactly. But even if something possesses these qualities, it is not automatically money. There also need to be people who agree that a specific currency fulfils these three roles. And this is where things get slightly more complicated.

If someone were to come up with a completely new currency one day – the grains of sand from his backyard for example –, it is unlikely that other people would instantly accept

[2] Glyn Davies, *A History of Money. From Ancient Times to the Present Day*, (Cardiff 1994) 47.
[3] Davies, *A History of Money*, 33-50.
[4] The European Central Bank also adheres to this definition: 'What is money?', (20-06-2017) as found on: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html accessed: 03-04-2018.

it as money. In fact, there is nothing in the world that naturally fulfils the three functions mentioned above. A critically large community is required to have faith in a currency for it to fulfil these functions and have any value. And how large this community needs to be, depends on the use you want to get out of your money. Two people can in theory have a working currency, but if neither one of them is a baker, they will not be able to buy any bread with it. And if they wanted to trade overseas with a completely foreign people, they would need a currency even more universal than the one the village baker accepts. The key concept in making anything work as money, is trust.[5] People need to be able to trust that they can buy stuff with their money (for it to work as a means of exchange), trust that it will not lose its value over time (as a unit of storage), and trust that they are paying a fair price for whatever they are buying (as a unit of account). All the different currencies in the world work like this and they paradoxically derive their value from people's convictions that they have value. So, for cryptomoney to ever be a serious alternative to traditional money, it will need to be able to fulfil the same three functions and garner enough trust. However, even if a cryptocurrency manages to do so, it would still be quite different from a traditional currency.

Defining cryptomoney is not easy, as there are thousands of different cryptocurrencies, all with slightly different traits.[6] In fact, cryptocurrencies have gotten so popular, that all kinds of companies and projects have adopted the terminology without having anything to do with cryptocurrencies, just to attract investors.[7] This does make it quite a bit harder to separate the real cryptocurrencies from the shams, and the definition proposed here will likely exclude many things that are cryptocurrencies in name only.[8] We can already exclude those that cannot fulfil the three functions of money listed above. Of course, many cryptocurrencies can, including some of the most popular like bitcoin or ether, but that alone

[5] Benjamin Cohen, *The Geography of Money*, (Ithaca 1998) 10-13.
[6] On 23-04-2018, there were 1584 different cryptocurrencies listed on www.coinmarketcap.com (the most used site giving an overview of cryptocurrencies' values) and not only is that number growing by the week, it is very likely that there are hundreds of other, so far unlisted, cryptocurrencies out there, trying to gain popularity.
[7] John Detrixhe, 'A dozen companies that reaped rewards by putting "bitcoin" or "blockchain" in their name', on: *Quartz (qz.com)* (12-01-2018) as found on: https://qz.com/1175701/putting-bitcoin-or-blockchain-in-a-company-name-is-sometimes-enough-for-a-pop-on-the-stock-market/ accessed: 18-04-2018.
[8] Venezuela, for example, plagued by hyperinflation, decided in February 2018 that all taxes could be paid in 'petro's', a 'cryptocurrency' launched by the government, that was in fact a regular – albeit virtual – currency much like Venezuela's bolivar. Calling it a cryptocurrency did little for the stability of the petro and after hyperinflation struck this currency too, its use was discontinued six months later. See:
Brian Ellsworth, 'Special Report. In Venezuela, new cryptocurrency is nowhere to be found', on: *Reuters.com* (30-08-2018) as found on: https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U accessed: 18-06-2019.
Other 'cryptocurrencies' have a centralized ledger controlled by a single company. The dangers of such a pseudo-cryptocurrency have been repeatedly demonstrated when several of them turned out to be nothing more than Ponzi-schemes (examples include: argyle coin, m-coin, onecoin and others).

is not enough for a definition. We do still need to look at what sets cryptomoney apart from things like euro's, dollars, gold, oil, or even weapons, things that in different places all fulfil the function of money.

Turning to cryptomoney for our answer, we are immediately confronted with the distinctly unique way the cryptocurrencies are organized. Although the variety is large, there is a tight family resemblance between all of them. They all have at least the following seven things in common: (1) they exist only online, (2) they are non-exclusive (meaning that everyone can partake), (3) transactions are made peer-to-peer, (4) a decentralized public ledger replaces the bank as middleman, (5) their value is partly derived from trust in cryptography instead of trust in a central bank, (6) algorithms regulate the creation of new units of cryptocurrency (called 'coins'), and (7) decisions on changes in the system are made in a decentralized way.[9]

It may be useful to repeat here that there are many so-called cryptocurrencies that do not fulfil these conditions, and that I therefore do not recognize as cryptomoney. And it should be clear to anyone that we have now decisively demarcated cryptomoney from other types of money, be it euro's or gold. It is not a physical kind of money, it is not backed by a (central) bank, there is no one organization in control. Instead, it is a completely online, virtual phenomenon, used and maintained by individuals and companies who trade directly with each other. Together they keep track of all of their transactions, which they record in a decentralized, public ledger. Their trust in the reliability, and incorruptibility of this ledger is a paramount reason why people want to use these cryptocurrencies. And this trust, in combination with the utility of this alternative money system, generates the demand that gives the different cryptocurrencies their value. No longer are banks needed to make the system function and, perhaps even more surprising, no longer are governments or central banks needed to guarantee the value of the money. This is revolutionary indeed, for ever since the abandonment of the gold standard (in 1971, although it had lost much of its use

[9] Apart from some other differences between our definitions, Jan Lansky excludes point (1) from his, probably because it is so obvious, but I think that is an important reason to include it.
Jan Lansky, 'Possible State Approaches to Cryptocurrencies', in: *Journal of Systems Integration* vol. 9.1 (2018) as found on: http://www.si-journal.org/index.php/JSI/article/view/335 accessed 22-04-2018.
For another definition, see:
David Lee Kuo Chuen (ed), *The Handbook of Digital Currency*, (Cambridge 2015) 7.
The Handbook proposes to treat cryptocurrencies as 'distributed and/or decentralized digital currency', but is very unsystematic in its usage of the term, sometimes being too vague, and other times too restrictive. For its definition of cryptomoney it draws heavily from:
Garrick Hileman, 'Alternative Currencies. A Historical Survey and Taxonomy', (01-03-2013) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747975 accessed 22-04-2018.

before) it had always seemed necessary that states backed their currencies. Cryptomoney, on the other hand, is only backed by its users and as a result puts itself outside the traditional system of money and finance. To see how that is possible, and explain why it can still function as money, we must look into the workings of these cryptocurrencies. If we do that, we will start to see where the seven conditions listed above come from, and why traditional money and cryptomoney are fundamentally different, and can never be made compatible (although they are exchangeable in one another).

§2. The workings of cryptocurrencies

Most cryptocurrencies can be deconstructed in four parts: algorithms, miners, users, and blockchain.[10] Every cryptocurrency starts with an algorithm that dispenses new 'coins'.[11] It usually gives these coins to 'miners', who secure the cryptocurrency by having their computers solve cryptographic puzzles. They do so voluntarily – there is no central organization that hires or commands them – in exchange for the coins they get. They can then exchange these coins with other users for goods, services, or other kinds of money. And while it is true that all miners are users, not all users are also miners. Users all have an online 'wallet' that holds their coins and is usually password protected. With the coins in their wallet they can trade with other users over the internet. All the transactions conducted by the users are then recorded in the 'blockchain', a public ledger. And truly *all* the transactions are recorded there. All transactions ever made by every user with this cryptocurrency. This enables everyone to calculate how much coins everyone else has.[12]

We now know how a cryptocurrency is structured. And from this structure follow some of the requirements for making the cryptocurrency work. There need to be users (who, as we have seen, need access to internet). Some cryptocurrencies, like bitcoin, have many, making it valuable and tradeable in many places. Others have virtually zero, making them worthless and useless. Another thing is that the algorithm needs to be fair and incorruptible. It needs to be fair, because no one is willing to adopt a cryptocurrency that randomly distributes

[10] Of all the most popular cryptocurrencies, only ripple is organized differently. The other main cryptocurrencies – bitcoin, ether, litecoin, bitcoin cash, eos, as well as many other small cryptocurrencies – all function more or less as explained in this section. At the time of writing – June 2019 – these types of cryptocurrencies make up at least four-fifth of the total market, and always have in the past. See for example: https://www.tradingview.com/markets/cryptocurrencies/global-charts/ accessed 12-06-2019.

[11] Most of the terminology used to describe cryptomoney, like 'coins' and 'miners', has originated within the bitcoin community. With bitcoin being the first – and still the most valuable – of all the cryptocurrencies, this terminology has spread, and is now used for most other cryptocurrencies too.

[12] Satoshi Nakamoto, 'Bitcoin. A Peer-to-Peer Electronic Cash System', (31-10-2008) as found on: http://nakamotoinstitute.org/bitcoin/ accessed: 02-02-2018.

coins, or favours specific persons or groups over others, and it needs to be incorruptible, because no one wants the founder of the cryptocurrency, or some hacker, to start directing all the newly generated coins towards themselves. Even the suspicion of the possibility of that happening could spell the end of a cryptocurrency. This is why the organizations of cryptocurrencies are decentralized, meaning that no one person or group of persons can change the algorithm on their own, and why the algorithms that govern the cryptocurrencies are open-source, meaning that anyone can see how they function. The last important thing is that the blockchain is incorruptible too. It is plain to see what kind of problems the system would run into if everyone could freely modify the ledger. Users could make coins disappear, or give everything to themselves, making the cryptocurrency worthless immediately.

To understand how cryptomoney is safeguarded against such fraud, it is helpful to go through a simplified hypothetical transaction step-by-step and, along the way, analyse the five security measures present in almost all the cryptocurrencies. Let us imagine a situation in which one person X wanted to send two coins of any cryptocurrency to another person Y. X would go online and enter the command: 'I give two coins to Y'. He would have to authorize this command with his password (the first security measure). The command now goes to all the miners that this cryptocurrency has. For them to add this command to the ledger, they have to solve a very complex cryptographic puzzle (the second security measure). The first one to do so adds the command to the ledger and immediately sends his solution and the updated ledger to all the other miners, who verify if the offered solution is correct (the third security measure). Often, as a reward, the miner who was the quickest with the solution gets a new coin of his own, specially created for this purpose. This method of processing commands – if we use the technical terms – follows a 'proof-of-work' protocol. The idea of this protocol is that it is very hard to initially solve the cryptographic puzzle, but that it is very easy for others to verify the soundness of the solution. Another check performed by the miners, is whether the user who made this transaction has enough funds (the fourth security measure). They do so by checking someone's entire transaction history. If the two coins that X tried to send to Y are one or two coins more than the sum total of all of X's transactions, he has insufficient funds and the transaction is cancelled. If the transaction passes all these checks, however, it is added to the ledger (thus making the transaction final and Y receiving his two coins) and everybody starts working from there. A new 'block' of information is added to the

already existing ‘chain’ as it were, hence the name blockchain for this constantly updated ledger.[13]

But how do the miners know for sure that they have the latest version? It is because they always work with the version of the ledger with the most blocks (the fifth security measure). As we have seen, the fastest miner to solve a puzzle gets to add a block. Let us assume that a hypothetical blockchain has 146 blocks. One of the miners cracks the puzzle and adds the transaction between X and Y as block 147. All the miners verify the validity of this block and continue with a blockchain with 147 blocks. It is not impossible, however, for a miner to continue to work on a puzzle that is already solved by someone else. He could solve this puzzle again, and in such a way create a block that contains information that is already in the ledger. But because our miner is behind with his solution, as he is still working on the block directly following 146, his new block would also get number 147. If he now sends his updated ledger to the other miners, they will note that they are already working with a blockchain with 147 blocks and they will automatically reject this ledger, because it is not really an update after all. This ensures that no transaction can ever be processed twice.[14]

Explained in simple terms, it comes down to this: if two people make a transaction, they have to record it in the (online) public ledger. Or, put differently: because nothing physical changes hands, the amendment in the public ledger is the transaction. Strictly speaking, cryptomoney is nothing more than information about transactions recorded in the blockchain. After every transaction the updated ledger gets sent to the miners. For them to make the update permanent, they have to solve very complex cryptographic puzzles. Once they have done that, the transaction is added to the ledger, and it can never be undone. That is to say, this is how it works if everyone has the best intentions. It is insightful to take a closer look at what happens when someone tries to cheat the system, because seeing how difficult that is also helps to understand why cryptomoney can command our trust in a way that hitherto only central banks could.

§3. Fraud in the blockchain

Imagine that malevolent agent Z tries to corrupt the ledger. Z could not pose as someone else and transfer money to himself because he does not have the password of another wallet than his own (although he could start stealing them, like any other password). Z can also not make

[13] Lee (ed), *The Handbook of Digital Currency*, 392-397.
[14] Idem.

transactions with money that he does not have, since every time someone makes a transaction it is checked whether or not he or she has sufficient funds. Creating money is also not an option, as the history of all transactions is complete and incorruptible. So, coins were either transferred to Z, or he earned them by mining. A coin with neither of these two backgrounds is therefore immediately caught out as being fake. The only chance for Z is to mess around with the blockchain. As noted before, Z cannot make false transactions, but he can try to make a valid transaction with the same money more than once. This is called the 'double-spending problem'. It sounds strange, and it is in fact a type of fraud that is quite unique for virtual money. It works like this: Z buys a nice car with his cryptomoney. He makes a valid transfer to the car company and they send him his car. After he receives the car, he must make it look like he never spent the money in the first place. To do that, he needs to cheat the blockchain.

The only possibility for cheating lies in the fifth security measure, the one concerning the length of the blockchain. As explained before, Z cannot add an already existing block to the blockchain again. If there is a block 293 that says he spent the money on the car, he cannot make another block 293 that says he did not spend that money, because it would be rejected by the other miners. Still, that is exactly what he is going to do. For his plan to work, Z will need to craft a longer blockchain than the existing one and send it to the other miners. Because it is longer, they will accept it and take it to be the true blockchain. So, what Z does, is perform the transaction where he buys the car and let other miners add it to the blockchain. At the same time, he makes another block that says he did not spend that money. However, he does *not* send that block to the other miners, so it will not be rejected and for the time being only exists on Z's computer. And while he waits for the car, he tries to keep adding the same blocks to his own corrupted blockchain as the faithful miners do to the public, true blockchain, but without sending any of these updates to the others.

When his car arrives, he can put his plan in motion. If everything worked out as planned, Z now has a blockchain identical to the one all the other miners use, with one difference: block 293, that contains the money transfer to the car store in the public blockchain, contains a different transaction in Z's blockchain (perhaps a very insignificant money transfer to a friend). All the blocks before and after block 293 are identical between the two blockchains. Let us assume that while Z was waiting for his car, 20 more blocks were added to both blockchains. All Z now has to do is find the 21st faster than anyone else and add it to his corrupted blockchain. But this time, he *does* send the update to the other miners. It is the longest version of the blockchain (because he solved the new puzzle first) so they

will review it. All the cryptography will check out, because Z has been solving the puzzles of the 20 blocks since block 293 correctly. And because he made identical blocks to the public blockchain, no issues with insufficient funds will arise. So, probably without even realizing it, the other miners adopt this version of the blockchain and continue from there. The only difference is that Z now has a brand-new car and the car store has not gotten any money. In fact, because the coins are not physical and cryptomoney is nothing more than the record of these coins in the blockchain, it is like the car store never even had the money in the first place. And since all transactions are final (unless you play the system like Z), the car store can turn to no one for help or reimbursement. Z, at the same time, can start spending the coins he retained again somewhere else ('double-spending').[15]

This sounds very easy to do, and makes cryptomoney look quite vulnerable to fraud, but in reality, it is really hard to execute a scam like this. The reason for that is the cryptography that encrypts every block. The puzzles are extremely difficult to solve and require a lot of computing power. So not only do you need a lot of that, the fact that the first to find a solution gets to add a block to the blockchain, also means that there is a race for every block. That is not a problem if you are a miner who is satisfied with finding one solution in every hundred attempts. But if you, like Z, want to keep up with the blockchain by adding blocks to your own, hidden blockchain, you will always have to be at least as fast as the fastest of all the other miners. And for the last block, 21 in our example, you will have to be faster than the fastest, so you become the fastest yourself. In practice, this means that you will need more computing power than all the other miners *combined*. This is why it is also popularly called a '51% attack' (because you would need more than half of all the computing power).[16] And apart from the enormous investment in computer systems this requires, you also need the electricity to power these machines. The currently largest cryptocurrency, bitcoin, was reported in July 2018 to use as much energy as the whole of Ireland.[17] Getting to use that much power is not only a question of money, but also of having access to an enormous power source, like your own nuclear reactor for example. Nonetheless, attacks like these do sometimes happen, although usually on blockchains of smaller and less valuable

[15] Usman W. Chohan, 'The Double Spending Problem and Cryptocurrencies', (19-12-2017) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174 accessed 18-04-2019.
[16] Tom Rodgers, 'Ethereum Classic Price Roaring Just Weeks After 51% Attack', on: *Forbes.com* (08-04-2019) as found on: https://www.forbes.com/sites/tomrodgers1/2019/04/08/ethereum-classic-price-roaring-just-weeks-after-51-attack/ accessed: 21-04-2019.
[17] G.F., 'Why bitcoin uses so much energy. Its consumption is roughly the same as Ireland's', on: *Economist.com* (09-07-2018) as found on: https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy accessed: 14-09-2018.

cryptocurrencies because they have fewer miners and thus require less computing power to corrupt.[18] The name gives us a clear hint already, but it is really important for all cryptomoney that it is as safe as can be. Without that guarantee of safety, no one would trust the money, and it would never gain any value.

Now that we have a basic understanding of what cryptomoney is, how it works, and how it is protected against fraud, we can turn to the question of what this all adds up to. What advantages and disadvantages follow from these qualities? What would our financial system look like if cryptomoney reaches a size significant enough to transform our monetary markets? In what circumstances would it perform better than traditional money? And how would it be worse? Taking the four-part deconstruction of cryptomoney's workings from section two, together with the seven conditions for what sets cryptomoney apart from traditional money from section one, we will in chapter two explore what sort of impact cryptomoney could have on states, corporations, and individuals.

[18] Primavera De Filippi, 'A $50M Hack Tests the Values of Communities Run by Code. The Ideal of a Perfectly Trustless Technology is Nothing More than an Ideal', on: *Motherboard.Vice.com* (11-07-2016) as found on: https://motherboard.vice.com/en_us/article/qkjz4x/thedao accessed: 09-09-2018.

Chapter 2

What would a financial system based on cryptomoney look like?

§1. Cryptomoney's advantages

So, why do people find cryptomoney appealing? If we know that, we will better understand why states may have to deal with the effects of cryptomoney, even if they themselves try not to engage with it. In doing so, it will become clear why there may be a conflict of interest between individuals and states when it comes to adopting cryptomoney. Many arguments in support of cryptomoney have been given by its proponents, and additional ones can be inferred by simply looking at the conditions that need to be fulfilled for something to be called a cryptocurrency. Together, these arguments make for an impressive list of reasons why people will want to use cryptomoney alongside, or instead of, a traditional currency. Whether all of cryptomoney's supposed advantages will turn out as positive as its supporters hope, remains to be seen however. The changing role of banks, for example, means that cryptomoney users will no longer have to pay fees to a bank for safely storing their money, which will please most. Their money is now safely stored in the blockchain, where it cannot be touched by thieves. The downside to this system is clear, though. If someone were to lose his password, there is no one that can help him get his money back. But whatever some of the drawbacks are, the advantages listed below are still real:

1. Its online nature makes cryptomoney more accessible and easier to use than traditional money.
2. The decentralized nature of cryptomoney means that there is no one in control who can prevent anyone from joining or using it.[19]
3. Peer-to-peer transactions are potentially quicker than traditional ones that need to be processed by a bank, online server, or courier.
4. Cutting out the middle man (a bank or transfer agency) saves costs.
5. Any technical or formal obstructions to sending large sums to many different people are lifted.[20]

[19] Flamur Bunjaku, Olivera Gjorgieva-Trajkovska and Emilija MitevaKacarski, 'Cryptocurrencies. Advantages and Disadvantages', in: *Journal of Economics* vol. 2.1 (2017) pp. 31-39; p. 37.
[20] Lee (ed), *The Handbook of Digital Currency*, 23-24.

6. The nature of the blockchain makes thefts almost impossible. When thefts happen, it is almost never as a result of a compromised blockchain.[21]
7. Being decentralized is an insurance against the sudden disappearance of a cryptocurrency, as many people have a copy of the blockchain.[22]
8. The complete history of all transactions (recorded in the blockchain) makes it impossible to introduce counterfeit cryptomoney.
9. With some cryptocurrencies, it is possible to completely map all users and all their transactions. This can be used to combat illegal markets.[23]

With this last argument we are slowly shifting our focus from some pragmatic considerations to arguments based on more principled grounds. This second category is different from the first in that the validity of the arguments it contains does not rest on the question whether or not the projected advantages actually turn out to be advantageous, but rather on a subjective assessment of its value. It could be that cryptomoney turns out to be less practical than traditional money, but that people still choose cryptomoney over traditional money based on (some of) the principled arguments presented in this paragraph. In that situation there would be a trade-off between convenience and principles. So, let us see if these additional arguments are worth such a trade-off.

10. Cryptomoney gives an alternative means of payment to those that are dissatisfied with the (current) banking system.[24]
11. For libertarians, anarcho-capitalists, anarchists, and others who desire a small (or no) state, cryptomoney can be a tool to take power from governments.[25]
12. Governments lose much of their grip over currencies, which will please those who think that government interference hurts the economy.[26]

[21] Kate Rooney, '$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do', on: *CNBC.com* (07-06-2018) as found on: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html accessed: 10-09-2018.
[22] Bunjaku, Gjorgieva-Trajkovska and MitevaKacarski, 'Cryptocurrencies. Advantages and Disadvantages', 37.
[23] Lee (ed), *The Handbook of Digital Currency*, 21-22.
[24] Oscar Williams-Grut, 'One of the world's biggest banks just admitted bitcoin could destroy existing finance firms', on: *BusinessInsider.com* (06-07-2015) as found on: https://www.businessinsider.com/bnp-paribas-bitcoin-blockchain-securities-firms-redundant-2015-7?international=true&r=US&IR=T accessed: 07-07-2019.
[25] Ian Bogost, 'Cryptocurrency Might be a Path to Authoritarianism', on: *theAtlantic.com* (30-05-2017) as found on: https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/ accessed: 02-06-2019.
[26] Friedrich Hayek, *Denationalisation of Money*, (London 1976) 13-15.

13. Because the algorithms that govern the various cryptocurrencies are transparent, complete predictions can be made on how it will dispense new coins in all situations. This makes the initial distribution of cryptomoney more predictable than the traditional money governed by humans.[27]
14. Many cryptocurrencies have a supply limit.[28] When that limit is reached it is unlikely that these cryptocurrencies will see any inflation, which will appeal to those who think inflation is bad.[29]
15. Cryptomoney would eliminate some restrictions placed on what you can do with your money, as you can spend your money on everything, everywhere.[30]
16. Modifications to the code and/or algorithm behind cryptocurrencies are made in a decentralized way. Everyone can propose an alteration, and all the other users can then decide to adopt the new version of the currency.[31] Depending on the cryptocurrency, voting power may be differently distributed (not all users necessarily get the same amount of votes in all cryptocurrencies), but the pool of people who can make direct changes to the way a currency is governed is likely to be much larger than in the traditional system. And if you do not agree with certain changes, you are always free to move to another cryptocurrency. Some have argued that this makes cryptomoney much more democratic than traditional money.[32]
17. Although some cryptocurrencies are completely transparent (as was noted at point 9), some other are completely anonymous.[33] This offers more privacy than most other types of monetary transactions.[34]

---

[27] It does, of course, not make it easier to predict the price of a cryptocurrency, as that is subject to market forces.
[28] Some of the bigger ones are bitcoin, bitcoin cash, eos, litecoin, cardano, and tron. Some others (like monero) have a supply cap but will continue to dispense a fixed, very low amount of coins after this cap is reached, to prevent deflation in the currency, which could be economically devastating.
[29] Hayek, *Denationalisation of Money*, 13-15.
[30] Sean Foley, Jonathan R Karlsen and Tālis J Putniņš, 'Sex, Drugs, and Bitcoin. How Much Illegal Activity is Financed through Cryptocurrencies?', in: *The Review of Financial Studies* vol. 32.5 (2019) pp. 1798-1853.
[31] Selena Larson, 'Bitcoin Split in Two, Here's What That Means', on: *CNN.com/business* (01-08-2017) as found on: https://money.cnn.com/2017/08/01/technology/business/bitcoin-cash-new-currency/index.html accessed: 02-03-2019.
[32] Josh Zerlan, 'Bitcoin as the Ultimate Democratic Tool', on: *Wired.com* (11-04-2014) as found on: https://www.wired.com/insights/2014/04/bitcoin-ultimate-democratic-tool/ accessed: 02-03-2019.
[33] Zcash and monero are examples. For Zcash, see:
Eli Ben-Sasson, Alessandro Chiesay, Christina Garmanz, et al., 'Zerocash. Decentralized Anonymous Payments from Bitcoin', in: *2014 IEEE Symposium on Security and Privacy* (2014) pp. 459-474.
Some others are somewhere in between transparency and anonymity. Bitcoin, for example, does not require users to identify themselves, but has a blockchain that discloses enough information to make it possible to deduce from it who is behind an individual wallet.
[34] Daniel Genkin, Dimitrios Papadopoulos and Charalampos Papamanthou, 'Privacy in Decentralized Cryptocurrencies', in: *Communications of the ACM* vol. 61.6 (2018) pp. 78-88.

All in all, a monetary or financial system based on cryptomoney would constitute a radical departure from the way in which monetary matters are currently organised. Of course, not all these arguments in favour of cryptomoney will turn out to be actually advantageous. Anonymous cryptocurrencies can facilitate illegal trade, and probably very few people want to replace states with anarchism, to name just two possible negative consequences of some of the supposed 'advantages' listed here. Nor is this list complete. But we have compiled enough arguments to see why cryptomoney could still be attractive to many people and ideological movements, even if it turns out to pose a threat to states' monetary policies. For some, that might even be the exact reason why they support cryptomoney. The fact that there are arguments in this list that can be contested (especially in the second category) does not mean that people will not believe them or use them to propagate cryptomoney. And when they do, and cryptomoney becomes more prevalent, its nefarious effects on states will become all too real. But before we get ahead of ourselves, let us see how states currently control traditional money, and what kind of benefits they reap from this monopoly.

§2. Cryptomoney is no state money

Important for our inquiry is to realise right away that money currently is always an institution under the auspices of the state. There is even a school of thought that claims that money has always been a state enterprise.[35] It is true that there have also been numerous more or less successful attempts to create local money but their influence on the economy, even the local one, is often negligible and needs no further discussion here.[36] It should be noted, however, that saying that money is a state enterprise does not mean that it is the enterprise of one and no more than one individual state. The euro, for example, is still a state enterprise, although it is under the control of several different states.

---

[35] The so-called Chartalists hold the opinion that money is by definition sanctioned by the state. They are embroiled in a longstanding debate with what is now known as the Catallactic school who assert that money has a spontaneous origin and was over the course of history integrated by states.
See for example: Zelmanovitz, *The Ontology and Function of Money*, 9-48.

[36] Local currencies (in the United States) are extensively discussed in:
Alan Thomas Schussman, *Making Real Money. Local Currency and Social Economies in the United States*, Ann Arbor 2007.
Leiden tried to launch the 'Leidse Zonnemunt' in 2013. The idea was that if a Leidenaar installed solar panels on his or her roof, he or she would get some 'zonnemunten', that were only redeemable in cultural institutions in Leiden. This would promote investments in solar energy, and introduce a local currency in Leiden. It never gained much traction. For more information see:
http://www.p-nuts.nu/nieuws/56ste-inzending-p-nuts-2013-leidse-zonnemunten-voor-leiden-cultuurstad/
(accessed 02-06-2019).

One of the most remarkable aspects of cryptomoney is, of course, that it bypasses the state. But just as states have gone through enormous transformations over the course of history, so has money. We could regard cryptomoney as the next step in a development towards increasingly abstract money, a process that was already described by Georg Simmel in his seminal *Philosophie des Geldes*, published in 1900.[37] In this book, Simmel describes how money becomes more and more abstract as society becomes more and more complex. His idea is that a more complex society will have a more abstract economy, with more abstract (financial) products, and as a result will develop a more abstract type of money through its progressing technology and institutions. The money we use, according to Simmel, reflects the sort of economy we have. It could be that cryptomoney is to the current globalizing economy what livestock was to a feudal lord, gold to an early modern dynastic state, and fiat money is to our current nation-states. If the largely agricultural feudal society measured its wealth in how much livestock one had, it may be that the current globalized society based on (internet) trade will relinquish the physical, national coins and banknotes and instead opt for a virtual, international type of money that exists only on the internet.

§3. Monetary tools of the state in the current financial system

One of the most obvious and most important results from not being produced by states, is that cryptomoney largely escapes state control. Would cryptomoney come to dominate financial markets, it would erode many of the tools governments have to exercise influence over society. The current monopoly over money gives states four main tools to promote their political ends. Political, because, as we said in the introduction, monetary policy (like any policy) is never strictly 'technical', and always aims to make real change to the lives of real people through the economy. These four tools are: seigniorage, macroeconomic management, political symbolism, and monetary insulation. A government with its own money can choose to use these tools, or not. They often do, and when they do, it is usually through the institution of a central bank that they do it. But more on banks in the next section.[38] Let us now first see what these tools entail.

The first tool is seigniorage. This refers to the difference between the production costs of money and its nominal value. As the former is much lower than the latter, this is in effect a form of income for the state. In practice, this is often used in two ways: by directly selling

[37] Georg Simmel, *The Philosophy of Money*, (London 2001).
[38] Dominick Salvatore, Thomas D. Willett and James W. Dean (eds.), *The Dollarization Debate*, (Oxford 2003), 140-144.

money (usually coins) and by exchanging money (usually banknotes) with commercial banks for bonds and assets of equal value. As the revenue made from these assets is usually higher than the cost to produce these notes, central banks can turn big profits this way.[39] Most of these profits then go to the state's budget.[40] An added benefit is that if a central bank creates more money than is in demand, it raises inflation and as a consequence decreases the value of the governments' debts.[41] There is a limit to these boons, however, because if a central bank prints too much, hyperinflation will be the result. The second tool, macroeconomic management, has to do with the impact that changes in the money supply can have on the economy. The theory is that if you give people money, they will spend it. This results in higher demand of various goods, which will increase production. That in turn might lead to higher employment, which will give people even more money to spend. This extra money needs to be printed by the government too, who profits from seigniorage again, and from a higher tax income too. In practice, people may of course choose to do all sorts of things with their money, but that does not withhold governments from trying to get them to spend by giving them (access to) money. The third tool, political symbolism, is derived from the sense of unity or pride that paying with the same money brings. Not everyone may have very strong feelings for their currency, but combine it with a flag, an anthem, license plates, etc., and you get a clear separation between 'us' and 'them'.[42] The fourth tool, monetary insulation, comes from the ability to have a different currency than other countries. It is a negative tool in the sense that the absence of it makes a country vulnerable. Having to rely on someone else's money means that you have no access to the three tools listed above. What is more, is that you have to maintain good relations with the country whose money you use, or else they might start manipulating your economy in ways that can potentially be very harmful.[43] For example, countries like France and Italy have been reported to suffer substantially from the loss of an independent currency. Although they still have a say in the macroeconomic management of their currency, and still profit from seigniorage, without their respective

[39] 'The Fed's profits. The other side of QE', on: *Economist.com* (26-01-2013) as found on: https://www.economist.com/finance-and-economics/2013/01/26/the-other-side-of-qe accessed 09-09-2019.
[40] As is explained on the website of the European Central Bank: 'Does the ECB make a profit?', https://www.ecb.europa.eu/explainers/tell-me-more/html/ecb_profits.en.html (16-02-2017) accessed 09-07-2019.
[41] The entry on: "inflation tax", in: John Black, Nigar Hashimzade and Gareth Myles (eds.), *A Dictionary of Economics*, (Oxford 2012) as found on: https://www-oxfordreference-com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-1598 accessed: 03-06-2019.
[42] Eric Helleiner, 'National Currencies and National Identities', in: *American Behavioral Scientist* vol. 41.10 (1998) pp. 1409–1436.
[43] Benjamin Cohen, *The Future of Money*, (Woodstock 2004) 20-24.

currencies to insulate them from their fellow eurozone members, their economies have started to lag behind the others.[44]

§4. The role of central banks

These monetary tools are so potent in fact, that most modern states have placed them outside of direct political control. The temptation to maximize the short-term use of the monetary monopoly could harm the long-term stability of the currency, and many countries have founded a central bank to protect the currency against the government. These central banks have been given powers of their own to carry out this task of controlling the national money. There are many, and they differ from country to country, but most central banks share some vital functions. Firstly, they control the money supply, and produce the physical coins and banknotes used by individuals and businesses alike. Secondly, they oversee and regulate the actions of commercial banks in the country. Thirdly, they act as lender of last resort. They will lend money to banks who do not have enough money in the vault to give everyone what they are entitled to get, which for example can happen in case of a bank run: a central bank can then jump in to make sure the bank does not go bankrupt. Fourthly, they set interest rates. This determines how much interest commercial banks must pay if they borrow money from, or deposit money with the central bank. Keeping these rates high means that it is profitable for commercial banks to deposit their money with the central bank. As a result, investments in the economy will drop. The total amount of money in circulation decreases, making money scarcer, which leads to a smaller amount of inflation (or even to deflation). This scarceness also leads to an increased value compared to foreign currencies whose central banks set lower interest rates. Decreasing the rates, on the other hand, gives commercial banks incentive to loan money from the central bank and invest it someplace where they can get a higher return. The money added to the circulation will generate inflation and make a currency cheaper compared to foreign currencies. This means that central banks play a large part in determining the exchange rate between the national currency and a foreign currency.[45]

Combined, these are powerful methods to align the economic performance with long-term and short-term political goals. These goals are not set by the central banks themselves, but by the governments that instituted them. Very basic goals include making sure there is

[44] Andre Tartar, Cindy Hoffman and Paul Murray, 'As the Euro Turns 20, a Look Back at Who Fared the Best. And Worst.' on: *Bloomberg.com* (28-12-2018) as found on: https://www.bloomberg.com/graphics/2018-euro-at-20/ accessed: 03-06-2019.
[45] Thomas Cottier (ed.), *The Rule of Law in Monetary Affairs*, (Cambridge 2014) 153-177.

enough physical money for people to use (function one), preventing the commercial banks from engaging in illegal or high-risk activities (function two), and safeguarding the entire banking system against collapse (function three).[46] Implicit in many central banks' goals is that they conduct an anti-cyclical budgetary policy. A prominent economic theory, first proposed by John Maynard Keynes, holds that an economy in trouble can be stimulated by creating money. The deficit created in the process can later be reduced when the economy has recovered. Although it is hard to prove validity of this large macroeconomic theory, it is still widely put in practice by central banks everywhere.[47]

Other common goals include keeping prices more or less stable with a small amount of inflation, promoting economic growth, and increasing employment levels. These goals are more often associated with central banks' fourth function. It is through the setting of interest rates that central banks can influence the amount of inflation of a currency. Low inflation (2% for example) strikes a balance between incentivising people and businesses to invest their money rather than hoard it, and at the same time not undermining people's faith that their currency will retain its value. It also helps to decrease the worth of the government's debts (the amount stays the same of course, but every year it is worth 2% less). Employers can profit from inflation too, as the wages they need to pay will also decrease in worth. This means that they will have more budget for hiring new employees, thereby increasing overall employment.[48] Other benefits can be achieved by manipulating the foreign exchange rates. Having a relatively high-valued currency means that imports are cheap and exports bring in a lot of money. But if another country produces the same goods and has a relatively low-valued currency, its products will be relatively cheaper and it will be able to export more, thereby undercutting the profits from the country with the high-value currency. The downside is, of course, that imports will be relatively expensive for the country with the low-value currency.[49]

---

[46] The entry on: "central bank", in: Black, Hashimzade and Myles (eds.), *A Dictionary of Economics*, as found on: https://www-oxfordreference-com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-379?rskey=6vyxNq&result=401 accessed: 06-04-2019.

[47] The entry on: "Keynsian economics", in: Black, Hashimzade and Myles (eds.), *A Dictionary of Economics*, as found on: https://www-oxfordreference-com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-1731?rskey=2dZ6Hc&result=3 accessed: 06-04-2019.

[48] Mike Berry, *The Affluent Society Revisited*, (Oxford 2013) 98-100.
The effect is temporary, however, because employees will usually demand an increase in wages when they start to feel the effects of inflation themselves.

[49] The entry on: "misaligned exchange rate", in: Black, Hashimzade and Myles (eds.), *A Dictionary of Economics*, as found on: https://www-oxfordreference-

If we review the monetary tools available to states, and the influence that central banks can exercise over economies, we can conclude that these are some serious powers. But all this could change, if people start to favour cryptomoney over traditional money. As we will see in the next two chapters, cryptomoney could put the current system under serious pressure. And if states' monetary institutions start to lose much of their power, they paradoxically may even be tempted to look to cryptomoney as an alternative. They should not, though, as in the next two chapters, I will argue why replacing traditional money by cryptomoney means giving up values worth way more than any type of short-term monetary gain.

com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-1989# accessed: 06-04-2019.

Chapter 3

Cryptomoney and the problem of national sovereignty

§1. The foundations of sovereignty

Cryptomoney might be advantageous to certain individuals. Although many of the arguments in support of cryptomoney presented at the start of the previous chapter might not hold up when seriously critiqued. But that is not the point of this inquiry. The final two chapters are devoted to constructing a normative judgment that condemns the large-scale use of cryptomoney, even if all the advantages listed above were real. This judgment is passed on cryptomoney because of its detrimental effects on national sovereignty and inequality. The latter will be discussed in the next chapter, the former in this one. The value of these two principles is more important than the more practical arguments in favour of cryptomoney, and therefore trumps any of them. In practice that means that we cannot discard them if we believe the world order should be just.

National sovereignty cannot be counted among the (almost) universally celebrated concepts like 'happiness', 'good will', 'eudaimonia', 'justice', etc. to name a few ideas from which countless numbers of prescriptive philosophies have been derived. Yet, it is the order that rules the modern world. Although its definition is by no means fixed, we can gain understanding by borrowing from Stanford's Encyclopaedia of Philosophy and state that sovereignty is 'supreme authority within a territory'. This definition contains three elements, as we will see. It is not the necessary form, as history shows us, but we need to go no further than the state to find the present-day embodiment of sovereignty. A sovereign state possesses authority, that is to say: it has a legitimate claim to obedience by its subjects. This authority, furthermore, is supreme: the sovereign state is at the top of the pyramid of authorities. Lastly, sovereign states wield this supreme authority over a certain territory. Their dominion is delimited by other sovereign states. This is the current picture of national sovereignty.[50]

If we remind ourselves of the well-known maxim that an is never implies an ought, we should not confuse the current state of territorial organization with the right one. National sovereignty has had many opponents over the years. The idea, originating with Jean Bodin, and expanded upon by Thomas Hobbes, that a sovereign is above the law and does not have to account to any human, has, rightly so, been gradually replaced with a slightly more

[50] Daniel Philpott, 'Sovereignty', in: *The Stanford Encyclopedia of Philosophy* (2016) as found on: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/ accessed 17-10-2018.

restrictive conception of sovereignty.[51] Most people tend to think that there are certain restrictions to what a sovereign state can and cannot do. In that sense, sovereignty is not absolute. For others, these amendments are not restrictive enough. They ask legitimate questions about whether sovereignty should be enshrined in states, or if perhaps there is some more legitimate type of sovereign conceivable. Others still, anarchists mainly, dispute the validity of sovereignty altogether, claiming that no person can wield legitimate authority over another.[52]

Valid as some of these objections are, sovereignty has certain advantages too. Hobbes cum suis did not sign away everyone's rights for nothing. At the heart of sovereignty lies the idea that it is a sensible principle on which to govern. Sensible, because it will benefit people. A sovereign state will likely be an improvement from a state of chaos and anarchy (often called the state of nature). For Hobbes this was even necessarily true, but others have pointed out that history holds countless examples of cruelties committed by sovereign states against their own people.[53] To overcome the problems of legitimacy that could arise because of these transgressions against the citizens of a state, it is now broadly shared politically (although maybe not philosophically) that a sovereign should rule in accordance with the people's will, an idea that originated with Jean-Jacques Rousseau.[54]

Now a rule in accordance with the people's will is something most can probably rally behind. If not in accordance with the people's will, then with whose? Even if we want a rule in accordance with, for example, a divine will, surely that can be instituted under the banner of the will of the people too. Still, that does not answer the question if sovereignty is also the right way to let this will rule. But it certainly is convenient in a number of ways. If we return to our definition of sovereignty, we can readily accept that the authoritative part makes sense if you want to transform any will into policy. That this authority should maybe not be absolute, but restricted by natural rights, human rights, private property, or some other unalienable aspect of human life that philosophers have defended over the years, is a reasonable limitation. But without any authority, cooperation between humans would be very difficult. We do not have to accept that without hierarchical relations we succumb to a 'war of every man against every man' – as Thomas Hobbes pictured – to still recognize that

[51] F.H. Hinsley, *Sovereignty*, (Cambridge 1986) 126-157.
[52] See, for example: Robert Paul Wolff, *In Defense of Anarchism*, (New York 1976).
[53] Christian Davenport, *State Repression and the Domestic Democratic Peace*, (Cambridge 2007) 33-44. History holds examples of cruelties against other states too, but these are acts that infringe on the sovereignty of the other state first, thereby already disqualifying themselves as acts committed under the banner of sovereignty.
[54] Jean-Jacques Rousseau, *Het maatschappelijk verdrag, of de beginselen der staatsinrichting*, (Amsterdam 2014).

humans find it hard to create consensus on a purely voluntary basis in groups numbering more than maybe a couple of dozen people.[55] If everybody accepts the same authority, however, we may be able to realize some common desiderata that make us all better-off.

The second element of the definition – supremacy – is a reasonable extension of the authority part. Once the agreement is reached that something or someone has authority over others, it would be inconvenient to assign this role to multiple institutions that are on equal footing. If the authority is accepted by the people under it, undermining this authority by creating a competitor seems confusing, inefficient, and even illegitimate. If we thus accept a supreme authority, we must further examine who fall under it. This is where the third element of the definition comes into play: territoriality. In the current political age, this is organized through states. There are other ways to make a divide between who falls under a certain authority and who falls under the next, and ethnic or religious groups have often been used as a demarcation line. But the state has proven to be the most efficient way to organize human societies. Whether that is good or bad is another matter, but the more basic fact that there are different territories that do not all share the same supreme authority is a logical result of historical challenges presented by the sheer size and diversity of humankind. For an authority to truly be supreme, it must be able to make all its subjects feel its presence. An all-encompassing sovereign might not be impossible in theory, but it is in practice. And although controversial for its possible intolerant consequences, dividing territory up between several different sovereigns also helps establishing a special bond between the sovereign and its subjects through the exclusion of others.[56]

If we thus conclude that a sovereign state is maybe not good in itself, but can be worthwhile because it manages to organize people in a way that helps them to turn their will into policy, we also have found a criterion to judge a sovereign by. The better he, or she, or it is at actualizing the people's will, the better the sovereign is. Again, you may think that there are restrictions to what a sovereign can or cannot do in regards to certain unalienable rights people may have. Or you may think that to be able to exercise its supreme authority over a territory at all, only (very) limited aspects of the people's will can be taken in consideration by the sovereign. Nevertheless, the sovereign state provides a foundation for human cooperation. So, it is through establishing a sovereign that people can try to exercise their will.

[55] Thomas Hobbes, *Leviathan*, (Oxford 1996) 68.
[56] Stephen D. Krasner, *Sovereignty. Organized Hypocrisy*, (Princeton 1999) 20-25.

It is true that not all states have a very good score when it comes to putting its people's will in practice. But certainly democratic regimes, where the sovereignty is exercised by the people through the institutions of government, have been proclaimed by many as the pinnacle of legitimate governance. Historically not uncommon is also the recognition of the 'benevolent despot' as a sovereign who rules its subjects in their best interests. Perhaps even more remarkable is the fact that governments – dictatorships so you will – that clearly do not rule in the best interest of its people, still often claim they do. As Sergei Guriev and Daniel Treisman show, dictators increasingly legitimize their claim to power by trying to convince their subjects that they are competent rulers, instead of terrorizing citizens into submission.[57]

In the end, most sovereign states derive their legitimacy from their citizens. Democracies clearly do so: the citizens authorize the states and they (indirectly) constitute the governing body themselves, making the electorate the sovereign. And often non-democratic states too rely on the people to legitimize their rule: benevolent despots by ruling according to the people's will and dictators by claiming to rule according to the people's will.[58] The importance of sovereignty then, lies in its capacity to transform the will of the people into policy. In order to do this well, a sovereign needs two things: a knowledge of the will of the people, and the policy tools that can put this will into practice. Non-democratic states often have problems with the first part, because they either do not care for, or have little understanding of the will of the people. This does hurt the legitimacy of their sovereignty, and therefore I will not spend too much time arguing why it is bad if cryptomoney undermined sovereignty in non-democratic states. It is much harder to defend these states' sovereignty if they cannot even sufficiently legitimize this sovereignty. Nonetheless, both democratic and non-democratic states will see the efficiency of their governance decrease if they lose access to certain policy tools. In so far as this governance is in accordance with the will of the people, this means that the power of the people will be eroded, and that they have fewer means to shape their lives and societies in the way they want to. This is why it would be bad if sovereignty was undermined.

[57] Sergei Guriev and Daniel Treisman, 'How Modern Dictators Survive. An Informational Theory of the New Authoritarianism', (02-03-2015) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2572452 accessed 09-03-2019.

[58] A true benevolent despot is more an archetype than reality, of course. No authoritarian leader does only good things for his or her subjects, but likewise, no dictator, cruel as he or she may be, does ever only do bad things for his or her subjects. That does not really matter, however, as both the dictator and the benevolent despot try to legitimize their rule in the same way.

§2. National money versus competitive money

With this inquiry into the nature of sovereignty in the back of our minds, we can return to cryptomoney and start to see why it will indeed undermine sovereignty. What lies at the heart of the inherent incompatibility of national sovereignty and cryptomoney, is that the latter is produced by the market. And what ultimately drives all market forces is competition. It is not necessarily so that market agents *want* to outperform their competitors, they *have* to. Being uncompetitive spells annihilation. Not immediately, but certainly eventually. As a result, market agents can only promise performance. But performance is measured in profit, economic growth, production etc. And maybe people want something else from their governments. That it guarantees their basic rights, for example, or promotes their well-being. Many proponents of 'competitive money' – i.e., produced by the market – fail to see that economic performance is not the most important variable for choosing what money we want to use.[59] This choice is based on other things too. On who gains and who loses power, or authority. On who becomes richer and who becomes poorer. So, as Benjamin Cohen said: 'economics may matter, but politics matters more'.[60] Where is cryptomoney in this picture? Well, cryptomoney is a form of competitive money. And it could be a very good one too. Currently, it is lacking in many fields deemed important to seriously challenge traditional money, but if the value of one or more cryptocurrencies stabilizes, it could rapidly start to outperform many traditional currencies. It may be worthwhile to examine why it can succeed as money where previous attempts have failed, in order to better understand why it is so fundamentally different from national money.

What always has been a problem for establishing competitive currencies is how to garner enough trust to make it function as money. Local money, of the kind used within a village, a neighborhood, or a small island, can exist because people know each other. The trust required there is not so much in the money, as it is in the personal relations these people have. Money to be used on a larger scale needs to be backed by something that can be trusted beyond any doubt. No person, organization, or corporation seems to fit the bill. If Deutsche Bank had started to issue its own money, it would have gained little traction before the last financial crisis, and would only provoke hilarity now. The blockchain is part of the solution to this problem. Because it is incorruptible, people want to store their money there. And the fact that it is decentralized means that people are not afraid that there is someone behind it all

[59] Zelmanovitz, *The Ontology and Function of Money*, 340-344.
[60] Cohen, *The Geography of Money*, 84.

who will run away with their money. These two simple ingredients make cryptomoney more trustworthy than any previous competitive money.

In chapter one, however, we saw that trust is not enough to give a currency any value. There needs to be demand for it too.[61] Agents in the market like predictability. Cryptomoney can theoretically provide that like no other. The algorithms that govern the cryptocurrencies give more certainty than any central banker could ever give.[62] The demand this generates is another reason why we should take cryptomoney seriously. But if there is demand, there must be supply too. And cryptomoney provides a very stable and predictable supply. More processing power means more coins, less power less coins, at an extremely reliable rate. And, more importantly perhaps, there are no geographic restrictions on where they can be mined. Take all these qualities together – the safety of the system, the predictability that attracts demand, the stable supply – and, for the first time in decades, we can see the emergence of a serious rival to states' monetary monopoly. In a – at the time – somewhat prophetic passage, Cohen stated the impact such an event could have on monetary institutions:

> In fact, the only real threat of competition on the supply side lies in the future – in the developing realm of cyberspace […] Around the world, entrepreneurs and institutions are racing to develop effective electronic means of payment […] If and when they succeed, governments will face a competitive challenge like none they have experienced in living memory […] Then their dominance of supply, not just demand, truly would be lost.[63]

He continues by giving an outline of what such an 'electronic means of payment' would have to look like initially, and what difficulties it would have to overcome:

> The key issue, as for all moneys, is trust: how to command confidence in the general acceptability of any sort of e-cash? Initially, at least, value is likely to be assured only by promising full and unrestricted convertibility into conventional legal tender. Later on, as *The Economist* has written, "it is possible to imagine the development of e-cash reaching [a] final evolutionary stage … in which convertibility into legal tender ceases to be a condition for electronic money; and electronic money will thereby become indistinguishable from – because it will be the same as – other, more traditional sorts of money"[64]

[61] Cohen, *The Geography of Money*, 154.
[62] Presently, no cryptocurrency has a stable enough price to be called even remotely predictable. But I am more concerned here with the role cryptomoney could play than with what it looks like today. And if we return to advantage 13 in section 1 of chapter 2, we will remember that the algorithms governing the different cryptocurrencies are completely deterministic, although that naturally does not mean that their price is completely predictable too.
[63] Cohen, *The Geography of Money*, 135.
[64] Idem.

It seems we have arrived at the future envisioned by Cohen. The elusive Satoshi Nakamoto can lay claim to being the first entrepreneur to develop an effective electronic means of payment when he launched bitcoin. As Cohen suspected, bitcoin (and other cryptocurrencies) are indeed easily convertible into 'conventional legal tender'. And at this point they would likely be abandoned if they would cease to be so. But as the alternative economy that uses cryptomoney grows, it will increasingly be able to stand on its own, without the requirement that it can be exchanged for traditional money.

Of course, we cannot know for certain now if cryptomoney will ever realize its 'final evolutionary stage'. But the combination of its algorithms and the blockchain technology give it an edge over other attempts to create a credible supply of money outside the jurisdiction of the state. And this is an impressive feat. Because although, superficially, phenomena like Donald Trump give a different impression, states are still among the most trustworthy institutions in human society. At the end of the day, what gives a currency its worth is that you and I both believe that government X will not disappear, appropriate all our savings, or create hyperinflation from one day to the next. With most non-state actors, we are usually not so sure. Cryptomoney may very well prove an exception to that rule. If you and I both believe that the algorithm governing the cryptocurrency is fair, and we both trust in the security of the blockchain, we have taken an enormous step towards general acceptance of this money. However, this will not be the money that we know so well. It is a form of competitive money that functions fundamentally different from traditional money. To see what this type of money will do to our sovereignty, we turn to the next section.

§3. Monetary tools and cryptomoney

Currently, there are some practical reservations, but what, essentially, stops us from converting all our money into cryptomoney? What can a government realistically do about it? Cryptomoney has already been called a 'super tax haven' and its utility no longer needs to be proven. Easily accessible and still out of the reach of tax authorities, it could become attractive even for people who never even thought about tax evasion.[65] And the increasing demand this could generate will lead to higher prices, making it more attractive as an investment. Like a runaway train picking up speed, there are many factors that, when a critical volume is reached, will all contribute towards accelerating the expansion of

[65] Omri Marian, 'Are Cryptocurrencies Super Tax Havens?', (05-07-2015) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863 accessed 12-04-2019.

cryptomoney. Stores will start to accept it, companies can pay their employees with it, international trade will pick it up, etc. And, as opposed to traditional foreign currencies, it will be hard for governments to combat the growing use. Which of course, for some people, makes it even more attractive.[66]

If and when this happens, cryptomoney would have a big impact on states' ability to conduct monetary policy. From the four monetary tools that flowed from the monetary monopoly of the state listed in the previous chapter, not many remain available to governments once they start using cryptomoney. Unable to print cryptomoney, the first tool, seigniorage, shifts from central banks to miners. States could start mining themselves, of course, but the fact that they now have to compete with others means that they will have a much smaller and less reliable source of income. Macroeconomic management, the second tool, also becomes less effective. Central banks can no longer artificially enlarge or shrink the amount of money at will. Mining amounts large enough to create inflation where there was none before will be too costly to be of any practical use. Because of that, the option to grow the economy by pumping newly created money into it disappears. In practice, this means that governments can only spend money on one thing, if they do not spend it on another. What happens to the third tool, political symbolism, is clear: it functions no longer. Maybe a global government like the United Nations can find some use in it, but for individual states, or monetary unions, the decentralized, online nature of cryptomoney simply renders it unsuitable to tie a political region together. The fourth tool, monetary insulation, can also no longer be maintained. Restricting the use of several currencies within a country is already quite difficult, restricting the use of several cryptocurrencies within a country seems impossible.[67] The money is not issued by the state, nor can the state affect its accessibility unless it wants to establish complete control over the internet in a country. Outright seizing cryptomoney is also impossible. Banks can be forced to handover the contents of someone's vault so to speak, except when these banks are outside of a state's jurisdiction. The blockchain, however, is outside of any jurisdiction, so although a government can try to force someone to give up his or her cryptomoney, they will not succeed without some form of cooperation from the owner. States will thus have to deal with the cryptomoney used by their citizens, and as a result of it become much more dependent on markets and on big financial actors for their monetary policy.

[66] Lee (ed), *The Handbook of Digital Currency*, 24-25.
[67] Cohen, *The Future of Money*, 11-14.

Central banks also lose a lot of their power. They no longer control the money supply as that is now in hands of algorithms. Influencing the exchange rate becomes much harder, as the price of the cryptocurrencies is determined by the actions of all its users combined. Although it is possible in theory to have a national cryptocurrency, the low exit costs mean that it would quickly be abandoned in favour of a more widely accepted, and thus more useful currency. Or in favour of one that has stronger deflation, as this makes people's money worth more over time. Such a process will eliminate most (national) cryptocurrencies, until only a small number – possibly just one – remain. This means that countries will usually use a currency that many other countries use too. Together with other players on the monetary market, they determine the price of the currency. As a result, the power of one state to influence this price will become much smaller. A final function that can no longer be efficiently provided by central banks is that of being a lender of last resort. Without the possibility to create new money they can only loan failing banks as much money as they have in stock at that point. And even the suspicion that that might not be enough would undermine the whole financial basis on which contemporary banking is funded.[68]

The legitimate question might be raised why governments would ever adopt cryptomoney if they know how disastrous the results would be. As long as it is an option not to use it, there seems no real danger in cryptomoney. But that seems slightly naïve, as cryptomoney is undermining states' monetary tools already. It facilitates tax evasion and illegal trade. And the more prevalent cryptomoney gets, the more serious these problems will become. At a certain point cryptomoney could even become so widely accepted that people start treating it like any other money, with no difference in people's perception between a dollar or a bitcoin. If that ever happens, the erosive effects on traditional currencies would be enormous. As we saw in the previous chapter, people can have a whole host of reasons to abandon traditional money in favour of cryptomoney. The effect this would have on traditional currencies might be so severe that maintaining one would become practically impossible. And once people realize that they might have been better off with their trusted, traditional money it might already be too late.

§4. Sovereignty under a cryptomoney regime

And so, we arrive at the question if we should want to relinquish control of monetary institutions and place them under the command of the market. Supporters of this proposition

[68] Michel Aglietta, *Money. 5,000 Years of Debt and Power*, (London 2018) 209-215.

usually point to the expected gains in stability and efficiency of such a move. National governments do not have a flawless record when it comes to monetary policy. Sometimes they just err, sometimes they even wilfully abuse their monetary powers. That is a serious problem, of course. Unfortunately – difficult as it is to predict the outcomes of macroeconomic decisions – it is not clear that the market would indeed perform better. Leaving monetary policy to the market, on the other hand, would probably also not lead to anarchy, and it could very well benefit the economy in certain situations under certain restrictions. However, market governance is clearly inferior to state governance in one important aspect: it undermines sovereignty. There is nothing in the promise of performance that the people can use to demand more well-being. People would lose the earlier discussed reality that sovereignty allows them to exercise their will. As long as their will coincides with the performance goals of the market, there may not be a problem in practice, but the market is not an extension of their will, as a sovereign would be (in a democracy at least). Politics, as a way for people to organize their community from within, is replaced by a technocratic institution. A market can succeed or fail to deliver performance, but it cannot be held accountable for aiding human well-being. Although markets do not exist outside of human society, the laws by which they govern are not devised by humans. Whereas a sovereign is a purely human institution, and as such part of us, markets are merely mechanisms used by us. Shifting power from sovereignty to markets is like giving up a part of ourselves.

Granted, people who live in a malign dictatorship might not care too much about this, as they already have very limited political tools to actualize their will, but even there the citizens would now no longer be able to hold the regime accountable if they suffer monetary related hardships. A regime without the tools to influence monetary policy is – even theoretically – unable to act on its subjects' will. Of course, if such a regime does not want to rule in accordance with the people's will, taking any policy instrument out of their hands might be a good thing. For people living under such regimes, it probably is a matter of degree and of individual preference whether they are willing to trade accountability of their government for possible economic gains. In many of the most desperate cases, this accountability already exists only in principle. Not in practice, maybe not even in name. In such a scenario, all considerations regarding national sovereignty are likely to go out the window, and that is of course no more than logical. The loss of sovereignty brought about by an increased use of cryptomoney can therefore not be said to be bad for everyone. Still, this is no reason for people who face dire political times in their home country to rally behind

cryptomoney, as in the next chapter we will see that there are other factors that make it improbable that they will benefit much, if at all, from cryptomoney.

Very different is the picture for the states where the people are not only ruled by, but form part of the sovereign themselves. People ruled by the hypothetical benevolent despot would see their government lose an important tool to promote their interests. And an even more fundamental impediment would be felt in democratic countries. As the electorate is the sovereign in a democracy, it would sign away essential rights by moving from national money to competitive money. Even more so, being the sovereign, the people would give up part of themselves if they place monetary institutions outside of their authority. They would lose some of the ability to determine their own government and future, and to shape the state in the way that they want. When the rule of parts of society that do have a major impact on people's lives is transferred to the market, this is at odds with the very notion of democracy itself. The sovereign people will no longer be able to turn their will into monetary policy, adding money to the long list of things that they already have no influence over. Removing such a central institution as money from the democratic realm seems a very high price to pay, even if cryptomoney would perform better than traditional money (and that remains to be seen),

As noted before, this study has started from the understanding that cryptomoney has a lot of potential, could become a serious alternative to traditional money, and as such could be a real threat to states' ability to conduct monetary policy. It should therefore not be considered too lightly. Not only would there be serious economic effects, but there are other, normative, things to consider too, as we have seen. For people in non-democratic states, the question is if they want to give up the accountability of their government in favour of (assumed) monetary improvements. But for democracies, cryptomoney poses a challenge to their core constitution as democracies. It seems that only libertarians or anarchists could reasonably want national sovereignty to be eroded as it has been described above. But, as we will see in the next chapter, that is not the last of the harmful effects that cryptomoney could bring.

Chapter 4

Cryptomoney and the problem of equality

§1. Equality between people and between states

Cryptomoney – as abstract as it sounds – is a real product. Many of the effects it could produce listed in chapter two were theoretical in nature, meaning that they probably will not work out exactly as described. The development of cryptomoney does not happen in a vacuum, after all. If it did, and if the homo economicus existed and all countries were exactly the same, we would not need this chapter. But cryptomoney has some inherent aspects that can have quite undesirable results in the real world. One of the results it is likely to produce is inequality. Both between states and within them. The main reason for this is that cryptomoney is decentralized and produced by the market. Those in the market with the best information and most expensive computers can make an enormous amount of money and leave the rest far behind. That does not mean that people in the lower echelons of society would necessarily become poorer (although they might), but (high) inequality has negative effects of its own, regardless of how wealth is distributed in society. It makes people unhappier, could hamper economic growth, and most of us think it is unfair too.[69]

Equality – maybe unlike national sovereignty – is one of those things that most people think is good. We tend to think that as we are all humans, we all have the same rights and obligations. Although not necessarily the same, no one is better than someone else qua human. From this basic conception flows the popular idea that if we are all equal, we also should enjoy the same opportunities to excel in our humanhood, or to become who we want to be. And that is where opinions start to diverge immensely. Because what does it mean to have the same opportunities? And what kind of opportunities do we need? It is easy to recognize differences in capabilities between people. But if we are equal, does that mean we should compensate for those capabilities? Also, there are certain factors outside of people themselves that do matter in how they will end up. Their gender, place of birth, upbringing, education, social class etc. play an important role too.

[69] For inequality and the decrease in happiness that arises because it violates our ideas of fairness, see:
Ada Ferrer-i-Carbonell and Xavier Ramos, 'Inequality and Happiness', in: *Journal of Economic Surveys* vol. 28.5 (2014) pp. 1016-1027.
For inequality and economic growth:
Inyong Shin, 'Income Inequality and Economic Growth', in: *Economic Modelling* vol 29.5 (2012) pp.2049-2057.

Although there are many arguments that could be made here, this paper offers a view from a Rawlsian perspective, because it holds that, all other things being equal, choices affecting the way material goods are distributed should always favour the least well-off in society. This idea, also known as the 'difference principle', was put forward by John Rawls in a larger framework aimed at describing a just society. What seems fitting here, is that money is one of the easiest things to measure and compare. Much easier than other material things that can be distributed in society, like healthcare or good quality food. So, if we want to assess if using cryptomoney is a good idea for an individual society, the difference principle will prove very useful.[70] And although Rawls himself did not devise the principle to decide how goods should be distributed between different countries, others have taken his project in that direction.[71] Thomas Pogge, for example, has argued that there are no good reasons to use the difference principle only within national societies. He writes: 'Nationality is just one further deep contingency (like genetic endowment, race, gender, and social class), one more potential basis of institutional inequalities that are inescapable and present from birth. Within Rawls's conception, there is no reason to treat this case differently from the others.'[72] If we agree that all humans are equal, then – if we follow Pogge's line of reasoning – we have an obligation to consider everybody when making distributive choices. Pogge is quite a bit more radical in what he advocates, but at the very least this more universalistic approach subscribes to the notion that (people in) one state should at least try not to make things worse for (people in) other states. From that perspective, cryptomoney is a bad idea.

§2. Cryptomoney and inequality through initial creation

There are two main aspects of cryptomoney that are likely to lead to inequality within states. The first has to do with how the coins in most cryptocurrencies are created; the second with a loss of redistributive power of governments. Let us start with the first. Cryptocurrencies usually have no value when they are first designed. Those that are pegged to an existing currency do, but they are strictly speaking not cryptocurrencies, merely virtual forms of money.[73] All real cryptomoney has to prove its worth first. Getting from being worth nothing

[70] John Rawls, *Justice as Fairness. A Restatement*, (Cambridge 2001) 42-43.
[71] Michael Blake and Patrick Taylor Smith, 'International Distributive Justice', in: *The Stanford Encyclopedia of Philosophy* (2015) as found on: https://plato.stanford.edu/archives/spr2015/entries/international-justice/ accessed: 11-06-2019.
[72] Thomas Pogge, *Realizing Rawls*, (Ithaca 1989) 247.
[73] Facebook's new coin, the libra, is one of the examples. They are more aptly called 'stablecoins'. Tom Wilson, 'Explainer. 'Stablecoins' in the spotlight as Facebook unveils Libra cryptocurrency', on: *Reuters.com* (18-06-2019) as found on: https://www.reuters.com/article/us-crypto-currencies-

to being worth something is the hardest step for any cryptocurrency. And unlike traditional money, that is struck in a mint, or gold that is mined with a pickaxe, cryptomoney needs computer processing power to come into existence. Some need relatively little, as, for example, they automatically generate a certain amount that is dispensed at predetermined intervals or start out with a fixed amount. But since at least three-quarters of the total capital volume of cryptocurrencies is based on the proof-of-work system – and thus requires the crypto kind of mining – usually quite a lot of processing power is involved.[74] Of this processing power, the sum of the individual miners' attempts to solve the cryptographic puzzles needed to add blocks to the blockchain makes up the lion's share. If that power is too costly relative to the value of the coins, nobody will want to mine.

Generally speaking, it is quite easy to mine the first couple of coins of a cryptocurrency. The reason why it is easy, is that the cryptographic puzzles safeguarding the system are still relatively simple.[75] This means that if you manage to mine a lot of coins in this early stage, and they later become valuable, you could get very rich. The anonymous founder of bitcoin, Satoshi Nakamoto, for example, presumably is in possession of at least half a million bitcoins that he mined at the very start of the currency. At that time, all of them combined were worth maybe a couple of euros, but if he sold them now it would make him a billionaire.[76] And although it is virtually impossible to predict the future price of bitcoin with any certainty, it could very well increase a hundredfold if it were ever to become more than a speculative toy. This would make Nakamoto, and possibly some other people who got in at the right time, as rich as anyone has ever been in the history of mankind.

To profit like Nakamoto did, we can see that you need two things: information and processing power. Information to know which cryptocurrencies might have a shiny future, and processing power to mine the coins of preference. Both information and processing power are not distributed within society equally, however. Hiring the specialized people to monitor what cryptocurrencies will do well, buying the computers to do the mining, and accepting that investments in certain cryptocurrencies will sometimes not turn out to be profitable, all require deep pockets. So, only someone who already has the capital to produce cryptocoins, can profit from the seigniorage that it brings. And these profits could be huge.

---

explainer/explainer-stablecoins-in-the-spotlight-as-facebook-unveils-libra-cryptocurrency-idUSKCN1TJ1T6 accessed: 19-06-2019.

[74] The trade volume of cryptocurrency is tracked by a website like: https://coinmarketcap.com for example.

[75] Nakamoto, 'Bitcoin', 3.

[76] Maxime Lambrecht and Louis Larue, 'After the (Virtual) Gold Rush. An Economic and Ethical Assessment of Bitcoin', [Advance publication 2018] 4.

Mine one cryptocoin for a few cents, and you will already have profited one cryptocoin minus the production costs. But an additional factor is the nascent state of cryptomoney we are in now. The value of most cryptocurrencies is currently nowhere near what it will be if cryptomoney becomes as widely accepted as traditional money. Early adopters could profit many times over in the future. Mine now, and you could get fabulously rich in five years.

If we recall the difference principle and apply it to the rise of cryptomoney, we can see that it is not the least well-off in society that profit from it, but that in fact it only exacerbates existing inequalities. What is more, is that it is not through a difference in capabilities that the different outcomes are produced, nor that cryptomoney does seem to further a higher, immaterial goal that would eventually benefit everyone in society. It is merely money creating money. The resulting distribution of wealth cannot be considered fair.[77] To make things worse, it will be difficult to compensate for these injustices, because – as we noted before – governments will lose important redistributive tools. In fact, as we will see in the next section, this loss will only increase inequality within societies, even if the problem of an unfair initial distribution could be somehow solved.

§3. Cryptomoney and inequality through tax evasion

The second problematic aspect of cryptomoney when it comes to a just distribution of wealth is that parts of it escape governmental control. States cannot produce it as easily as traditional money, and it is quite a bit harder to tax. This means that governments will not be able to correct injustices, should they want to. As we have seen before, the monopoly of central banks on the creation of money is lost with cryptomoney. Surplus seigniorage benefits that central banks add to the national budget disappear. Another handicap is the less effective monetary policy that is the result of the inability to create any amount of money at will. In so far as this policy is geared towards increasing employment and decreasing government debt, it weakens the position of the unemployed relative to the employed, and of governments relative to the governments' creditors. This already means that governments will have less resources to alleviate the worst of the inequalities.

[77] Naturally, there are people who will disagree. A famous critique of Rawls' theory was offered by Robert Nozick in *Anarchy, State, and Utopia*, (New York 1974). His 'entitlement theory' stipulates that a distribution of goods is just if these goods are rightfully obtained. So, if your capital was originally acquired in a rightful way, and you use it to mine cryptomoney, there is nothing unjust about it. I do disagree with Nozick, but the discussion concerning distributive justice is a much larger one, that is beyond the scope of this paper. For an overview of some of the important positions in this debate, I refer the reader to:
Julian Lamont and Christi Favor, 'Distributive Justice', in: *The Stanford Encyclopedia of Philosophy* (2017) as found on: https://plato.stanford.edu/archives/win2017/entries/justice-distributive/ accessed: 12-06-2019.

More serious, however, appears to be the problem of taxation. Compared to traditional currencies, it is quite a bit harder to tax most cryptocurrencies. The core problem is one of access. Governments will have a hard time finding out who owns what amount of cryptocoins, and even if they do, it will be difficult to confiscate the tax debts. Most traditional money is held and transferred through intermediaries, usually banks. A state can force a bank to disclose person W's possessions, and subsequently make the bank hand over to the state whatever it is that W owns in tax. Of course, in the current system there are ways for people like W to make their money 'disappear', but that does take some effort. With cryptomoney it is considerably easier to keep your money out of sight of the taxation authorities. If you do not voluntarily reveal your identity, initially no one will know that you are behind an online wallet holding cryptomoney. No longer able to ask banks for information, the taxation authority is then tasked with the considerable challenge to prove that it is you who is behind that wallet. Proving that may not be impossible, but the costs of doing so will be high, meaning that states lose a considerable amount of revenue.

Let us take income tax for example. If W's employer was to pay W in cryptomoney exclusively, W could fill in a sum on his tax return just large enough to not provoke suspicion. To catch W, the tax authorities would have to map parts of the blockchain and identify his wallet. If a certain wallet then showed transactions with W's employer, his local supermarket, and his (previously identified) mother, they would have reasonable ground to suspect that they had identified W's wallet. And that the five thousand coins W's employer sends W every month is his salary. But if W wants, he can make things much more complex for the tax authorities. We can envision a scheme in which W's employer enters into a payroll construction and sends the combined salaries of all employees to a third party in one large sum. Other employers may do the same. The payroll company then pays W and hundreds of others their wages out of this combined wealth.[78] What is more, W may have several wallets that all a receive a percentage of his salary. Some of these he uses for things that can be used to identify him, like paying his local supermarket and his mother. Others, however, he only uses to buy expensive electronics from China every once in a while. How are the tax authorities to know which of all the employers associated with this payroll company W works

[78] This is a simplified example of how a so-called 'mixing service' works. The effectiveness and reliability of these services varies greatly between different providers:
Ian Allison, 'Bitcoin Tumbler. The Business of Covering Tracks in the World of Cryptocurrency Laundering', on: *IBTimes.co.uk* (13-02-2015) as found on: https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480 accessed: 15-06-2019.

for? And how much W makes exactly? Although probably not impossible to find out, the amount of investigation needed to show that W is a fraud is considerable.

Difficult as this is for the tax authorities already, things get even more complicated if W would use a cryptocurrency specially designed to be untraceable. It is not necessary to discuss the technical details here, but there are cryptocurrencies with a blockchain that shows the minimum of information.[79] The only things disclosed in these blockchains is that at a certain time, a valid transaction has taken place. But it does not show who made the transaction, or how much coins changed hands. Still, this is not the end of the problems that states would face when collecting their taxes. Because if the tax authorities overcome all these obstacles and finally find out what W owes them, they would still need to come and collect it. Which is also not easy. Cash can be physically taken, and money in banks (within a government's jurisdiction) can be confiscated. Paying taxes in cryptomoney, however, requires W to transfer this money using his own password. If he does not want to do that, his money is absolutely unassailable. This again puts the state in the difficult position of having to find different means to get their hands on the taxes that are due.

All in all, cryptomoney is likely to make collecting taxes from people who do not wish to voluntarily pay them much harder. It will probably not prove to be impossible, as there might be strategies available to states that we do not yet know about. Things like value-added tax (VAT) may be much easier to enforce, and as long as people still need to convert their cryptomoney into traditional money, tax authorities could monitor the (online) exchange platforms to catch tax evaders there. A more radical approach would be to adopt a fully transparent cryptocurrency and raise its status to that of forced legal tender, meaning that the state prohibits the use of any other cryptocurrency within its borders. The state could then further stimulate the use of the only legal cryptocurrency by using it to pay all subsidies and welfare benefits. However, this will probably not prevent the rise of a large shadow economy that remains out of the reach of the tax authorities. It seems that there is still much to be said on the problem of cryptomoney and tax evasion. So far, legal scholars have not even reached consensus on how cryptomoney should be taxed.[80] How to then collect the taxes that are due is a whole different discussion, that we are only just seeing the beginnings of. The TAX3 Committee of the European Parliament published a study last year that reported:

---

[79] A nice and simple explanation of the principle underlying these cryptocurrencies is offered here:
Jean-Jacques Quisquater, Louis Guillou et al., 'How to Explain Zero-Knowledge Protocols to Your Children', in: *Advances in Cryptology — CRYPTO' 89 Proceedings* (New York 1990) pp. 628-631.

[80] See Aleksandra Bal's dissertation for a thorough exploration on this matter:
Aleksandra Bal, *Taxation of Virtual Currency*, (Leiden 2014).

> […] the EU framework that is in place on the exchange of information in tax matters, specifically aiming at combating tax evasion, is not very well equipped to address the use of virtual currencies for tax evasion, because to be able to share information on this, authorities must have the information in the first place, which is being complicated, if not made impossible, by the anonymity surrounding cryptocurrencies.[81]

Currently, there is the recognition that there may be a problem. But as cryptomoney is still quite a marginal phenomenon, there is no reason to panic yet. There may be a (technological) solution just around the corner. If there is not, however, we might be in severe trouble, as the incapacity to raise taxes will not only lead to an enormous increase of inequality, but will also undermine the whole functioning of the modern nation-states.

§4. Cryptomoney and setting foreign exchange rates

Inequality between people within a society is one thing, but cryptomoney would also increase inequality between states. This has mainly to do with the loss of the capacity to use the monetary tools listed in chapter two. Let us now assume that one is not at all concerned with the loss of national sovereignty that cryptomoney might inflict upon states. In that case, the loss of the capacity to utilize monetary policy by governments is not something to worry about in itself. But cryptomoney could also undermine the particular strategies of individual countries to cope with the unequal distribution of wealth around the world. Two of these main strategies are the setting of foreign exchange rates, and prohibiting (or promoting) the domestic use of foreign currencies. Losing those would result in a world where the balance between rich and poor countries becomes even more uneven.

The setting of exchange rates is a relatively simple tool. Imagine a situation wherein the central bank of country C used to sell one unit of its currency for four units of the currency of country K. Now, they start selling one unit for five units of K's currency. The exchange rate of country C's currency has now fallen. In practice, it might not be as easy as this example, and even if it is done with great care the outcomes may still differ within a margin, but it is a useful tool to some governments nonetheless. The exchange rate determines to a large extent how expensive imports relative to exports are. If country C made

[81] Robby Houben and Alexander Snyers, 'Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion', (2018) p. 70, as found on: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf accessed: 13-06-2019.

its currency worth less, as we saw in this example, its exports will become cheaper for other countries. At the same time, it will have to pay more for its imports. For country K, the opposite is now true (in relation to country C).[82]

Richer countries tend to favour stronger currencies. They usually produce high-value goods and services. Poorer countries like weaker currencies better, as they often supply raw materials and other basic products. The rationale behind this, is that production lines for high-value goods and services are not moved somewhere else that easily. They require expensive and specialist equipment for example, that is assembled locally to maybe serve only one specific purpose. Or very highly trained professionals are needed, who work together in highly specialized institutions. And because these goods are often in high demand, people will pay the price, whatever the value of the currency is. Raw materials, on the other hand, are not as hard to obtain somewhere else. If a stronger currency makes rice, or t-shirts, or coals, etc. more expensive in one country, there is probably another country that can also produce these goods. This is why it is then better to have a weaker currency, as the lower price you get per unit is more than made up for by the greater volume of units you can sell. Although the trick described above is a very common one, there are many more that can be used in the international money market to gain competitive advantages over rivals, or influence the domestic economy. Revaluating a currency makes pensions worth more, to name but one example. All of these tricks have their repercussions, though, and are not a magic tool to fix an otherwise broken economy. China is known to have devaluated its currency quite a number of times over the last couple of decades, to make its exports cheaper.[83] It was in such a position also because it had tight control over the money held by citizens; it did not have to fear ordinary Chinese exchanging their renminbi for dollars in any large numbers.

With cryptomoney, however, governments can be expected to lose all these monetary possibilities, as they have little control over cryptomoney. The principal problem is that the price of cryptocurrencies is largely decided outside of the power of a country. Without a monopoly on the money production, it is the market that will generate the price, based on supply and demand. States can try to influence the supply side a little, by putting more or less effort into the mining of new coins, but only the wealthiest countries can be expected to

---

[82] The entry on: "exchange rate regime", in: Black, Hashimzade and Myles (eds.), *A Dictionary of Economics*, as found on: https://www-oxfordreference-com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-1084?rskey=nFqEPm&result=9 accessed: 06-06-2019.

[83] Claus Zimmermann, *A Contemporary Concept of Monetary Sovereignty*, (Oxford 2013) 85-90.

influence the price of a cryptocurrency more than a little. Most states will simply not command a large enough percentage of the total resources devoted to the mining process. In chapter two, we already determined that the number of cryptocurrencies is likely to be rather small, as the low exit costs will mean that people will gravitate towards the most reliable and deflationary cryptocurrencies.[84] As a result, all international trade will be conducted with few cryptocurrencies, depriving the poorer countries of an important tool to protect their economies. This will increase the pressure to produce at ever lower costs, as it is no longer possible to make products artificially cheap by manipulating the foreign exchange rate. As a result, some poor countries may become even poorer. Richer countries, on the other hand, can profit from this situation, as the raw materials they import to fuel their own more advanced economies will become cheaper.

§5. Cryptomoney and prohibiting foreign currencies

Unfortunate as the loss of being able to set a foreign exchange rate potentially is, the situation would be made even worse by the inability to utilize the second strategy used by poorer countries to deal with monetary inequality: promoting or prohibiting domestic use of foreign currencies. Currently, currency substitution is already a problem for countries with weaker currencies. They often have trouble with enforcing the use of their own national currency within their own borders.[85] This mainly happens in countries who have trouble controlling their inflation. There, citizens prefer to use a foreign currency that preforms the basic functions of money a little better. This is in itself not so bad. For the people who manage to get a hold of a strong currency it is certainly better than seeing your savings disappear through inflation. For states, however, it is less than ideal, because issuing a currency that nobody uses is not helping anyone. Cryptomoney will make this problem worse and most countries will face a whole new level of currency substitution if cryptomoney makes an ascent.

Getting any kind of foreign currency is currently often not very easy and also not so cheap. Maybe for westerners it is, but for the people who want it the most it is not. Getting your hands on dollars is hard in Venezuela, Iran, or Chad. But if you want to keep your money out of the hands of the government, or do not want to lose it all through inflation, you

[84] Benjamin Cohen presents part of the discussion on the matter of how many cryptocurrencies will form an equilibrium:
Cohen, *The Future of Money*, 189-192.
[85] Cohen, *The Geography of Money*, 113-115.

might be willing to try a little harder to get hold of a more secure currency. In that case, cryptomoney might present an opportunity. Its online nature and the fact that it is outside of the direct control of banks and states makes it easily accessible to anyone who has an internet connection. If we put it in a broader perspective, however, this flow of capital from traditional money to cryptomoney puts a process in motion that might have unpleasant side-effects for everyone. Let us see how this process could play out.

The use of foreign currencies in a country could hitherto always be pushed back by making these foreign currencies illegal, and forcing companies and consumers to use the national currencies. Control over the supply of foreign money is never complete, but in all but the most fragmented states these measures ensure that the national currency dominates the domestic market. It is thanks to this, that something like devaluating the currency has any effect. Cryptomoney could pose a serious problem to the control states have over what currencies are used within their borders. The first countries where cryptomoney will get a foothold are clearly the more developed ones. People there have better access to information and internet, and plenty of time to study technological changes. We have seen this happen already. But the most practical use, initially, will be had by people in less-developed countries. They will now have an easily accessible alternative for the weak national currencies available. The demand for cryptocurrencies will cause higher inflation in the national currency, which generates an even higher demand for cryptocurrencies.[86] When cryptomoney is then in a position to rival the national currency, the economic insulation that the national currency provided starts to disappear. The government faced with an exodus of its national currency can no longer use its monetary tools. Devaluating currency A while everybody already uses foreign/cryptocurrency B does nothing. But not only do states lose economic insulation if they no longer have control over their money, they also lose political insulation.[87] Without strong central banks to regulate currency speculation, poorer states are virtually powerless against currency manipulations by the larger market agents, be it other states or financial institutions. The chances that some states will be completely dominated by foreign financiers is likely to increase if cryptomoney continuous its expansion.

In conclusion, we can say that cryptomoney will increase inequality in all sorts of ways. The first reason for that is the head start wealthier people, companies, and states have

[86] The entry on: "capital flight", in: Black, Hashimzade and Myles (eds.), *A Dictionary of Economics*, as found on: https://www-oxfordreference-com.ezproxy.leidenuniv.nl:2443/view/10.1093/acref/9780199696321.001.0001/acref-9780199696321-e-329?rskey=V0Csbn&result=1 accessed: 06-06-2019.
[87] Cohen, *The Geography of Money*, 44-46.

over their poorer counterparts. They can buy more processing power and hire expensive teams of financial specialists. This means that they can produce more cryptomoney, make better judgments on what cryptocurrencies will be successful, and reap large seigniorage benefits as a result. To correct inequality in societies, progressive taxation is one of the most used and effective tools. Yet cryptomoney, in all likelihood, makes it much easier to evade taxes. Being a decentralized peer-to-peer system, it is impervious to many of the enforcement mechanisms currently used by tax authorities. Inequalities between states will also be exacerbated. When the price of one or more cryptocurrencies stabilize, people in poor countries especially will have an incentive to trade their local currency for a cryptocurrency. When this happens, these countries can no longer set exchange rates to make their products artificially cheaper, and thus more attractive. They lose an important tool to protect their economies against the cruellest bouts of the international markets. It seems that little can be done to shield these vulnerable economies, as it will prove to be very hard to prohibit the use of cryptomoney. It can easily be purchased online and requires no further identification. The only way to combat this is for states to heavily censor the internet. But that too would be quite an unfavourable consequence of the introduction of cryptomoney. And whether it would work, remains entirely to be seen.

Conclusion

Cryptomoney is undoubtedly an interesting phenomenon. One of the first successful types of competitive money, it can rival governments current monopoly on monetary matters. But due to cryptomoney's erosive character, it seems destined to collide with national money sooner or later. Although we cannot know for sure how things will develop and whether or not a substantial mutation in cryptomoney will take place, we have seen that the different cryptocurrencies as they exist now will necessarily violate two normative principles that are too important to simply be discarded because of some other, more practical gains. It has been argued here that national sovereignty will be undermined, and that inequalities within, and between states will be exacerbated. Although not everyone may think these principles are all that important, they have been defended here in two separate manners.

National sovereignty was shown to be a human institution, that allowed people to turn their will into policy. Cryptomoney, on the other hand, was criticized for taking away some of these powers and replacing them with a technocratic mechanism aimed not at promoting people's best interests, but at performing well in the market. The material inequality that cryptomoney will produce was then condemned because it violates our ideas about the equality between humans. Siding with John Rawls, it was asserted that if we are equal qua humans, we must try to make changes in society only in so far as they improve the lives of those that are least well-off. Cryptomoney does not do that and instead favours the rich over the poor. Furthermore, with cryptomoney the poorer countries also lose important monetary tools that they could hitherto use to mitigate some of the worst effects of the unequal distribution of wealth around the world.

An interesting additional question that was not answered here is whether in the future we will in fact ever see a vehement clash between national money and cryptomoney. Trying to predict such a thing is largely a product of speculation, but that does not mean that we cannot start at the beginning and try to see the developments that are the nearest at hand. Thinking about these things – even if the claims cannot be substantiated with empiric evidence – may help us avoid the most obvious pitfalls associated with cryptomoney. So, how would cryptomoney make its ascent? At the start, it is mainly idealists and criminals that trade in cryptomoney. People who want to evade taxes and those who fear their national currency might implode join next. The increasing demand attracts investors. From an object of investment, it now slowly transforms to money proper. Some stores start accepting it. People and businesses start conducting non-illegal transactions with cryptomoney. This might

be the point where we are now. From there on, governments might start taxing it. That is not so easy, as they will find out. This presumably makes cryptomoney even more popular, through a sort of free-rider type problem. Now, employees want to get paid in cryptomoney, to avoid banks and tax collectors knowing anything about their salaries. Cryptomoney is now so stable and widespread, that it is completely accepted as a form of money, and starts to replace national currencies. First in international trade and finance and later in domestic use too. Semi-anonymous cryptocurrencies get mapped, so accounts get linked to individual people, making tax-evasion a whole lot harder. There might be a move toward fully anonymous cryptocurrencies. Governments now face an incredible loss of revenue. Adopting cryptomoney themselves does not repair this situation, so they issue laws that make their national currencies forced legal tender. Everyone now needs to pay in the national currencies. This does little to stop the use of cryptomoney, as token payments are being made in the official currency, while the largest cryptomoney cashflows stay out of sight.

This is a worst-case scenario to be sure. And if we ever reach this point, a number of things can happen, but what is certain is that much damage has then been done already. Now I do not want to give the impression that cryptomoney is some sort of force of nature that either is or is not, and is impervious to human will. We are the creators of cryptomoney and we continue to constantly adapt and mould it to our wishes. This means that we can change its trajectory based on where we feel it should go. Were it different, than this research would be able to pass no more of a normative judgment than it would on a hurricane, or an earthquake. Uncertain as the future of cryptomoney is, it has a number of advantages over traditional money, so it is at the same time not unthinkable that it will one day be as prominent as gold once was. Its current marginal status, however, gives us some time to think about whether we think cryptomoney can be good or bad, and as a result, whether we should foster or try to stop it. I opt for the latter.

Bibliography

- Aglietta, Michel, *Money. 5,000 Years of Debt and Power*, (London 2018).
- Allison, Ian, 'Bitcoin Tumbler. The Business of Covering Tracks in the World of Cryptocurrency Laundering', on: *IBTimes.co.uk* (13-02-2015) as found on: https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480 accessed: 15-06-2019.
- Bal, Aleksandra, *Taxation of Virtual Currency*, (Leiden 2014).
- Ben-Sasson, Eli, Alessandro Chiesay, Christina Garmanz, et al., 'Zerocash. Decentralized Anonymous Payments from Bitcoin', in: *2014 IEEE Symposium on Security and Privacy* (2014) pp. 459-474.
- Berry, Mike, *The Affluent Society Revisited*, (Oxford 2013).
- Black, John, Nigar Hashimzade and Gareth Myles (eds.), *A Dictionary of Economics*, (Oxford 2012).
- Blake, Michael and Patrick Taylor Smith, 'International Distributive Justice', in: *The Stanford Encyclopedia of Philosophy* (2015) as found on: https://plato.stanford.edu/archives/spr2015/entries/international-justice/ accessed: 11-06-2019.
- Bogost, Ian, 'Cryptocurrency Might be a Path to Authoritarianism', on: *theAtlantic.com* (30-05-2017) as found on: https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/ accessed: 02-06-2019.
- Bunjaku, Flamur, Olivera Gjorgieva-Trajkovska and Emilija MitevaKacarski, 'Cryptocurrencies. Advantages and Disadvantages', in: *Journal of Economics*, vol. 2.1 (2017) pp. 31-39.
- Chohan, Usman W., 'The Double Spending Problem and Cryptocurrencies', (19-12-2017) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174 accessed 18-04-2019.
- Cohen, Benjamin, *The Future of Money*, (Woodstock 2004).
- Cohen, Benjamin, *The Geography of Money*, (Ithaca 1998).
- Cottier, Thomas (ed.), *The Rule of Law in Monetary Affairs*, (Cambridge 2014).
- Davenport, Christian, *State Repression and the Domestic Democratic Peace*, (Cambridge 2007).
- Davis, Glyn, *A History of Money. From Ancient Times to the Present Day*, (Cardiff 1994).
- De Filippi, Primavera, 'A $50M Hack Tests the Values of Communities Run by Code. The Ideal of a Perfectly Trustless Technology is Nothing More than an Ideal', on: *Motherboard.Vice.com* (11-07-2016) as found on: https://motherboard.vice.com/en_us/article/qkjz4x/thedao accessed: 09-09-2018.
- Detrixhe, John, 'A dozen companies that reaped rewards by putting "bitcoin" or "blockchain" in their name', on: *Quartz (qz.com)* (12-01-2018) as found on: https://qz.com/1175701/putting-bitcoin-or-blockchain-in-a-company-name-is-sometimes-enough-for-a-pop-on-the-stock-market/ accessed: 18-04-2018.

- Economist, the, 'The Fed's profits. The other side of QE', on: *Economist.com* (26-01-2013) as found on: https://www.economist.com/finance-and-economics/2013/01/26/the-other-side-of-qe accessed: 09-09-2019.
- Ellsworth, Brian, 'Special Report. In Venezuela, new cryptocurrency is nowhere to be found', on: *Reuters.com* (30-08-2018) as found on: https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U accessed: 18-06-2019.
- European Central Bank, the, 'Does the ECB make a profit?', (16-02-2017) as found on: https://www.ecb.europa.eu/explainers/tell-me-more/html/ecb_profits.en.html (16-02-2017) accessed: 09-07-2019.
- European Central Bank, the, 'What is money?', (20-06-2017) as found on: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html accessed: 03-04-2018.
- Ferrer-i-Carbonell, Ada and Xavier Ramos, 'Inequality and Happiness', in: *Journal of Economic Surveys* vol. 28.5 (2014) pp. 1016-1027.
- Foley, Sean, Jonathan R Karlsen and Tālis J Putniņš, 'Sex, Drugs, and Bitcoin. How Much Illegal Activity is Financed through Cryptocurrencies?', in: *The Review of Financial Studies* vol. 32.5 (2019) pp. 1798-1853.
- Genkin, Daniel, Dimitrios Papadopoulos and Charalampos Papamanthou, 'Privacy in Decentralized Cryptocurrencies', in: *Communications of the ACM* vol. 61.6 (2018) pp. 78-88.
- G.F., 'Why bitcoin uses so much energy. Its consumption is roughly the same as Ireland's', on: *Economist.com* (09-07-2018) as found on: https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy accessed: 14-09-2018.
- Guriev, Sergei and Daniel Treisman, 'How Modern Dictators Survive. An Informational Theory of the New Authoritarianism', (02-03-2015) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2572452 accessed 09-03-2019.
- Hayek, Friedrich, *Denationalisation of Money*, (London 1976).
- Helleiner, Eric, 'National Currencies and National Identities', in: *American Behavioral Scientist*, vol. 41.10 (1998) pp. 1409–1436.
- Hileman, Garrick, 'Alternative Currencies. A Historical Survey and Taxonomy', (01-03-2013) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2747975 accessed 22-04-2018.
- Hinsley, F.H., *Sovereignty*, (Cambridge 1986).
- Hobbes, Thomas, *Leviathan*, (Oxford 1996).
- Houben, Robby and Alexander Snyers, 'Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion', (2018) p. 70, as found on: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf accessed: 13-06-2019.
- Krasner, Stephen D., *Sovereignty. Organized Hypocrisy*, (Princeton 1999).

- Lambrecht, Maxime and Louis Larue, 'After the (Virtual) Gold Rush. An Economic and Ethical Assessment of Bitcoin', [Advance publication 2018].
- Lamont, Julian and Christi Favor, 'Distributive Justice', in: *The Stanford Encyclopedia of Philosophy* (2017) as found on: https://plato.stanford.edu/archives/win2017/entries/justice-distributive/ accessed: 12-06-2019.
- Lansky, Jan, 'Possible State Approaches to Cryptocurrencies', in: *Journal of Systems Integration* vol. 9.1 (2018) as found on: http://www.si-journal.org/index.php/JSI/article/view/335 accessed 22-04-2018.
- Larson, Selena, 'Bitcoin Split in Two, Here's What That Means', on: *CNN.com/business* (01-08-2017) as found on: https://money.cnn.com/2017/08/01/technology/business/bitcoin-cash-new-currency/index.html accessed: 02-03-2019.
- Lee Kuo Chuen, David (ed), *The Handbook of Digital Currency*, (Cambridge 2015).
- Marian, Omri, 'Are Cryptocurrencies Super Tax Havens?', (05-07-2015) as found on: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863 accessed 12-04-2019.
- Nakamoto, Satoshi, 'Bitcoin. A Peer-to-Peer Electronic Cash System', (31-10-2008) as found on: http://nakamotoinstitute.org/bitcoin/ accessed: 02-02-2018.
- Nozick, Robert, *Anarchy, State, and Utopia*, (New York 1974).
- Philpott, Daniel, 'Sovereignty', in: *The Stanford Encyclopedia of Philosophy* (2016) as found on: https://plato.stanford.edu/archives/sum2016/entries/sovereignty/ accessed 17-10-2018.
- Quisquater, Jean-Jacques, Louis Guillou et al., 'How to Explain Zero-Knowledge Protocols to Your Children', in: *Advances in Cryptology — CRYPTO' 89 Proceedings* (New York 1990) pp. 628-631.
- Rawls, John, *Justice as Fairness. A Restatement*, (Cambridge 2001).
- Rodgers, Tom, 'Ethereum Classic Price Roaring Just Weeks After 51% Attack', on: *Forbes.com* (08-04-2019) as found on: https://www.forbes.com/sites/tomrodgers1/2019/04/08/ethereum-classic-price-roaring-just-weeks-after-51-attack/ accessed: 21-04-2019.
- Rooney, Kate, '$1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do', on: *CNBC.com* (07-06-2018) as found on: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html accessed: 10-09-2018.
- Rousseau, Jean-Jacques, *Het maatschappelijk verdrag, of de beginselen der staatsinrichting*, (Amsterdam 2014).
- Salvatore, Dominick, Thomas D. Willett and James W. Dean (eds.), *The Dollarization Debate*, (Oxford 2003).
- Schussman, Alan Thomas, *Making Real Money. Local Currency and Social Economies in the United States*, Ann Arbor 2007.
- Shin, Inyong, 'Income Inequality and Economic Growth', in: *Economic Modelling* vol 29.5 (2012) pp.2049-2057.
- Simmel, Georg, *The Philosophy of Money*, (London 2001).

- Tartar, Andre, Cindy Hoffman and Paul Murray, 'As the Euro Turns 20, a Look Back at Who Fared the Best. And Worst', on: *Bloomberg.com* (28-12-2018) as found on: https://www.bloomberg.com/graphics/2018-euro-at-20/ accessed: 03-06-2019.
- Williams-Grut, Oscar, 'One of the world's biggest banks just admitted bitcoin could destroy existing finance firms', on: *BusinessInsider.com* (06-07-2015) as found on: https://www.businessinsider.com/bnp-paribas-bitcoin-blockchain-securities-firms-redundant-2015-7?international=true&r=US&IR=T accessed: 07-07-2019.
- Wilson, Tom, 'Explainer. 'Stablecoins' in the spotlight as Facebook unveils Libra cryptocurrency', on: *Reuters.com* (18-06-2019) as found on: https://www.reuters.com/article/us-crypto-currencies-explainer/explainer-stablecoins-in-the-spotlight-as-facebook-unveils-libra-cryptocurrency-idUSKCN1TJ1T6 accessed: 19-06-2019.
- Wolff, Robert Paul, *In Defense of Anarchism*, (New York 1976).
- Zelmanovitz, Leonidas, *The Ontology and Function of Money. The Philosophical Fundamentals of Monetary Institutions*, (London 2016).
- Zerlan, Zerlan, 'Bitcoin as the Ultimate Democratic Tool', on: *Wired.com* (11-04-2014) as found on: https://www.wired.com/insights/2014/04/bitcoin-ultimate-democratic-tool/ accessed: 02-03-2019.
- Zimmermann, Claus, *A Contemporary Concept of Monetary Sovereignty*, (Oxford2013).