Dealing with hackers in a bitcoin trading model

Thesis by:	Wesley Opgenoort
Student number:	3048993
Supervisor:	Frank Bohn
Year:	2017-2018
Master:	Financial Economics

Contents

Introduction

Bitcoin has been introduced after the crisis in 2009, and is to date the most widespread used cryptocurrency in the world. In recent years, the number of bitcoin users and bitcoin trading volume has increased strongly, with a supply of more than 17 million bitcoins[1], a market cap of over 112 billion dollars at the time of writing and a value of over 6000 dollar per bitcoin (July 2018)[2]. This creates strong incentives for hackers to start hacking bitcoin exchanges, which is where most people store their bitcoins. In fact, evidence shows that bitcoin hacks are increasingly more common, with the hack of the large Japanese bitcoin exchange 'Coincheck' in January 2018 and the South Korean exchange 'Coinrail' in June 2018 as leading examples[3]. Due to the increased risk of hacking, the demands for safe storage of bitcoin or measures against hacking are increasing rapidly.

In this thesis I use three papers that either use a monetary exchange model that includes bitcoin, or adds hackers to a model to see how this influences the decisions of agents to use bitcoin. These are the papers by Hendrickson, Hogan, and Luther (2016) on government intervention to ban bitcoin use, Luther (2016) on whether bitcoin gains widespread acceptance, and Sauer (2015) that uses a model with hackers and central bank regulation to show under what condition agents use bitcoin. I use the framework by Hendrickson, Hogan, and Luther (2016) and add hackers in a fashion similar to Sauer (2015). Moreover, I add two measures that help agents to deal with hackers; a government tax and the option of buying private security against hacking. Using the extended model; I show a tax range that successfully bans hackers while agents are still willing to trade bitcoins. Also, I find that private security is more effective if the cost is of buying this security is lower, and that a higher tax level is more effective in banning hackers. Furthermore; I conclude that both measures supplement each other and that they are more effective if bitcoin holders have a large utility compared to producing agents.

[1] https://coinmarketcap.com/currencies/bitcoin/historical-data/. Accessed on 03-07-2018.
[2] https://coinmarketcap.com/currencies/bitcoin/#charts. Accessed on 03-07-2018.
[3] Other hacks can be found in e.g. this article: https://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck.

The remainder of this thesis is as follows: chapter 2 is a literature review, while chapters 3 to 5 are an in-depth explanation and discussion of the aforementioned papers. Chapter 6 shows an extended model that adds hackers to the model of Hendrickson, Hogan, and Luther (2016), and shows how useful two measures are in dealing with hackers. Further; chapter 7 shows the conclusions of this thesis, which is followed by the references and appendix.

Chapter 2: Literature review

Since bitcoin is developed by Nakamoto (2008) and launched in 2009; research on bitcoin has been done on several topics. These include regulatory issues (Trautman, 2014), the role of institutions (Evans, 2014), volatility (Donier and Bouchaud, 2015; Dwyer, 2015; Sahoo, 2017; Blau, 2018), and predictability (Moore and Christin, 2013). Furthermore, numerous studies have focused on whether bitcoin is a bubble (Godsiff, 2015; Cheah and Fry, 2015; Fry and Chea, 2016) and if bitcoin can be considered as money (Yermack, 2013; Bjerg, 2016).

Little is known however on the reasons for people to use cryptocurrencies, and in particular bitcoin. Some surveys are held (Bohr and Bashir, 2014; Yelowitz and Wilson, 2015; Presthus and O'Malley, 2017) but hardly any theoretical modeling is done in the literature. Exceptions are the papers by Luther (2016) on network effects and switching costs, and Sauer (2015) on hacking and central bank regulation.

Luther (2016) uses a model for currency acceptance, developed by Dowd and Greenaway (1993) and adapts this model by assuming adaptive expectations in a sense similar to the work by Selgin (2003). Furthermore, Luther (2016) adds switching costs to the model to show how a model with switching costs and network effects can explain the lack of widespread acceptance of cryptocurrencies like bitcoin.

Sauer (2015) uses a network model that is based on the model developed by Shy (2001). It is extended by hackers, which was previously proposed in the paper by Bartholomae (2013). Based on these papers, Sauer (2015) includes central bank regulation in a model showing that it is optimal for the central bank to abstain from bitcoin regulation, as long as the bitcoin network remains small and there are few agents that use bitcoin for speculation.

Research on modelling government transaction policies was first done long before the introduction of bitcoin. Aiyagari and Wallace (1997) and Li and Wright (1998) were the first to model government transaction policies. A matching procedure for trade in different currencies was first described in Kiyotaki and Wright (1993) with random matching. Models based on these transaction policies with random matching are found in Lotz and Rocheteau (2002), to see if these policies can support a new currency, and Waller and Curtis (2003) that show how these policies affect competing international currencies. Corbae, Temzelides, and

Wright (2003) were the first that used non-random matching ('endogenous search'), which means that agents could choose their trading partner instead of being randomly matched to another agent. Combining these elements; the paper by Hogan and Luther (2014) was the first to create a monetary model with endogenous search and random consumption preferences. The paper by Hendrickson, Hogan, and Luther (2016) builds upon the model used in Hogan and Luther (2014) by imposing a government transaction policy, similar to Aiyagari and Wallace (1997) and Li and Wright (1998), to find under what conditions the government can successfully ban or discourage bitcoin.

Chapter 3: The model by Hendrickson, Hogan, and Luther (2016)

Hendrickson, Hogan, and Luther (2016) use a model to consider the extent to which the governments can successfully ban or discourage bitcoin. The model of Hendrickson, Hogan, and Luther (2006) is an extension of the models of Kiyotaki and Wright (1993) and Corbae et Al. (2003). I start by explaining the basic structure and show how the model was adapted. I explain the model both in terms of intuition and mathematics. Thereafter is a discussion on the assumptions, mechanisms and relevance of the model.

3.1: Basic Structure

Hendrickson, Hogan, and Luther (2016) assume an economy with some random number of agents (A), shown as

$$A = [0, 1]. \quad (1)$$

These agents are divided in a random number of different types (G). Since each agent can only be of one type, the number of types is smaller than or equal to the number of agents:

$$G \leq A.$$

Each type of agent produces a different good. Since each agent of a certain type produces the same good, the number of products in the economy is equal to the number of types. It is assumed that goods are non-divisible and non-storable. This means that it is not possible to buy or sell any part of a good; only the entire good can be traded. Since goods are non-storable; goods must be consumed in the same time period. Hendrickson, Hogan, and Luther (2016) assume time is discrete and agents are infinite living. Note that the model only uses one time period, but works the same for multiple time periods.

Agents receive utility from consuming certain goods. Each agent of a certain type consumes several goods, called a subset of goods. The number of goods consumed (n) is the same for each type, but the exact goods that are consumed can differ per type. This means that each agent of a certain type has the same preferences for goods, and therefore consumes the same subset of goods. Agents of other types have other preferences and consume other goods.

The costs for *producing* a good (c) are assumed to be positive (c > 0). This means that there are always costs involved in producing, and when the gains from trade are low, an agent can have an incentive to not trade at all.

Consuming a good gives a certain level of utility (u) which depends on the costs of production (c) and on a discount factor (r), where r is the rate of time preference

$$u = \frac{c}{1+r} \tag{2}$$

The implicit assumption is that utility is larger from goods consumed that were more expensive to produce.

Since goods are non-storable, no storage costs are in place for goods. Money is storable however, and has some storage costs (ϒ), where ϒ = Storage costs per period of holding a coin, in terms of utility. So, larger storage costs make the value of a trade lower. Thereby lowering the probability that a trade takes place.

There is a random number of coins distributed over all agents. This number (M) is

$$M \in [0, 1] \tag{3}$$

which is smaller than the total number of agents, so M<A. This means that some agents in the economy have coins, while others do not. In fact, an agent has exactly one or zero coins in its inventory, since it is assumed that each agent can store at most 1 indivisible coin. Having a coin or not is shown as

$$z^i_t \in \{0,1\} \tag{4}$$

so, if z = 1 then an agent of type i (at time t) has a coin in inventory, and if z = 0, then it has not. So, the proportion of z=1 is equal to M, since M is the total number of coins in the economy.

All trading is bilateral, so trade only occurs between two agents. Trade can occur after two agents are matched. The only possible trades are between an agent with money (z=1) and an agent without money (z=0). Trade between two agents without money cannot occur, since it is assumed that goods can only be traded for money. Trade between two agents with money will not occur, since trading a coin for the same coin does not gain any utility whatsoever.

3.2: Non-random matching

It is assumed that matching is non-random[4], because agents can choose with agents of which type and with which inventory ($z^i_t = 0$ or $z^i_t = 1$) they want to trade. Then, they get a random draw from this type with the chosen inventory, and from that draw they match an individual that is willing or not willing to trade[5].

Hendrickson, Hogan, and Luther (2016) assume that the number of agents with money was equal to M, while the agents without money equals all other agents minus those holding money (so 1-M). However, we do not know the actual number of agents having money, so there are two possible outcomes: M<1/2 or M>1/2.[6] If M<1/2: there are less agents with money than agents without money. Therefore, every agent with money will match an agent without money (since they have an incentive to trade and will therefore always choose to match an agent with money in its inventory). The number of agents without money that matches one with money, is equal to

$$a^e_0 = \min\left(\frac{M}{1-M}, 1\right) \quad (5)$$

The superscript ^{e} stands for "endogenous[7]" meetings. The subscript $_0$ indicates that it is about agents without money. If M>1/2: there are more agents with money than without. So, each agent without money is matched with an agent with money. Agents with money are matched with a moneyless agent with a probability of

$$a^e_1 = \min\left(\frac{1-M}{M}, 1\right) \quad (6)$$

where the subscript $_1$ shows that it is about money holders.

[4] In Kiyotaki and Wright (1993) and Corbae et Al. (2003) random matching was assumed.
[5] So e.g. they want to trade with an agent of type i that has money (z=1). Then, from all agents of type i that have money, they get a random draw. Once they are matched with such an agent, both agents must choose if they want to trade.
[6] There are actually three options, since M=1/2 could also be possible. However, as shown later, this has (for now) the same implications as M<1/2, since every agent with money can match another agent without money.
[7] This means that agents can now choose the type of agent they want to trade with, instead of being randomly matched.

Once they are matched, both agents must indicate if they want to trade or not. If both want to trade; trade occurs, if one or both say no, there is no trade, and both will draw a new agent in the next matching round.[8]

There is a certain probability (π) that an agent without money wants to trade when matched to an agent with money. This depends on how much utility is gained from trading. For money holders, the value function is

$$rV_1 = a^e_1 (u + V_0 - V_1) - \Upsilon \quad (7)$$

This means that the discounted value for holding money (rV_1) is equal to the chance of being matched with someone without money (a^e_1) times the net gain from trade ($u + V_0 - V_1$), minus the storage cost of money (Υ). Note that u is the utility from consuming the good, and V_0-V_1 is the gain from switching from money holding to non-money holding[9]. For agents without money, this function is

$$rV_0 = a^e_0 (-c + V_1 - V_0) \quad (8)$$

where the discounted value for holding no money (rV_0) is equal to the change of being matched with someone with money (a^e_0) times the net gain from trade ($-c + V_1 - V_0$). This net gain is the gain from switching from non-money to money-holding (V_1-V_0), minus the costs of producing the consumption good (c). The assumption that there is some net gain from switching from non-money holder to money holder is key for trade to take place. This is further discussed in paragraph 3.4.

It is assumed that agents choose to trade in accordance to their value function. There are three possible outcomes for the probability that an agent without money wants to trade when matched to an agent with money (π). These are

$\pi = 1$ if V_1-V_0-$c > 0$ (everyone accepts money) (9)

$\pi = 0$ if V_1-V_0-$c < 0$ (no one accepts money) (10)

$\pi \in (0, 1)$ only if V_1-V_0-$c = 0$ (Some agents $\pi \in (0, 1)$ accept money) (11)

[8] This is in the next time period (remember that time is discrete and continues forever).

[9] Equation 4 shows that all agents can have either 0 or 1 coin in their inventory. After trading their coin for a consumption good, money holders now have 0 instead of 1 coin. Therefore, they are now non-money holders (producers) instead of money holders. The gain from such a switch is V_0-V_1.

Furthermore, Hendrickson, Hogan, and Luther (2016) assume that the money-holding agent gets a preference shock[10], where they only want to trade one good out of the subset that gains them utility. This shock is assumed to be random and determines which of the n goods in an agents' subset, the money-holding agents wants to trade for his money. The other goods in the subset will therefore not be traded, even if the non-money-holding agent wants to trade. So effectively; the probability of trading a good -after the matching process is over- is just one out of these n goods, or

$$\rho \equiv \frac{1}{\mathrm{n}} \tag{12}$$

where ρ is the probability of trading a good after the matching process is over. If the agent wants to consume, if can offer the type of money it has: bitcoin or currency. The agent without money can then choose to accept or not[11]. This assumption does little to the model, apart from making trade less likely overall. This is discussed further in paragraph 3.4.

3.3: A modified model with bitcoin

With the addition of bitcoin to the model; Hendrickson, Hogan, and Luther (2016) assume that agents now have three possible options: owning currency[12], bitcoin, or no money at all. Therefore, a fraction of agents is endowed with currency (m), a fraction with bitcoin (b), and a fraction with neither (1-m-b). It is assumed that agents can trade bitcoin and currency for goods, but bitcoin and currency cannot be traded vis-à-vis. This is a notable assumption, because it limits possible trade scenarios and constrains the model. This assumption is discussed in more depth in paragraph 3.4.

Further it is assumed that the fraction of currency and bitcoin holders combined (m+b) is smaller than 0.5, which means that the number of agents in the economy without a form of money is larger than the fraction of agents with currency and bitcoin combined. This is an unnecessary assumption, which is discussed further in paragraph 3.4.

[10] Actually, each agent gets a preference shock. However, if the agent does not have any money, this shock will not lead to a trade, since the agent can then only trade its produced good. So, the preference shock does not matter here.

[11] Agents accept neither money or bitcoin if the costs of producing a good is larger than the utility obtained from accepting current cy or bitcoin.

[12] This is assumed to be a type of money that is not bitcoin.

3.3.1: Probability functions

This implies that the matching probabilities change. For agents without money, the probability of being matched to an agent with currency becomes

$$a^{e}_{0,m} = \frac{m}{1-m-b} \tag{13}$$

where the subscript $_{0,m}$ indicates that it is a probability of agents without money ($_0$) matching agents with currency ($_m$). For agents without money, the probability of being matched to an agent with bitcoin becomes

$$a^{e}_{0,b} = \frac{b}{1-m-b} \tag{14}$$

where the subscript $_{0,b}$ indicates that it is a probability of agents without money ($_0$) matching agents with bitcoin ($_b$).
The probability that an agent without money is matched with another agent without money, and therefore has no chance to trade, is 1- $a^{e}_{0,m}$ - $a^{e}_{0,b.}$ This is simply 100 per cent minus the probability of meeting a currency or bitcoin holder.

Recall from paragraph 3.1 that an agent gains utility from consuming a subset of goods. The total number of goods in this subset is a random number (n). Hendrickson, Hogan, and Luther (2016) assume that agents can choose the type of agent that they want to be matched with. Since each type makes only one good, the agent can choose agents of those types that produce a good that is within the subset of goods that give the money-holding agent utility. So, the agent can be matched with agents that produce n different goods.

3.3.2: Value functions

Note that there are now two probabilities for accepting money: π is the probability that an agent accepts currency, and θ is the probability that an agent accepts bitcoin. The best response[13], given π and θ are shown as: Π(π) and Θ(θ)[14]. This is the decision on whether to accept the money offered or withdraw the offer. Now there are no longer two value functions,

[13] This is the decision on whether or not to trade.
[14] It is assumed that Π(π) = π, and Θ(θ) = θ. So, for best response; these terms can be used as substitutes.

but three: V_0 for those that hold no money, V_m for those holding currency, and V_b for bitcoin holders. These are

$$rV_0 = a^e_{0,m}\,\Pi(\pi)\rho\,(V_m - V_0 - C) + a^e_{0,b}\,\Theta(\theta)\rho\,(V_b - V_0 - C) \quad [15] \quad (15)$$

$$rV_m = a_m\pi\rho\,(U + V_0 - V_m) - \delta_m \quad (16)$$

$$rV_b = a_b\theta\rho\,(U + V_0 - V_b) - \delta_b \quad [16] \quad (17)$$

The value function for non-money-holding agents (equation 15) is twofold. The first term shows the probability of an agent without money to match an agent with currency ($a^e_{0,m}$) times the probability of the moneyless agent to accept currency, based on the best response Π given a fraction of agents that are willing to accept currency (π), times the probability that the currency-holding agent wants to trade (ρ), times the net gain from trading the good for currency ($V_m - V_0 - C$). The second term is the same as the first, but for probabilities of matching a bitcoin holder.

Note that equations 16 and 17 are similar to equation 8, since the discounted value for holding currency (rV_m) is equal to the chance of being matched with someone without money ($a^e_{0,m}$) times the net gain from trade ($U + V_0 - V_m$), minus the storage cost of currency (δ_m). The same holds for bitcoin[17].

3.3.3: Equilibria

Based on the value functions there are four possible equilibria.

1) A currency equilibrium where currency, but not bitcoin, is accepted in exchange
2) A bitcoin equilibrium where bitcoin, but not currency, is accepted in exchange
3) An equilibrium where both currency and bitcoin are accepted
4) An equilibrium where neither currency nor bitcoin are accepted

[15] This is the simplified form of this equation. The actual equation and the reason for simplifying it is shown in the appendix.
[16] Note that capital letters and small letters for u and c are used interchangeably in the paper. I follow the paper, therefore from paragraph 3.3.2 onwards, U is used for utility and C for production costs.
[17] Only then the subscript $_b$ is used instead of $_m$.

The first equilibrium is one where agents accept only currency. A trade only takes place if the best response is to trade. Therefore, the expected value must be positive (V_m-V_0-C > 0) or at least 0 so that some agents are willing to trade currency. This is the case in equilibrium if at least the threshold value of agents ($\pi = \pi^*$) wants to make the trade or that all agents do ($\pi=1$). Recall that Hendrickson, Hogan, and Luther (2016) assume that if more than the threshold number of agents accept currency, than all agents do. Therefore; $\pi=1$ if $\pi>\pi^*$. Bitcoin is not present in the equilibrium if the number of agents that accept bitcoin is below the threshold value. This is the case if the expected value of accepting bitcoin is below zero (V_b-V_0-C < 0), in which case nobody accepts bitcoin in equilibrium. Also, if the expected value is zero, but the actual number of agents that accepts bitcoin is below the threshold value, nobody accepts bitcoin in equilibrium. Therefore, the fraction of agents that accepts bitcoin must be below the threshold probability ($\theta < \theta^*$) in a currency-only equilibrium.

For a bitcoin-only equilibrium, the same reasoning applies as for a currency-only equilibrium. We need enough agents that are willing to accept bitcoin, so that the number of bitcoin accepting agents is equal to the threshold ($\theta = \theta^*$) or larger than the threshold, which means that all agents accept bitcoin ($\theta = 1$). Also, the number of currency-accepting agents must be below the threshold value ($\pi < \pi^*$) in an equilibrium without currency trading.

To have both currency and bitcoin trading in equilibrium; there must be sufficient[18] agents that accept currency and sufficient agents that accept bitcoin. So, both for currency and bitcoin it must be that the fraction of agents accepting money in trade is at least the threshold probability. So $\pi = 1$ or $\pi = \pi^*$ and $\theta = 1$ or $\theta = \theta^*$.

An equilibrium without currency and without bitcoin can only occur if there is a small number of agents willing to trade currency and a small number willing to trade bitcoin. This number must at least be lower than the threshold value to exclude trade from equilibrium, because otherwise everyone or some fraction were willing to trade. Therefore, it must be that the number of agents accepting currency is below the threshold value ($\pi < \pi^*$) and the number of agents accepting bitcoin is below the threshold ($\theta < \theta^*$).

[18] So at least the threshold value.

3.3.5: Government transaction policy

Hendrickson, Hogan, and Luther (2016) assume that governments have an incentive to prevent equilibria wherein bitcoin is accepted, because they can compete with government-controlled fiat currencies[19]. Therefore, the question raised by Hendrickson, Hogan, and Luther (2016) is whether governments can effectively ban bitcoin as a medium of exchange if everyone were willing to accept it. To answer this question, governments must in some way be represented in the model. Therefore Hendrickson, Hogan, and Luther (2016) assume that some fraction of agents are government agents -representing the government-, whereas the rest are private agents. So; these government agents can be used to execute certain policies on behalf of the government. Other ways for the government to be represented in the model, are discussed in paragraph 3.4.

It is assumed that trade is anonymous, so private agents cannot know that they are dealing with a government agent. However, we know from paragraph 3.2 that agents can choose the type of agent and the money holdings of these agents, which are observable. Therefore, a producing agent can choose to only match with agents that hold currency if they wish to transact in currency only. Vice versa, a producing agent can match with bitcoin holders if they want to transact in bitcoin.

To determine if the government can ensure an equilibrium without bitcoin, it is assumed that there is a policy in place where all government agents accept currency but refuse bitcoin.

So, there is a certain fraction of government agents in the economy:

$$\phi \in (0, 1) \tag{18}$$

and the rest (1- ϕ) are private agents. The probability that a government agent accepts bitcoin is θ_g and the probability that a private agent accepts bitcoin is θ_p. The probability that a random agent (of any type) will accept bitcoin is:

$$\theta = \phi\, \theta_g + (1- \phi)\, \theta_p \tag{19}$$

[19] Some possible reasons are given like restrictions on monetary policy (if bitcoin is used), potential seigniorage, and willingness to disable certain transactions (think of illegal activities).

which is simply the weighted average of the two probabilities; the fraction of government agents times the probability that they accept bitcoin, plus the rest of the agents times their probability of accepting bitcoin.

Further it is assumed that all private agents accept bitcoin (while all government agents refuse bitcoin). Hence: $\theta_p = 1$ and $\theta_g = 0$. Recall from paragraph 3.3.3 that if the number of agents is below the threshold value for bitcoin, nobody uses bitcoin in equilibrium. So, the government can successfully ban bitcoin in equilibrium if the number of agents accept bitcoin is below this threshold value.

Since all government agents refuse bitcoin, and all private agents accept bitcoin; the probability of accepting bitcoin can be rewritten as

$$\theta = 1 - \phi \tag{20}$$

So, the probability of accepting bitcoin is the same as the probability that an agent is a private agent. Therefore, there is a certain size of the government (number of government agents) that will lead to:

$$\theta^* = 1 - \phi^* \tag{21}$$

In order to successfully ban bitcoin use in equilibrium, the number of bitcoin users must be lower than the threshold value: $\theta < \theta^*$. This can we rewritten as $1 - \phi < 1 - \phi^*$, which in turn can be rewritten to $\phi > \phi^*$. So, to ban bitcoin from use in equilibrium, the fraction of government agents (ϕ) must be larger than the threshold value ϕ^*.

Equation 20 shows that the higher the number of government agents (ϕ); the lower the probability that bitcoin is accepted (θ), and the larger the probability that the acceptance is below the threshold value ($\theta < \theta^*$). This means that the government can succeed in banning bitcoin as a medium of exchange, if the number of government agents is sufficiently large. Note that if the number of private agents that accepts bitcoin is lower than 1, the probability of bitcoin being accepted (θ) falls as well, and there are less government agents needed to get the bitcoin acceptance below the threshold value.

3.4: Discussion of the Hendrickson, Hogan, and Luther (2016) model

In this paragraph I discuss the assumptions by Hendrickson, Hogan, and Luther (2016) and show how they affect the model, and what happens if there were different.

Hendrickson, Hogan, and Luther (2016) assume representative agents. As a result, agents are identical and so are the decisions they make. This is a strong limitation of the model, because this means that a change in one of the variables in the model, affects either all or no agents. It is not possible that a change has an effect on some, while others decide otherwise (unless agents are indifferent about two options). The assumption of representative agents is not in line with empirical evidence, and limits the analysis to threshold values for indifferent agents. Note that this assumption is also relevant for the extended model in chapter 6.

Another assumption by Hendrickson, Hogan, and Luther (2016) is that two agents cannot trade their goods vis-à-vis. If this were to be released, this would mean that it is less likely that agents are willing to accept currency or bitcoin, due to the storage costs of these coins compared to no storage costs for goods. This would imply that using money is no longer necessary due to the possibility of payment in kind[20]. In reality; transaction costs among other problems provide a strong incentive to use some form of money in trade, which might be a reason for the assumption that exchanging goods is not possible in the model. It could be interesting to release this assumption and make a model that includes e.g. transaction costs, but this is beyond the scope of this thesis. Releasing this assumption would not change the actual working of the model, since trading decisions are still based on value functions, but it would make calculating threshold values irrelevant since payment in kind were strictly preferred over payment in money. Therefore, there is only one possible equilibrium: nobody accepts money. When looking at monetary exchange, as in this model, the assumption that producers cannot trade to each other is therefore vital.

There is no explanation on why private agents want to have currency or bitcoin into their inventories. It is assumed that both monies are distributed at random over the population, and that they can be used to buy goods that will give the consumer of those goods utility. The only reason for agents to accept currency or bitcoin is that they can use it themselves for

[20] Exchanging one good for another.

buying goods in a next time period. How much they value this transition from being a producing agent to an agent with a money inventory is shown in the model by the difference between the value of having money (V_m for currency and V_b for bitcoin) and the value of not having money (V_0). If the value gained from this transition (V_m-V_0 or V_b-V_0) is larger than the costs of producing a good (c), then the money is accepted (as in equation 9). Note that the papers in the core model give no explanation on where this transition value is based on, just that there is some random value from switching to a different inventory. Also, there is no assumption made on any differences on preferences for currency or bitcoin. There is an implicit assumption that having money has a least some positive value. This is not specified in the papers, but a negative value for holding money and positive producing costs, implies that trade always leads to a negative expected value. In other words: if the value for having money

Apart from government agents, there are other ways for the government to be represented in the model and lower bitcoin usage. Possible ideas are; a transaction cost (tax) to be paid to the government, for each time bitcoin is traded. This makes the utility from trade lower for those accepting bitcoin or the bitcoin holder (depending on who has to pay the tax), which makes it less likely that bitcoin is accepted in trade. Another idea is to increase the costs of bitcoin storage, to such a level that the storage cost is higher for bitcoin then for currency. This has in essence the same effect as a higher transaction cost, but might be harder to monitor if private bitcoin storage is relatively easy. Further, it is possible to ban bitcoin and include a fine as punishment for using bitcoin. The government can that fine someone if they find out that they are using bitcoin, which is forbidden. In line with this paper, it would then be possible to calculate an optimal fine (threshold level) for which bitcoin is excluded from trade.

Hendrickson, Hogan, and Luther (2016) add a preference shock to the model. There is no explanation on why this preference shock is added to the model or in what way it is meant to improve the model. If we look at the effects; this random shock means that agents are only willing to trade one out of the possible n goods in their subset. If matched to an agent without this one good, trade does not occur. However, if an agent is matched to an agent that actually has the one good from the preference shock, an agent's decision to trade still depends on the value functions. Therefore, the assumption of the added preference shock does not change the model, it just reduces the probability that a trade takes place.

Chapter 4: The model by Sauer (2015)

Sauer (2015) uses a model to look at central bank incentives for regulating bitcoin in a network model that includes hackers. Sauer (2015) shows the optimal level of regulation for the central bank, based on the assumption that the central bank wants to reduce the number of bitcoin users.

4.1: Network users

The model by Sauer (2015) consists of three types of players: private agents, hackers, and the central bank. It is assumed that all agents are potential bitcoin users (η), where

$$0 < \eta \leq 1 \qquad (1)$$

All agents are willing to pay some amount to start using bitcoin, and hence joining the network, but the exact amount differs per agent. How much agents enter the bitcoin network depends therefore on their willingness to pay for joining the network. So, if a new person joins the network, its willingness to pay is lower compared to those with a higher willingness to pay, that already joined the network. The number of agents that join the network, is shown by x, where

$$x \in [0, 1] \qquad (2)$$

A larger x means that more people join the network. Note that only those agents have joined, that were willing to pay more than the cost of joining the network (ρ). Sauer (2015) assumes there is a cost involved with joining the network, but does not make it clear where this cost is based on. This might be a fee to buy bitcoins (e.g. transaction cost) or a cost of educating yourself on how to use and trade bitcoins. In any case; the cost is the same for each agent that joins the network, regardless of the number of bitcoin users.

The expected size of the bitcoin network (N^e) can be written as

$$N^e = \eta * x \qquad (3)$$

Where η is the number of potential users, and x is the fraction of those users that wants to join the network. Therefore, N^e is the expected number of users to join the bitcoin network.

Note that if x were higher; this would mean that people with a lower willingness to pay are now also expected to join the network.

Sauer (2015) makes the simplifying assumption that users have perfect foresight and can therefore determine the actual number of users. This makes it possible to set the expected number of users (N^e) equal to the actual number of users (N), so that

$$N^e = N = \eta * x \quad (4)$$

Agents base their decision to join the network on their utility function. Sauer (2015) assumes the utility an agent receives from joining the network (U_u) is

$$U_u = (1-x) * N - \rho \quad (5)$$

Which is inconsistent with the model so far. One would expect that people are willing to pay more, if they receive more utility from joining the network. If utility is high, this implies a high willingness to pay and join the network. However, with this utility function, this is not the case. This is further discussed in paragraph 4.4.

Sauer (2015) assumes the bitcoin network is stable if everyone in the network uses bitcoin for transaction purposes, and hence there is no speculation. This stable network is

$$x_1^0 \leq x \leq x_2^0 \quad (6)$$

Where the lower limit (x_1^0) is the minimal number of (two) participants needed to actually be a network, while the upper limit (x_2^0) is the last agent with non-negative willingness to pay. It is assumed that agents with a negative willingness to pay are never joining the network for transaction purposes, so they cannot be included in a stable network.

4.2: Hackers

Now hackers are introduced to the model. It is assumed that bitcoins can be stored on private computers, or on a platform where it is possible to buy and sell bitcoins (called a bitcoin exchange). It is assumed that hackers can hack both unprotected individual users, and (protected) bitcoin exchanges. The value of a bitcoin is called the 'exchange value' (e), which is the exchange rate of bitcoin versus the dollar, euro or any other currency for which it is traded.

The share of unprotected individual users in the bitcoin network is χ. The value of the bitcoins for the hacker is the product of the number of bitcoins obtained (b) and the exchange value (e), so the value of bitcoins obtained is b*e[21], where b ≥ 0 and e ≥ 0. If the hacker decides to hack an exchange, all bitcoin users that have stored their bitcoins on this exchange lose a certain share (a) of these bitcoins. For simplicity, it is assumed that all users hold the same share of bitcoins at a single exchange. Further there is a fine (S) that hackers have to pay if they are getting caught. Their probability of getting caught is κ. Note that S>0 and that κ ϵ [0, 1].

Hackers decide to join the network (by hacking either individual users or bitcoin exchanges), based on their utility function (U_h)[22]. This function is

$$U_h = \chi * N * be + \alpha * N * be - \kappa * S \quad (7)$$

The first term is the utility from individual hacking. This is based on the share of unprotected users (χ), times the actual users in the network (N) times the gains from hacking these individuals (be). The second term is about exchange hacking, which is based on the share of bitcoins that is stolen of each user (α), times the number of users in the network (N) times the value of these bitcoins (be). The last term shows the costs of being caught, which is the fine (S) times the probability of getting caught (κ).

It is now possible to calculate the number of users in the network that is needed for the hacker to obtain a positive utility from hacking bitcoins. This threshold value (x_h) is

$$x_h = \frac{\kappa * S}{(\chi+\alpha) * \eta * be} \quad (8)$$

So, a higher fine or a higher probability of getting caught means that the number of users in the network must be higher for hackers to receive positive utility from hacking bitcoins. All remaining variables have the effect that they reduce the threshold number of users for hackers to start hacking bitcoin.

It is now possible to extend the user utility with hacking. This allows to expand equation 5 to

$$U_u = (1-x) * N - \rho - \chi * be - \alpha * be \quad (9)$$

[21] I use 'be' from now on for referring to b*e.

[22] Hackers decide to hack if the utility of hacking is positive, hence if $U_h > 0$.

Both individual losses and losses of bitcoins stored on the exchange will lower utility of bitcoin users. The damage of getting hacked directly (individual hacking) is the share of users that is unprotected (χ), times the number and value of the bitcoins stolen (be). The damage of exchange hacking is the share of bitcoin held at the exchange (α) times the number and value of the bitcoin stolen (be). If hackers join the network, the expected utility goes down. Therefore, fewer agents are willing to join the network. Therefore, introducing hackers decreases the size of the bitcoin network.

4.3: Central bank regulation

The third player in the model is the central bank. Sauer (2015) assumes that the central bank has an incentive to keep the bitcoin network small or failing, because the official currency system and the bitcoin network have conflicting interests. Further it is assumed that the central bank can influence the bitcoin network by regulation, which includes all statements and rules that make bitcoin safer, more liquid and generally accepted. Therefore it is assumed that more regulation increases the utility of bitcoin users.

The level of regulation is captured by r and is between 0 and 1, where 0 is no regulation and 1 is total regulation. For simplicity, it is assumed that regulation only applies for bitcoin exchanges, not for bitcoins held at private computers. Adding regulation to the model changes equation 9 to

$$U_u = (1-x) * N - \rho - \chi * (be) - (1-r^*)*\alpha * be \quad (10)$$

With regulation (1-r*) added to the utility function; the loss for bitcoin users is smaller if there is more regulation. This might not hold if hackers gain as well from regulation, which in turn would lower (instead of increase) the bitcoin users' utility. This is discussed further in paragraph 4.4.

4.3.1: Intuition on central bank regulation

Sauer (2015) assumes that the central bank has an incentive to destabilize the bitcoin network; either by reducing the number of bitcoin users, or by increasing the number of bitcoin speculating agents. In the case that the number of users is low, the central bank can lower regulation. With a lower level of regulation, the utility of bitcoin users decreases (see

equation 10), which decreases the number agents that wants to join the network, since the utility is lower for a given willingness to pay. So, the central bank should limit regulation to the lowest possible level, which is 0.

However, Sauer (2015) assumes that if the number of users in the network is high (around the upper limit x_2^0), then a higher level of regulation will increase the number of agents that buy bitcoin with the sole purpose of speculation. This increases the number of bitcoin users that do not use bitcoin for transaction purposes, which destabilizes the network. Therefore, Sauer (2015) assumes that it is optimal for the central bank to use optimal regulation (r=1) if the bitcoin network is large.

4.3.2: Central bank loss function

Formally, the level of central bank regulation depends on the loss function for the central bank (L). This is

$$L = N * (((1 - \mathrm{x})N - \rho - \chi * be + (r - 1) * \ \alpha * be)^2 + R - be * r) \quad (11)$$

The loss of the central bank is higher if the number of bitcoin users (N) is larger. This is in line with Sauer (2015)'s assumption that the central bank has an incentive to reduce the size of the bitcoin network. This number of users is multiplied by the utility of these users, which in turn makes sense. The utility of a single users is squared, because Sauer (2015) assumes that the loss of the central bank is larger than the gain for the users. This is because the central bank also loses part of its reputation, and some control over variables like the interest rate and inflation. The last term (R-be*r) is not so clear. According to Sauer (2015); R is the cost of regulation. It is assumed that this cost increases if more people use bitcoin. A higher cost of regulation is a loss for the central bank. However, a higher level of regulation also leads to a gain for the central bank, due to the assumption that regulation leads to the partial control that the central bank has on the bitcoin system. This gain is assumed to be higher if the value of bitcoin increases. How or why the control by the central bank affects the loss function of the central bank, is not explained in Sauer (2015), but just assumed.

We learn from this model that the central bank experiences a loss if:

1) The utility from using bitcoin increases; which leads to more agents joining the bitcoin network.
2) The value of all bitcoins increases. This can be due to an increase in the number of bitcoins, or due to an increase in the value of a bitcoin (determined on the bitcoin exchange).
3) The cost of regulating bitcoin increases.

Sauer (2015) assumes that the fraction of potential bitcoin users that joins the network is below ½. This makes sense in a model where bitcoin is risky (due to hacking) and where a significant portion of utility is based on others joining the network. Therefore, Sauer (2015) shows us that since the number of bitcoin users is low; the central bank has an incentive to restrict regulation to a minimum. Regulation is costly and will increase the utility of agents and makes it more likely that they join the network. Avoiding this is assumed to be in the central banks' best interest. Therefore, we learn from this model that it is optimal for the central bank to abstain from bitcoin regulation, as long as the bitcoin network remains small and there are few agents that use bitcoin for speculation.

4.4: Discussion of the Sauer (2015) model

In this paragraph I show some critique on both the underlying assumptions in the model, and the main conclusion of the paper by Sauer (2015).

The utility function (equation 5) is inconsistent with the assumptions that Sauer (2015) makes in her model. It is explained that a low x means that only those with a high willingness to pay join the network. This implies that they receive more utility from joining the network, which makes a correlation where utility is higher for a higher x. This is not the case however.

We can combine equation 4 and 5, to write the utility function as

$$U_u = (1-x) * \eta * x - \rho \quad (12)$$

This in turn can be rewritten to

$$U_u = (x-x^2)* \eta - \rho \quad (13)$$

Now I used excel to graph this utility function[23] which shows that utility is not necessarily higher for those with a higher willingness to pay. Also, although it is assumed that a higher x means higher utility, the actual utility function turns out to be quadratic. This means that utility no longer increases with x, if x if larger than 0.5. The graph is shown below:

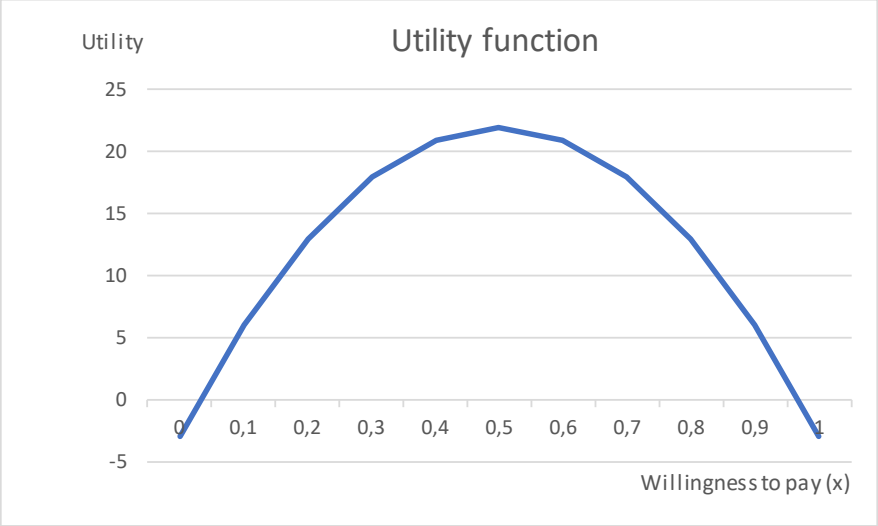


Figure 1: Utility function of bitcoin users

Changing the utility function to

$$U_u = \eta * x - \rho \quad (14)$$

seems to make more sense, since utility than depends on the number of people in the network, and on the cost of joining the network. The number of people in turn depends on the willingness to pay (x), and hence a higher willingness to pay would indicate that utility is higher. If more people join, x will be lower (now only those with lower willingness to pay can join, because others have already joined), and utility for the new joiners goes down. This continues until the cost of joining becomes higher than the utility from joining and we reached an equilibrium with no incentives to join or opt out. I argue that this is a better representation of utility in the model, since Sauer (2015)'s utility function is not consistent with the assumptions in her model.

[23] This specific case I used the following values: x=0 to x=1, with 0.1 steps, η=100 and ρ=3, x on x-axis, utility on y-axis.

Equation 10 shows that a higher level of regulation lowers the loss for bitcoin users if an exchange is hacked. This in turn increases their utility. This makes some sense, since e.g. deposit securities (getting you money back or the equivalent value after a hack) lowers the loss in case of being hacked. This in turn increases utility from using the bitcoin network since risks are reduced. It does however say little about hackers' incentives if regulation is at a high level. If regulation is beneficial for hackers as well (e.g. an increase in the legitimacy of bitcoin; which makes selling bitcoin easier), than more hackers might decide to hack an exchange. This effect is not captured in the utility function of hackers, nor is it shown in the utility function of bitcoin users (since more hackers lowers their utility). Just assuming some ambiguous effect of regulation is not very strong, especially if the main goal of the paper is to calculate an optimal level of regulation. Some more depth in the effects of regulation on bitcoin users and hackers would definitely benefit the model.

The main conclusion from Sauer (2015) is that the central bank should increase regulation if there are few bitcoin users, and increase regulation in case of a large network. I question this, since in the case of few bitcoin users, the network effects are still fairly small. Therefore, more regulation will increase the network, but might also stimulate speculation if we assume that the exchange value of bitcoin in a small network is more volatile; increasing potential returns for speculators. Furthermore; it makes hacking more attractive, since equation 6 shows us that hacking utility increases if the number of bitcoin users increases. Therefore increasing regulation can increase speculation and hacking, which makes the bitcoin network less stable. In addition, the effect of an unstable network would probably influence the utility of bitcoin users, but equation 10 does not capture this effect.

It might be assumed that the exchange value of bitcoin is more volatile with less users in the network. If the network is large, more regulation will then increase the number of users for transaction purposes, but the gains from speculation are lower. Therefore, the proposed regulation by Sauer (2015) might be counterproductive, and actual effects from regulation might very well differ from those explained by this model.

Chapter 5: The model by Luther (2016)

Luther (2016) uses a network-based model with switching costs to demonstrate that agents may fail to adopt an alternative money, even if all agents agree that the prevailing money is inferior. Bitcoin serves as an illustration that cryptocurrencies are unlikely to gain widespread acceptance without monetary instability or government support.

5.1: The basic model

The model by Luther (2016) consists of N money-using agents. Luther assumes homogenous and infinitely lived agents. The agents have no choice on which type of money to use and all use the 'incumbent' money. The utility agents obtain from using their incumbent money is

$$u(T)_{\theta N} = \frac{(a+b*n)}{r} \quad (1)$$

where u(T) is the utility at time T, where θ is the fraction of agents using the same type of money. N is the total number of agents. Since here it is assumed that all agents use the same type of money; θ is equal to 1. The variable b shows the value obtained from network effects; the more agents that use a money, the more it is valued by other agents that use it. It is assumed that b>0, which means that network-related utility increases with a larger network. The variable a captures the non-network utility from using the incumbent money. The variable n is the natural logarithm of θN, which means that the gains from the network effect are larger if more agents join the network. Also, it means that the gains increase at a diminishing rate. So, if the network is large; the gain from another agent joining is smaller compared to a small network[24]. The variable r is a discount factor.

5.1.1: An alternative money

Now it is assumed that there is an unexpected new money available (at time T* > T). Further it is assumed that agents are limited to using one type of money, so they must decide to keep

[24] Marginal utility is lower.

using the incumbent money, or pay a one-time switching cost (s) in order to use the alternative money. If a number of agents[25] switch to the alternative money, they earn utility

$$v(T)_{(1-\theta)N} = \frac{(c+d*\eta)}{r} - s \quad (2)$$

where c is the non-network related utility (similar to a in equation 1), and d*η is the network related utility (similar to bn in equation 1). The variable η is the natural logarithm of the number of switchers, so η ≡ ln((1-θ)N), which means that the more switchers; the higher the network-related utility for the users of the alternative money. It is socially optimal[26] to switch if the utility of the alternative money is higher than the utility from the incumbent money. Hence if

$$N * \frac{(a+b*n)}{r} < N * \frac{(c+d*\eta)}{r} - s \quad (3)$$

Where $\frac{(a+b*n)}{r}$ is the utility for an agent continuing to use the incumbent money if nobody switches, and $\frac{(c+d*\eta)}{r}$ is the utility for a switching agent if everyone else switches. Note that n and η are the same in this situation[27], so η = n. This means we can substitute n for η in equation 3, which allows us to rewrite equation 3 such that it gives us the maximum switching cost for which it is socially optimal to switch. This is the case if the total utility is larger after everyone switches to the alternative money. This should happen if

$$s \leq \frac{[c - a + (d-b)*n]}{r} \quad (4)$$

Which means that the switching costs are smaller than (or equal to) the gains in utility from switching from the incumbent to the alternative money. This does not happen per se in this model, due to the assumption by Luther (2016) that agents form adaptive expectations, rather than having perfect foresight (as in the model by Hendrickson, Hogan, and Luther, 2016). Therefore there might be less or more switching by agents than is socially optimal, based on agent's expectations on how other agents behave. Luther uses the borrowed terms

[25] The number is (1-θ)*N, since θ is the fraction of agents that use the incumbent money, and hence (1-θ) are those using the alternative money.
[26] So aggregate welfare increases.
[27] This is because in the first term: n=ln(θ) where everyone keeps using the incumbent money, so θ=1 and n=ln(1). In the second term: η=ln(1- θ) where everyone switches, so θ=0, and η=ln(1-0)=ln(1). Therefore n=η.

'excess inertia' for too little and 'excess momentum' for too much switching. The next figure, taken directly from Luther (2016, p.556), shows this in a clear graph.

FIGURE 1
Network Effects, Switching Costs, and the Fraction of Population Continuing to Use Incumbent Money

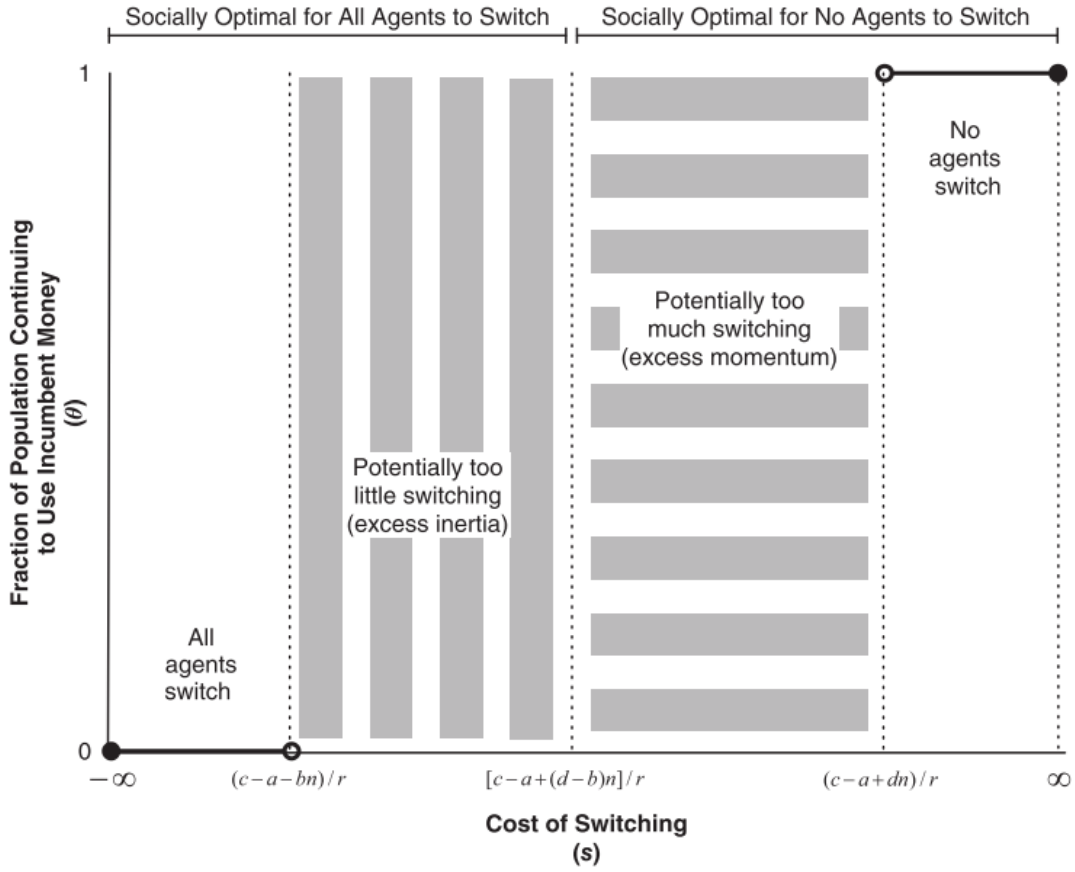


Figure 1: Switching in the Luther (2016) model

All agents switch if the non-network utility from switching (c) is larger than the non-network utility from using the incumbent money (a), plus the network gains from using the incumbent money when everyone else is expected to switch (bn). This is the case if

$$\frac{[c - a - bn]}{r} \leq s \tag{5}$$

It is also possible that no agent wants to switch. If an agent expects all others to switch, the utility from switching is equal to the non-network utility (c), plus the network-utility (dn) of the alternative money. Due to switching, the agents loses the non-network gains from using the incumbent money (a). Because the agents assumes everyone to switch, the network-utility of the incumbent money is assumed zero, so left out of the equation. If these gains

from switching do not exceed the switching cost, an agent will never choose to switch. This is the case if

$$\frac{[c - a + (d*n]}{r} \leq s \qquad (6)$$

5.1.2: Sub-optimal switching

Luther (2016) assumes that historical acceptance is the only factor that affect agents' expectations[28]. This means that agents form their expectations on what other agents do, based on previous acceptance of a certain money. That way; if no or few agents had switched to the alternative money in a previous time period, then network utility is still low and they do not adapt their expectations. Therefore excess momentum is unlikely and Luther assumes this cannot be an outcome from this model.

Excess inertia is still possible in the model, since historical acceptance can make people reluctant to switch to the alternative money, even if the cost of switching is relatively low. Successful transition to the alternative money will only take place if there is some form of coordination that reaches enough people and is not too costly. In order to make this coordination happen; (1) agents must be able to effectively coordinate, (2) the costs of coordination must be sufficiently low; at least below the utility gained from switching to the alternative money as a group. However, if all agents have the same adaptive expectations, then they either all switch or no one switches. Therefore, both excess momentum and excess inertia should not occur in this model. This is further discussed in paragraph 5.4.

5.2: A modified model with 2 types of agents

Now the model is modified so that agents are no longer homogenous. There are now 2 types of agents; there are φN 'type 1' agents and (1-φ)N 'type 2' agents[29]. At time T=T both types use the incumbent money. Their utility function is equal to equation 1 and the fraction of agents using the incumbent money is θ, but at this point simply equal to 1 because everyone

[28] The historical acceptance is referred to by Luther (2016) as a *focal point* on which people base their decisions.
[29] With $0 \leq \varphi \leq 1$.

uses the incumbent money at time T=T. Luther (2016) assumes that both types of agents have the same utility from the incumbent money.

As in paragraph 5.1.1 there is a new alternative currency available at time T=T*. Both types of agents can now decide to switch or not, based on the utility they gain from switching to the alternative currency. As in paragraph 5.1.2; Luther (2016) assumes that agents have adaptive expectations based on historical experience.

While both types of agents gain the same utility from the incumbent money, they differ in the utility they gain from using the alternative money. It is assumed that type 2 agents value the alternative money *at least as much* as type 1 agents, irrespective of network size. So: $c_2 \geq c_1$ and $d_2 \geq d_1$. Further it is assumed switching costs are at *least as large* for type 1 agents as for type 2 agents. Hence: $s_1 \leq s_2$.

Based on these assumptions; there are 4 possible equilibria:

1) Only incumbent money is used
2) Only alternative money is used
3) All type 1 agents continue to use the incumbent currency; all type 2 agents switch.[30]
4) Some agents of type 1 and/or 2 switch, while others keep using the incumbent money.

In the first equilibrium, only the incumbent money is used, which means that there is no switching by either type of agent. This is the case if the utility from the incumbent money is larger than the utility of the alternative money, or that the switching cost is too high. This is shown in equation 6.

The second equilibrium is where both type 1 and type 2 agents decide to switch. This is the case if the utility from the alternative money is high enough to convince even those of type 1 to switch, which means it should at least be higher than the switching costs. Also, due to adaptive adaptations, it should be high enough that even those that expect no or few agents to switch, still have enough utility from switching. This is the case if the non-network utility of the alternative money is larger than the switching cost (as in equation 5).

The third equilibrium shows a situation where the non-network utility of the alternative money is high enough for type 2 agents to switch, but where the total utility (network and

[30] Called a 'niche money equilibrium' in Luther (2016).

non-network) of the alternative money is too low for the type 1 agents to switch. This can occur due to the assumption that type 2 agents gain at least as much utility from the alternative money while never experiencing larger switching costs than type 1 agents.

The last equilibrium can occur if the non-network utility for both type 1 and type 2 agents does not exceed the switching cost, but when the utility of the alternative money with network-utility is higher than the switching cost. In this case, some agents switch if they expect enough other agents to switch, while others continue to use the incumbent money (if they expect few others to switch).

5.3: Real-life implications

This modified model provides two possible reasons for the limited success of bitcoin. Bitcoin can function as a niche money, when only certain people want to use it (equilibrium 3) due to some people finding the money less desirable (by experiencing lower network or non-network benefits from using bitcoin) and/or having higher switching costs. This way there remain people that do not switch, even in the case that everybody beliefs the alternative money (bitcoin) is better than the incumbent money. According to Luther (2016), those monetary transitions that do exist in history are typically accompanied by government support or hyperinflation. Without these events, Luther (2016) considers it unlikely that bitcoin gains widespread acceptance.

5.4: Discussion of the Luther (2016) model

Luther (2016) assumes that historical experiences is the only factor that affects agents' expectations. This assumption makes the model rather rigid, since there is little incentive left to switch. Because if in the last period there was little switching, agents expect little switching in the next period, which make them less likely to switch, and so on. It is also possible to allow other factors to influence agents' decision to switch. Potential candidates could be; central bank or government regulation on bitcoin[31], bitcoin price developments, bitcoin usage in other countries (that have other incumbent currencies) or trust in the government or the

[31] I use bitcoin here as an example, but these could be applied to each alternative currency that people can switch to.

economy. Allowing these factors to influence agents does alter the model in the sense that excess momentum remains possible in the model. This would imply a new (fifth) equilibrium where all type 2 agents switch and some of the type 1 agents switch. I think this is a better representation of reality, which is in line with Luther (2016)'s goal to use this model as a possible explanation for the limited acceptance of bitcoin in real-life.

Furthermore; Luther (2016) assumes that there is no excess momentum in the model, which indeed seems likely with only a historical focal point to base your expectation on. However, it is assumed that excess inertia is possible, which is not in line with the model. Since the model assumes homogenous agents and adaptive expectations, it must be that all agents have the same adaptive expectations. Since they know that all agents have these expectations, they know that other agents have the same information and make the same decision on switching or not. Therefore, either al agents switch, or no agents switch. This makes both too little and too much switching impossible in this model. The reason is that the model does not capture different adaptive expectations for different agents well. Luther (2016) does make a verbal argument, claiming that coordination costs can be a reason for people to have different expectations (some can coordinate to switch together while others cannot). This allows for a new focal point to base expectations on and then it could happen that some switch while others do not. This way, excess inertia might be possible, but this is not captured in the model.

The model is a network model, where switching to an alternative currency is largely dependent on network effects. This means that a money becomes more attractive to use (gains more utility) if there are more other agents using the money as well. I think this is not a good starting point for a model that is used to explain behaviour of the bitcoin market. This is because due to its speculative and risky nature, it is very unlikely that bitcoin is used for its network benefits. Bitcoin is typically used for speculation, since its volatility allows for large gains (and drops) in value. This would also be a major factor that leads to excess momentum, which is not possible in this model due to the assumption of Luther (2016) that people use only historical experiences for their switching decisions.

Also, bitcoin is different from fiat currencies, due to the anonymity of the blockchain technology. Trading anonymously could be a strong incentive to use bitcoin rather than fiat

currencies, especially for those with little trust in privacy protection or those involved in criminal activities.

Furthermore, bitcoin was founded at the start of the financial crisis, where trust in financial markets was very low. Bitcoin functions as a type of currency that is difficult to regulate by a central bank or government, which might attract some agents with little trust in these institutions. Using bitcoin because a lot of other agents use it, can hardly be an important factor that explains switching. Especially in countries that use a relatively stable (non-volatile) currency with trustworthy governments, where I expect that the number of fiat currency users and the correlated network effects are much larger than for the bitcoin network.

Lastly, Luther (2016) assumes adaptive expectations rather than rational expectations. Assuming rational expectations would give different results of this model. In paragraph 5.3 I explain that Luther (2016) thinks that a widespread acceptance of bitcoin is unlikely without government support or hyperinflation. I claim that if rational expectations are assumed, this is not necessary true. Rational expectations allows agents to act based upon their expectations about the future. If governments might claim to support bitcoin, and they are sufficiently credible; then agents can act upon their expectations of government support, and start switching to the alternative money. Note that this would happen even if the *actual* government support does not take place, as long as enough people belief the government support would take place. The same reasoning holds for expectations on hyperinflation.

Rational expectation also implies that the third and fourth equilibrium are no longer outcomes of the model. The reason is that type 1 and type 2 agents both know what the other agents will do. Therefore, coordination is no longer needed and there are only two relevant outcomes; either everyone switches if this is socially optimal, or nobody switches if switching is not optimal. This is irrespective of any exogenous shocks like government support or hyperinflation.

Chapter 6: Extending the model by Hendrickson, Hogan, and Luther (2016)

The model by Hendrickson, Hogan, and Luther (2016) is a monetary exchange model where agents can trade using bitcoin or fiat currency. It has some differences and similarities with the other papers discussed in this thesis, which are shown in table 1.

Table 1: Comparison of the models used in this thesis

Assumption	**Hendrickson/Hogan/Luther (2016)**	**Sauer (2015)**	**Luther (2016)**
Expectations	Perfect foresight	Perfect foresight	Adaptive expectations
Time	Discrete, infinite	Discrete, infinite	Discrete, infinite
Agents	Private, Government	Private, Hackers, Central Bank	Private; 2 types.
Money	Bitcoin, Fiat Currency, No Money	Bitcoin	Fiat currency, Bitcoin
Monetary Exchange[32]	Yes	No	Yes
Hackers	No	Yes	No
Regulation	Yes	Yes	No
Switching costs	No	No	Yes
Network effects	No	Yes	Yes

I add hackers to the model, because the possibility of hacking for bitcoin can affect the trust that people have in holding bitcoin, which affects their willingness to trade bitcoin. I think this makes the model more realistic[33] and allows the model to better deviate between different reasons agents have for using a certain type of currency.

I do not add switching costs to this model, because the model already assumes some sort of implicit utility from accepting a trade, and thereby switching to another currency. The same holds for network effects, because of the assumption that everyone accepts a currency if at least the threshold number of agents does. There is an implicit assumption there that more

[32] The possibility to switch to another currency.

[33] To illustrate: At June 11th, 2018, there was a hack on the South Korean bitcoin exchange 'Coinrail' which led to a decrease in bitcoin prices because people lost trust and started selling their bitcoins. 'Coincheck', a Japanese exchange was hacked in January. Other hacks can be found in e.g. this article: https://www.theguardian.com/technology/2018/jun/11/bitcoin-price-cryptocurrency-hacked-south-korea-coincheck.

agents accepting a currency yields more utility. Hence explicitly adding network effects to the model would not change any of the outcomes, which is why I chose not to include this.

In this chapter I extend the model of Hendrickson, Hogan, and Luther (2016) by making two additions. First, in paragraph 6.1; I add hackers to the model which affects the utility of trading agents. Second, in paragraph 6.2; I add two measures that can help to reduce the effects of hackers joining the model, which could be favourable for private agents. One measure is taken by the government, and the other by private agents. In paragraph 6.3 I show the effects of the different measures, and in paragraph 6.4 I show under what conditions the measures are useful. Finally, paragraph 6.5 concludes.

6.1: A model with hackers

Hendrickson, Hogan, and Luther (2016) assume an economy with some random number of agents (A), shown as

$$A = [0, 1]. \quad (1)$$

that differ in terms of their inventory. An agent can have money; currency or bitcoin, or no money. The fraction of agents with currency is m, the fraction with bitcoin is b, and the remainder (1-m-b) has no money. Agents with money are consuming agents, and agents without money are producing agents.

I extend the model by adding hackers, so that there are now agents and hackers in the economy. The number of hackers is

$$H = [0, 1] \quad (2)$$

I assume that hackers can only hack bitcoins, and they can hack each agent that has a bitcoin inventory. Further I assume that hackers are homogenous and that they all base their decisions on their utility function. Following Hendrickson, Hogan, and Luther (2016), where agents have perfect foresight; I assume that hackers have perfect foresight as well.

Because Hendrickson, Hogan, and Luther (2016) assume that an inventory cannot exceed 1 coin, I assume this applies to hackers as well. Therefore I assume that a hacker will try to hack at most 1 inventory in one time period. As in Hendrickson, Hogan, and Luther (2016), I assume

that the inventory of agents is common knowledge. Therefore, a hacker can try to match with an agent that has a bitcoin inventory.

I assume that the matching of hackers and agents with bitcoin inventories, goes via the same mechanism as matching between consumers and producers in Hendrickson, Hogan, and Luther (2016). Therefore, the probability that a hacker is matched with an agent with a bitcoin inventory (a bitcoin holder) is

$$h_{h,b} = \frac{b}{H} \quad (3)$$

where $h_{h,b}$ is the probability of a hacker being matched with an agent that has a bitcoin inventory. This is based on the number of bitcoin holders (b) divided by the number of hackers (H). If there are more bitcoin holders or less hackers; there is a larger probability that hackers and bitcoin holders are matched. I assume that the matching of hackers and bitcoin holders is independent of the matching by consumers and producers.

I assume that hacking does not always work, and that hacking can only take place once hackers and bitcoin holders are matched. Hacking is not always effective and is successful with a certain probability (ε). The probability of a successful bitcoin hack taking place (h_s) is the probability of a match between a hacker and bitcoin user (b/H), multiplied by the probability that the hack is successful (ε). This is shown in equation 4:

$$h_s = \frac{b*\varepsilon}{H} \quad (4)$$

I assume that the stolen bitcoin has some value (λ) for hackers, where λ>0. The utility function of hackers (U_h) is therefore

$$U_h = \frac{\lambda*b*\varepsilon}{H} \quad (5)$$

Adding hackers to the model does also affect the utility of private agents that hold bitcoin. The utility function of a bitcoin holding agent in Hendrickson, Hogan, and Luther (2016) is

$$rV_b = a_b\theta^* (U + V_0 - V_b) - \delta_b \quad (6)$$

[34]

[34] Actually; in Hendrickson, Hogan, and Luther (2016) it has an extra term, ρ, which is the preference for a certain good. Since this is not relevant for the model (see discussion in chapter 3); I chose to leave it out of the model. Since ρ was just a constant, this does not further affect the model.

Which is the probability of being matched to a producing agent ($a_b\theta$), times a gain from trade ($U + V_0 – V_b$), minus the storage cost for bitcoin (δ_b). With hackers in the model, agents are assumed to lose some trust in bitcoin, because of the risk of being hacked, which lowers utility. I assume that the loss in utility is equal to the probability of being matched to a hackers times the probability of a successful hack, which is equation 4. Therefore, the new bitcoin holders' utility becomes

$$rV_b = a_b\theta*(U + V_0 – V_b) – \delta_b - h_s \quad (7)$$

Which is now lower than in Hendrickson, Hogan, and Luther (2016) due to the lack in trust from possible hacking.

6.2: Measures that reduce hacking

In this paragraph I add two measures that reduce the negative effects of hacking on the utility of private agents. The first is a measure by the government, which is trying to catch and fine hackers in order to stop them from hacking bitcoin inventories. The second is a measure by private agents, where they buy security that stops hacking from being effective.

6.2.1: Government tax

The first measure is a that the government tries to catch and fine hackers. I assume that catching hackers and enforcing the law is in the best interest of agents, because it increases trust in bitcoin. Therefore I assume that the government demands a tax to cover the costs of law enforcement and the resources needed to catch the hackers. I assume that this tax is paid by bitcoin holders, which means that if an agent has a bitcoin in its inventory at a certain time, then it has to pay the tax in that time period. I assume that the tax is a fraction of the bitcoin holders' utility. This fraction of utility that is used as a tax is ϯ. I assume that the tax cannot exceed the utility of a bitcoin holder (V_b), because then no agent would use bitcoin, so $ϯ \in [0, 1]$. The tax reduces the utility of the bitcoin holder by $ϯ*V_b$.

The value function for currency holders is not affected by this measure, and is therefore the same as in Hendrickson, Hogan, and Luther (2016). The bitcoin utility is adapted by reducing the utility by the cost of the tax ($ϯ*V_b$). This changes the utility of bitcoin users to

$$rV_b = a_b\theta *(U + V_0 - V_b) - \delta_b - h_s - \tau * V_b \quad (8)$$

The utility for the producing agent declines as well, but because the utility of the bitcoin holder changes, and that utility is captured in the value function of the producer; there is no need to adjust the value function for the producer, which stays as in Hendrickson, Hogan, and Luther (2016). Hence, only the value function of the bitcoin user is different.

Sauer (2015) assumes that the government tries to catch hackers, and succeeds with a probability of κ, where κ ϵ [0, 1], meaning that they catch no hackers if κ=0 and that they catch all hackers if κ=1. In addition; the government gives hackers that are caught a fine (S), where S>0. If the government uses more resources to catch hackers (which leads to a higher κ) or if the fine increases (a higher S); this negatively affects the hackers' utility. I deviate a little from Sauer (2015) by stating that the probability of hackers being caught is linked directly to the tax ($\tau * V_b$), because if this increases, so do the funds available for catching hackers. This means that if the government demands a larger tax from private agents for catching hackers; this directly lowers the utility of hackers. However, there is a fixed fund ($\tau * V_b$) available to catch hackers, regardless of the number of hackers. If there are more hackers, then the probability of getting caught is lower for an individual hacker. So, an individual hacker has a larger utility if there are more hackers. I capture this by lowering the utility not by $\tau * V_b$, but by $\tau * V_b$ divided by the number of hackers. Therefore, utility is affected more if a lot of money is used to catch few hackers, and utility is affected less if the same money is used for catching more hackers. Therefore, I assume that the probability of getting caught (κ) is replaced by $\tau * V_b/H$.

Further; I keep assuming that the government fines hackers that are caught, where the fine is the same as in Sauer (2015); so S, with S>0.

Therefore the utility of a hacker (U_h) is the utility from a successful hack (λ), times the probability that a successful hack takes place (b*ε), minus the funds available per hacker for catching them ($\tau * V_b/H$) times the fine if being caught (S). This changes the hackers' utility function (equation 5) to

$$U_h = \frac{\lambda * b * \varepsilon - \tau * V_b * S}{H} \quad (9)$$

Where the utility for hackers increases if the utility of a successful hack (λ), the probability of a successful hack (ε) or the probability of being matched to an agent with bitcoin (b),

increases. The utility for hackers decreases if the available funds for catching hackers (τ^*V_b), the fine when being caught (S) or the number of hackers (H) increases. The number of hackers does both positively and negatively affect utility. If the gains from hacking are larger than the costs (risk of being caught times the fine), then an increase in the number of hackers lowers their utility. If the costs are larger, than an increase in the number of hackers increases utility. However, because of the assumption that hackers only hack if their expected utility is positive, the actual number of hackers were zero, and hence the only relevant outcome is that the gains are larger than the costs. Therefore; I assume that a larger number of hackers lowers utility.

6.2.2: Private security

If agents have little trust in the government, or if the government is not very successful in catching hackers; agents might take matters into their own hands. I assume that agents can protect themselves from hacking attacks on their bitcoin inventory by buying private security from an external company[35], which works as an extra layer of protection after the hacker has successfully hacked the inventory. So after hacking the inventory, a hacker is still unable to steal the bitcoin. I assume that the security always prevents hackers from stealing the bitcoin. Also, I assume this security works instantly once bought, so that there is no need to buy the security when an agent has no bitcoin inventory. Further, I assume that hackers cannot know which agents have bought the security.

The cost for the security is σ, where σ>0. I assume that an agent buys the security only if the cost is lower than gains from trading bitcoin. If security is bought, then the trust in bitcoin is restored, so h_s is no longer affecting utility because bitcoin hacking can no longer be effective. I assume that the probability that agents buy security is μ, where $\mu \in [0, 1]$, which depends on the cost of private security (σ). The probability of buying private security is in fact the same as the fraction of agents that buy security. However, because in this model all agents or no agents buy security; what matters is the probability that all agents buy security, which is μ.

[35] Exogenous, so the companies that sell this security are not modelled here.

For bitcoin holders; security is a cost (σ), but it might also restore trust because hacking is no longer effective. If the probability of buying security is larger, then so is the expected utility . How much this is lost depends both on the probability of buying the security, and on the price of the security. In addition; a larger probability of buying security reduces the effect of a successful inventory hack. Therefore, h_s is multiplied by (1- μ(σ)). This changes the bitcoin holders expected utility to

$$rV_b = a_b\theta *(U + V_0 – V_b) – \delta_b – (1-\mu(\sigma))*h_s – \dagger*V_b – u(\sigma)* \sigma \quad (10)$$

Where the lower trust no longer affect utility if the probability of buying security is 1, and where the costs of security have no effect on utility if the probability of buying this security is 0.

For the hacker, security negatively affects expected utility since it lowers the probability of successfully stealing the bitcoin. Expected utility decreases if the probability that agents buy security increases. Recall that security is always effective in protecting the bitcoin from being hacked. If the probability that agents buy security (μ) is 0; then there is no effect on the hackers' utility. However, a higher number of protected users will lower the hackers' expected utility. Therefore, the expected utility of a hacker is multiplied by (1- μ(σ)).

$$U_h = \frac{(1-\mu(\sigma))*\lambda*b*\varepsilon-\dagger*V_b*S}{H} \quad (11)$$

Where a higher utility from stealing bitcoin (λ), a higher probability of being matched (b), and a higher probability of successfully hacking the inventory (ε), increase hackers' utility. A higher probability of protected agents (μ), more funds to catch hackers (†) and a higher fine (S), reduce hackers' utility.

6.3: Effects of the measures

This paragraph shows how the different measures affect the model. Paragraph 6.3.1 explains the direct and indirect effects of the tax measure and calculates the relevant limits, and paragraph 6.3.2 explains the effects and shows the limits of the private security measure.

6.3.1: Effects of demanding a tax

An increase in the tax level[36] has three effects in this model. First; it reduces the utility of the bitcoin holder, because these agents have to pay the tax. Since the tax is a part of the value that bitcoin holders obtain from holding bitcoin; a higher tax means that more of this value is demanded, and hence utility decreases. Second; a tax reduces the utility of hackers, because the funds obtained from the tax are used to catch hackers. More funds leads to a larger probability that hackers are being caught and fined, which reduces the utility of hackers. The third effect is that a lower utility for hackers reduces the probability that hackers join the model. This is in the best interest of agents, and has therefore a positive effect on their utility.

The utility function for bitcoin holders (equation 8) shows that the utility of the bitcoin holders increases if the probability of a successful hack (h_s) decreases. In addition; equation 4 shows that this is the case if the number of hackers increases. This seems like an odd result, because the utility of bitcoin holders increases if the number of hackers goes up, which is counter-intuitive. The reason is that as in Hendrickson, Hogan, and Luther (2016), this model has some specific assumptions. One of the limitations of this model is that either all hackers start hacking, or no hackers do. Therefore; the only thing that matters is the probability that all hackers join the model. Equation 3 shows that with a larger number of hackers, there is a lower probability of being matched to an agent with a bitcoin inventory. The utility function of hackers (equation 11) shows that a lower probability of being matched leads to lower expected utility for the hacker. Since hackers base their decision to hack or not on their utility function; this reduces the probability that all hackers start to hack bitcoins. As a result; this lower probability of hacking increases the utility of bitcoin holders.

Note that this only holds for this specific set of assumptions. If it were possible that some hackers start hacking while others do not, then an increasing number of hackers would in fact reduce the utility for bitcoin holders. In the extended model, hacking has diminishing returns. This is because a larger number of hackers reduces the probability of being matched to an agent with a bitcoin inventory. Therefore, as the number of hackers increases; marginal utility decreases. However, in the extended model it is not possible that only some hackers start hacking, because hackers simultaneously decide whether to start hacking or not. The marginal

[36] A decrease in the tax level has the exact opposite effects.

utility is positive, zero, or negative, but this is the case for all hackers at the same time. Therefore, they all start hacking if expected utility is positive and nobody starts hacking if expected utility is negative. If the expected utility from hacking is zero; hackers are indifferent, so some hackers start hacking while others do not, which is determined randomly.

Note that there is no tax level for which some bitcoin holders pay tax and others do not. If the utility of bitcoin holders is zero; the government has to decide to continue demanding funds to catch hackers (and everyone pays) or to stop demanding funds (nobody pays). This is because I assumed that the tax is coordinated by the government and not by individual bitcoin holders. The reason is that I assume that the government has lower coordination costs than private agents, and because a government tax solves the problem of free riding that could occur if agents were to coordinate the funding of catching hackers.

Since the tax is used to discourage hackers from hacking bitcoin inventories, I claim that the tax is effective if it stops hackers from doing so. Since hackers base their decision to hack on their utility function; the tax level should minimally be such that hackers no longer start to hack bitcoin inventories, which is

$$\text{ŧ}^*V_b = \frac{(1-\mu(\sigma))*\lambda*b*\varepsilon}{S} \quad (12)$$

This equation shows us the tax level for which the expected utility from hacking is zero. If the fine is larger; there is less tax needed to stop hackers from hacking bitcoin inventories. If hackers obtain more value from hacking, then there is more funds needed to stop hacking, and therefore the tax level should increase. The derivation of equation 12 is shown in the appendix. For clarity; this tax level is indicated as T_1.

In addition, a tax is only useful for bitcoin holders if it does not lead to situations where agents obtain negative utility from using bitcoin. Therefore, I calculate the maximum tax level for which agents still use bitcoin, which is

$$\text{ŧ}^*V_b = a_b\theta^*(U - C) - (\delta_b + C) - (1-\mu(\sigma))^*h_s - \mu(\sigma) * \sigma - a_m\pi^*(V_m - V_0 - C) \quad (13)$$

This equation shows us that if the utility from holding bitcoin is larger; there is a larger fraction of this utility that can be used as tax for catching hackers. If the tax level is larger than in equation 13; bitcoin holders have negative utility from holding bitcoin. If this is the case than private agents do no longer use bitcoin for transactions. Therefore the tax level should not

exceed the level shown in equation 13. The derivation of equation 13 is shown in the appendix. For clarity; this tax level is indicated as T_2.

I claim that a tax is effective in restoring trust in bitcoin only under two conditions: 1) it should stop hackers for hacking bitcoin inventories ($T>T_1$), and 2) it should be such that agents still obtain positive utility from holding bitcoin ($T<T_2$). Note that both conditions are satisfied only if

$$\frac{(1-\mu(\sigma))*\lambda*b*\varepsilon}{S} < a_b\theta^*(U - C) - (\delta_b+C) - (1-\mu(\sigma))*h_s - \mu(\sigma)*\sigma - a_m\pi^*(V_m - V_0 - C) \quad (14)$$

Note that if expected utility of hackers is zero; their decision to join or not is random and therefore we cannot be sure that all hackers withhold from hacking. Therefore we need the tax level to be large enough to make the expected utility of hackers negative and not zero. The second condition is satisfied if the tax level is small enough for agents to have positive utility from holding bitcoin. If their utility is zero, then it is up to the government to determine whether or not to demand the tax. However, this decision is random and therefore we can only be sure that agents continue to use bitcoin if their expected utility from holding bitcoin is positive. Note that if equation 13 is smaller than equation 12; it is never possible (within this model) to have both zero hackers and positive utility from holding bitcoin within this model. Therefore, a tax will not be demanded by the government if this is the case. If both conditions are satisfied; this model shows a tax range that can successfully stop hackers from hacking bitcoin inventories, while leaving enough utility for private agents to continue holding bitcoins in their inventories.

6.3.2: Effects of buying private security

The possibility of buying private security has three effects. First; a higher cost of the security[37] makes it more expensive for bitcoin holders to protect themselves from hackers. A higher cost lowers the utility for bitcoin holders; regardless of the number of hackers that actually starts hacking. The second effect is that a higher cost of security decreases the probability that agents buy security. This means that there is a smaller probability that hackers can no longer successfully hack a bitcoin inventory. Therefore, expected utility from starting to hack is

[37] A lower cost of security has the exact opposite effects.

higher and it is more likely that all hackers start to hack. The third effect is therefore that the utility of bitcoin holders goes down, because the probability of being hacked successfully goes up, and so does the probability that all hackers start hacking.

The cost of the security determines the probability that bitcoin holders buy security. Note that in this model, either every bitcoin holder or no bitcoin holder buys security. Therefore; the cost of security does not change the fraction of bitcoin holders that buy security, but the probability that all agents buy security. Recall that this probability that all agents buy security is μ.

For bitcoin holders; a larger cost of security (σ) decreases utility. If this cost is too high, this decreases the probability that agents buy security, because agents no longer obtain positive utility from holding bitcoin. Therefore I calculate the probability of buying security for which bitcoin holders are indifferent about using bitcoin. This probability is

$$\mu(\sigma) = \frac{a_b\theta*(U-C)-(\delta_b+C)-\dagger*V_b - am\,\pi*(V_m - V_0 - C)-h_s}{\sigma-h_s} \quad (15)$$

This shows that the probability of buying security decreases if the cost of security (σ) increases and that the probability is higher if there is a larger probability that hacking is successful (h_s). Therefore equation 15 can also be interpreted as the maximum cost for which the probability is such that agents are indifferent about using bitcoin. A higher cost leads to a lower probability of buying security, which can lead to negative utility from using bitcoin. If the probability of buying private security is higher than in equation 15, then the utility from having bitcoin is still positive after buying the security against hackers. The derivation of equation 15 is shown in the appendix. For clarity; this probability of buying private security is indicated as μ_1.

For hackers it is not the price of private security itself that affects expected utility, but the resulting probability that agents buy this security. If the cost of security is lower; this increases the probability that agents buy security and are protected against hacking. This reduces the hackers' expected utility. It is possible to calculate a probability of buying security for which the expected utility of hackers is zero. This is

$$\mu(\sigma) = 1 - \frac{\dagger*V_b*S}{\lambda*b*\varepsilon} \quad (16)$$

which shows that the threat of buying security has less effect on hackers if their utility from hacking ($\lambda * b * \varepsilon$) is higher, and affects them more if the tax level is high, or if there is a larger fine. Also, it shows that per definition the probability of buying security cannot exceed 1, since no more than all private agents can buy security. If the probability of buying security is as in equation 16; hackers have zero utility from hacking. The derivation of equation 16 is shown in the appendix. For clarity; this probability of buying private security is indicated as μ_2. A summary of the different effect on the utility of bitcoin holders and hackers is shown in table 2.

Table 2: Effects of different variables

Variable	Symbol	Utility bitcoin holders		Utility hackers
		Direct effect	Indirect effect	Direct effect
Cost of producing a good	C	0	0	0
Utility from consuming	U	+	0	0
Utility producers	V_0	0	0	0
Utility bitcoin holders	V_b	+	0	0
Utility currency holders	V_m	0	0	0
Storage costs for bitcoin	δ_b	-	0	0
Number of bitcoin holders	b	+	-	+
Number of hackers	H	0	-	-
Bitcoin value for hackers	λ	0	0	+
Fine for hackers	S	0	0	-
Cost of private security	σ	-	-	0
Tax level	$\tau * V_b$	-	+	-
Effectiveness of hacking	ε	-	0	+
Probability of match producer + bitcoin holder	$a_b\theta$	+	0	0
Probability of match producer + currency holder	$a_m\pi$	0	0	0
Probability of successful hack	H_s	-	0	+
Probability of buying security	μ(σ)	0	+	-

6.4: Usefulness of measures

The limits calculated in paragraph 6.3.1 and 6.3.2 show how the different variables affect the decision of hackers to start hacking, and the decision of bitcoin holders to keep using bitcoin. These limits are summarized in table 3. In this paragraph, I show how different variables affect the usefulness of the measures, by showing what impact they have on the different limits.

Table 3: Limits of different measures

Measure	Notation	Symbol	Limit	Result
tax	T_1	†*V_b	>	$\frac{(1-\mu(\sigma))*\lambda*b*\varepsilon}{S}$
tax	T_2	†*V_b	<	$a_b\theta*(U-C)-(\delta_b+C)-(1-\mu(\sigma))*h_s-\mu(\sigma)*\sigma-a_m\pi*(V_m-V_0-C)$
Private security	μ_1	$\mu(\sigma)$	>	$\frac{a_b\theta*(U-C)-(\delta_b+C)-†*V_b-am\,\pi*(V_m-V_0-C)-h_s}{\sigma-h_s}$
Private security	μ_2	$\mu(\sigma)$	<	$1-\frac{†*V_b*S}{\lambda*b*\varepsilon}$

6.4.1: Usefulness of tax

I start by explaining the effects of different variables on the effective tax level. Figure 1 shows that at a certain tax level (T_1); hackers are no longer willing to start hacking. If the tax is below this level, then all hackers still start hacking and the tax is not effective. No agent is willing to pay for a tax if it has no effect. Therefore, I assume that the tax will not be demanded by the government. If the tax is too high (T_2), then agents are no longer willing to pay for the tax, because they no longer have positive utility from holding bitcoin. If this is the case, the government will also not demand the tax. Therefore; the tax will only be demanded if $T_2 > T_1$.

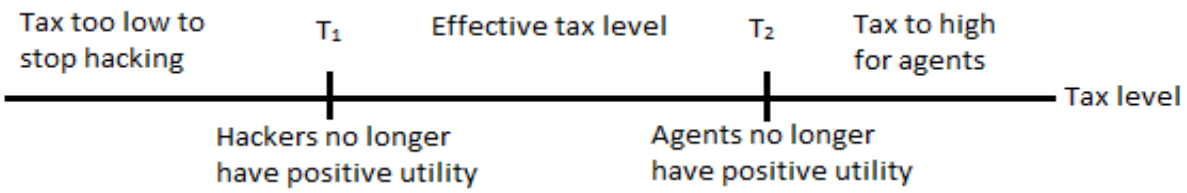


Figure 1: Results of different tax levels

If T_2 is not larger than T_1; this means that the tax will not be demanded. The tax is more effective if the probability that a tax is demanded goes up. This is the case if the tax range increases; so if T_1 goes down or T_2 goes up. The probability that a tax is demanded changes if the utility of bitcoin holders changes, without this effecting the utility of hackers. There is a positive effect from an increase in the utility from consuming a good (C), and a negative effect from higher storage costs for bitcoin (δ_b). Also, a larger probability that bitcoin holders are matched to producers increases utility and hence the tax range, while a larger probability of currency holders being matched to producers reduces the effective tax range. In addition, the

probability of a tax changes if hackers' utility is affected while bitcoin holders' utility is unaffected. There is a positive effect from a larger fine for hackers (S) , and a negative effect from the value that hackers obtain from hacking a bitcoin (λ), or when hacking is more effective (ε).

The effects are more interesting where both the utility of bitcoin holders and hackers are affected. This is the case for changes in the cost of private security (σ), the probability of successful hacking (H_s) and the probability of buying security μ(σ). We know from equation 15 that both the cost of private security and the probability of successful hacking have an effect on the probability of buying security. A larger cost of security decreases the probability that agents buy security. This has an effect on both the lower limit (T_1) and the upper limit (T_2). Table 3 shows us that if the cost of security increases; T_1 must increase as well, in order to keep the expected utility of hackers negative and stop hacking. This means that the effective tax range becomes smaller. This makes sense, because if the expected utility of hackers increases, they are willing to hack even if the probability of getting caught increases (slightly) as well.

The effect on the upper limit is less clear. Table 2 shows that a higher price of security affects utility in two ways. First; there is an effect on the probability of being hacked, which is (1-μ(σ))*h_s. I call this the 'trust effect'. Second; there is the effect that there is a smaller probability of buying security, but at a higher price. This is μ(σ)*σ, which I call the 'price effect'. The 'trust effect' is always a decrease in utility if the price of security rises. This is because this price increase reduces the probability of buying security, which increases the risk of being hacked. With the 'price effect'; the price elasticity of the security package matters. If this elasticity is high, then an increase in the price can lead to a stronger decrease in probability to buy. In this case; the 'price effect' leads to higher utility because the probability of actually paying for the security goes down. If elasticity is low; the 'price effect' leads to a decrease in utility. Note that only if the positive utility from the 'price effect' is larger than the negative utility from the 'trust effect'; utility increases, which means the upper tax limit (T_2) increases. If this increase of the upper limit is larger than the increase in the lower limit (because hackers obtain more utility); the effective tax range increases. In all other cases; an increase in the price of security reduces utility and reduces the effective tax range.

An increase in the price of security is likely to reduce the effective tax range. If the increase is large enough; it might be that there is no longer a tax that effectively bans hackers and yield positive utility for bitcoin holders. In this case; the government no longer demands a tax.

6.4.2: Usefulness of private security

Now I explain the effect of several variables on the probability of buying security. Figure 2 shows that the utility of hackers increases if the cost of security is lower, and that the utility of hackers increases if the cost of security is higher, because that leads to a lower probability of buying security.

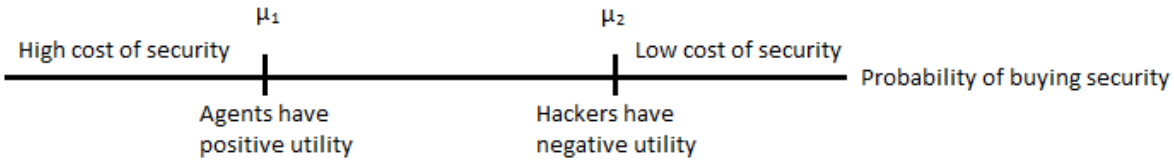


Figure 2: Probability of buying private security

Figure 2 can be interpreted as follows: μ_1 is the probability of buying security for which agents have positive utility. If the cost of security is lower, than the probability of buying security increases. The limit μ_2 shows the probability of buying security for which hackers have negative expected utility. If the cost of security is high enough, then the probability of buying security is low enough for hackers to obtain positive utility. Note that for the private security to be effective, the cost of security must be such that the probability of buying security is both higher than μ_1 and higher than μ_2. If this is not the case; then either bitcoin holders have negative utility, or hackers have positive utility and are not effectively banned. Below I explain which variables have which effect on the different limits.

For hackers; table 2 shows that a higher tax level and a higher fine lead to a lower expected utility. Conversely, a higher utility from having bitcoin, more bitcoin holders, and a higher probability of effective hacking increases the expected utility. For bitcoin holders; the probability of being matched to a producer increases utility, and so does an increase in the utility from consuming a good. We know that an increase in the cost of private security makes this measure less effective, because the probability of buying security decreases. Other variables (storage cost of bitcoin, production costs, probability of currency holders and

producers being matched) have a negative effect on the bitcoin holders' utility. The more interesting variables are the tax level (T^*V_b) and the probability of successful hacking (h_s).

Table 3 shows that a higher tax level means that the probability of buying security can decrease while still maintaining positive utility. This makes sense, since if there is a higher tax, there are more funds available for catching hackers. This reduces the need for buying security, so even with a larger cost of security; the measure is still effective. For hackers; a higher tax means that the probability that agents buy security must go down to obtain positive utility. This means that if the tax increases; the probability that agents buy security must go down in order for hackers to have positive expected utility. So, with a higher tax, a smaller probability of buying security is sufficient to ban hackers.

The probability of a successful hack (h_s), which is the number of bitcoin holders (b) times the effectiveness of hacking (ε), divided by the number of hackers (H) (equation 4), does not have an effect on the probability of buying security. However, the term $b^*\varepsilon$ does, and an increase in one or both of these variables (b or ε) leads to an increase in the limit (μ_2), while the number of hackers does not affect the limit. This means that since $b^*\varepsilon$ increases h_s; an increase in these variables will mean that h_s goes up as well (for a given number of hackers). As a result, the probability of a successful hack leads to hackers having positive utility even if the probability of buying security is higher. This means that there is a higher probability that hackers start to hack if the probability of a successful hack increases.

For bitcoin holders, table 2 shows that a higher probability of successful hacking decreases utility and decreases the probability that agents buy security. This means that bitcoin holders face a larger risk of being hacked, and therefore the utility from using security is positive at a lower probability of buying security. This means that if there is a larger probability of a successful hack, bitcoin holders are willing to pay more for security, so bitcoin holders are more inclined to use private security.

Table 4 summarizes the effects of the different variables on the different limits. The table can be interpreted as follows; a plus indicates that a variable increases the limit while a minus shows the opposite effect, and a zero means that there is no effect on the respective measure. A plus minus indicates that the effect is ambiguous and depends on mechanisms explained in

this paragraph. If the lower limit is decreased or the upper limit is increased; this means that the variable increases the usefulness of the measure. If the limits converge; the usefulness is reduced. If the effects are large enough, this can make that the different measures are not used because they either make bitcoin holders' utility negative, or fail to ban hackers.

Table 4: Effects of variables on measure limits

Variable	Symbol	Effect on tax (T_1)	Effect on tax (T_2)	Effect on probability of buying private security (μ_1)	Effect on probability of buying private security (μ_2)
Cost of producing a good	C	0	-	0	-
Utility from consuming	U	0	+	0	+
Utility producers	V_0	0	-	0	-
Utility bitcoin holders	V_b	0	+	0	+
Utility currency holders	V_m	0	-	0	-
Storage costs for bitcoin	δ_b	0	-	0	-
Number of bitcoin holders	b	+	0	+	0
Bitcoin value for hackers	λ	+	0	+	0
Fine for hackers	S	-	0	0	0
Cost of private security	σ	+	+/-	0	-
Tax level	τ^*V_b	0	0	-	-
Effectiveness of hacking	ε	+	0	+	0
Probability of match producer + bitcoin holder	$a_b\theta$	0	+	0	+
Probability of match producer + currency holder	$a_m\pi$	0	-	0	-
Probability of successful hack	H_s	+	-	+	-
Probability of buying security	μ(σ)	-	+/-	-	+/-

6.5: Conclusions

I showed that both measures are supplements, because an increase in the tax level, allows for a lower probability of buying security and vice versa. Note that if all bitcoin holders buy security; there is no need for an actual tax. However, because the utility of hackers is based on expectations, a probability that agents buy security that is below 1, might still give hackers a positive expected utility. Therefore, a higher tax level helps to ban hackers from the model.

Further I showed that the usefulness of both measures typically increases if the utility for bitcoin holders goes up, or the utility for hackers goes down. In addition, there are some

variables which have an ambiguous effect. The higher cost of private security is likely to have a negative effect on usefulness of private security. Unless elasticity is very high; private security only effectively bans hackers if the cost is low and bitcoin holders have a large expected utility if hackers are banned.

An increase in the tax level means that bitcoin holders lose a fraction of their utility and that this increases utility as well due to the lower probability that hackers enter the model. The tax is only useful if it high enough to ban hackers and if the utility gain from banning hackers is larger than the cost of the tax. Under all other circumstances, bitcoin holders are unwilling to pay for the tax and the government does not demand it.

Conclusion

In this thesis I explained and discussed three papers that deal with bitcoin. The papers by Hendrickson, Hogan, and Luther (2016) and Luther (2016) use a monetary exchange model that differs mainly in terms of their assumptions on the expectations of agents. Additionally, the first paper shows how the government can effectively ban bitcoin use, while the latter provides explanations on the limited widespread acceptance of bitcoin. The other paper, by Sauer (2015), was based on a model that includes hackers and the central bank. It shows under what conditions central bank regulation is optimal and how this affects the decision of agents to join the bitcoin network.

I extended the paper by Hendrickson, Hogan, and Luther (2016) by adding hackers to the model and providing two possible measures to stop hacking; a government tax and private security. I showed how the different variables have an effect on the utility of bitcoin holders and hackers, and what the limits are for which bitcoin holders and agents have zero utility. I used these limits to show how several variables affect the usefulness of the different measures. In this thesis I show a tax range that successfully bans hackers while agents are still willing to trade bitcoins. Also, I find that private security is more effective if the cost is of buying this security is lower, and that a higher tax level is more effective in banning hackers. Furthermore; I conclude that both measures supplement each other and that they are more effective if bitcoin holders have a large utility compared to producing agents.

Further research can be done on a wide range of topics. It is possible to add more or other measures to reduce negative effects of hacking. Also, adding more factors that determine the use of bitcoin is nice addition. Possible candidates could be adding exchange rate risk or government regulation to the model. This way, not only hackers are a risk for bitcoin holders, but other factors matter as well. Another idea is to release the assumption that agents have perfect foresight, and change this by letting agents form expectation in another way, like assuming adaptive expectations. Furthermore, releasing the assumption of representative agents, which means that only all or no agents switch, is a nice addition, because it allows for agents to respond differently to several measures. Moreover; it could be possible to add other (crypto)currencies to the model, and see if agents respond differently to the various currencies.

References

Aiyagari, S. R., and Wallace. N. (1997). Government Transaction Policy, the Medium of Exchange, and Welfare. Journal of Economic Theory, 74(1), 1–18.

Bartholomae FW (2013) Network, Hackers, and Nonprotected Consumers. *Working Papers in Economics* 25(3). Bundeswehr University Munich.

Bjerg, O. (2016). How is Bitcoin Money? *Theory, Culture & Society*, *33*(1), 53–72.

Blau, B. M. (2018). Price dynamics and speculative trading in Bitcoin. *Research in International Business and Finance*, *43*(July 2017), 15–21.

Bohr, J., & Bashir, M. (2014). Who Uses Bitcoin? *2014 Twelfth Annual Conference on Privacy, Security and Trust (PST)*, 94–101.

Cheah, E. T., & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters*, *130*, 32-36.

Corbae, D., Temzelides, T., & Wright, R. (2003). Directed matching and monetary exchange. *Econometrica*, *71*(3), 731–756.

Donier, J., & Bouchaud, J. P. (2015). Why do markets crash? bitcoin data offers unprecedented insights. *PloS one*, *10*(10).

Dowd, K., & Greenaway, D. (1993). Currency competition, network externalities and switching costs: towards an alternative view of optimum currency areas. *Economic Journal*, *103*(420), 1180–1189.

Dwyer, G. P. (2015). The economics of Bitcoin and similar private digital currencies. *Journal of Financial Stability*, *17*, 81–91.

Evans, D. (2014). Economic aspects of bitcoin and other decentralized public-ledger currency platforms.

Fry, J., & Cheah, E. T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, *47*, 343-352.

Godsiff, P. (2015). Bitcoin: bubble or blockchain. *Agent and Multi-Agent Systems: Technologies and Applications*, 191-203, Springer, Cham.

Hendrickson, J. R., Hogan, T. L., & Luther, W. J. (2016). The political economy of bitcoin. *Economic Inquiry*, *54*(2), 925–939.

Hogan, T. L., and Luther. W. J. (2014). Endogenous Matching and Money with Random Consumption Preferences. Working Paper.

Kiyotaki, N., and Wright. R. (1993). A Search-Theoretic Approach to Monetary Economics. *American Economic Review*, 83(1), 63–77.

Li, Y., and Wright. R. (1998). Government Transaction Policy, Media of Exchange, and Prices. *Journal of Economic Theory*, 81(2), 290–313.

Lotz, S., and Rocheteau. G. (2002). On the Launching of a New Currency. *Journal of Money, Credit, and Banking*, 34(3), 563–88.

Luther, W. J. (2016). Cryptocurrencies, Network Effects, and Switching Costs. *Contemporary Economic Policy*, *34*(3), 553–571.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *International Conference on Financial Cryptography and Data Security*, 25-33.

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

Presthus, W., & O'Malley, N. O. (2017). Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency. *Procedia Computer Science*, *121*, 89–97.

Sahoo, P. K. (2017). Bitcoin as digital money: Its growth and future sustainability. *Theoretical & Applied Economics*, *24*(4), 53–64.

Sauer, B. (2015). Central Bank Behaviour Concerning the Level of Bitcoin Regulation as a Policy Variable. *Athens Journal of Business and Economics*, *1*(4), 273–286.

Selgin, G. (2003). Adaptive learning and the transition to fiat money. *Economic Journal*, *113*(484), 147–165.

Shy O (2001). The Economics of Network Industries. Cambridge: Cambridge University Press.

Trautman, L. J. (2014). Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?.

Waller, C. J., and Curtis, E. S. (2003). Currency Restrictions, Government Transaction Policies and Currency Exchange. *Economic Theory*, 21(1), 19–42.

Yelowitz, A., & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, *22*(13), 1030-1036.

Yermack, D. (2013). Is Bitcoin a Real Currency? an Economic Appraisal.

Appendix

Chapter 3:

Value function simplification

The original equation for the value function for non-money holders, as used in the paper by Hendrickson, Hogan, and Luther (2016), was

$$rV_0 = (1- a^e_{0,m} - a^e_{0,b})\, \rho^2\, (U-C) + a^e_{0,m}\, \Pi(\pi)\rho\, (V_m - V_0 - C) + a^e_{0,b}\, \Theta(\theta)\rho\, (V_b - V_0 - C)$$

The first term shows the probability that two agents without money are matched ($1- a^e_{0,m} - a^e_{0,b}$), times the probability of both of them willing to trade the other agent's good[38] ($\rho*\rho$ or ρ^2), times the utility from trade minus the costs of production (U-C). However, due to the constraining assumption that two agents without money cannot trade; the probability of trade taking place between the two agents is zero. Therefore; the first term is zero and therefore I removed it from the equation.

Threshold values

To calculate the best response, we need to use the value functions. The expected value of accepting currency is given in the first term of equation 15: $a^e_{0,m}\, \rho\, (V_m - V_0 - C)$.[39] For bitcoin[40], the expected value is given in the second term of equation 15: $a^e_{0,b}\, \rho\, (V_b - V_0 - C)$.[41]
The intuition is as follows: it is a best response to trade if expected value is positive, not trade if expected value is negative, and agents are indifferent about trade when the expected value is zero. In the first case, this means that all agents will accept money[42], so that the probability of accepting money is one ($\pi=1$). In the second case, where expected value is negative, nobody will accept money. So, the probability of accepting money is zero ($\pi=0$). In the last case, where the expected value of accepting money is exactly zero, there is a certain probability for accepting money that is called a *threshold* probability (π^*). This is the

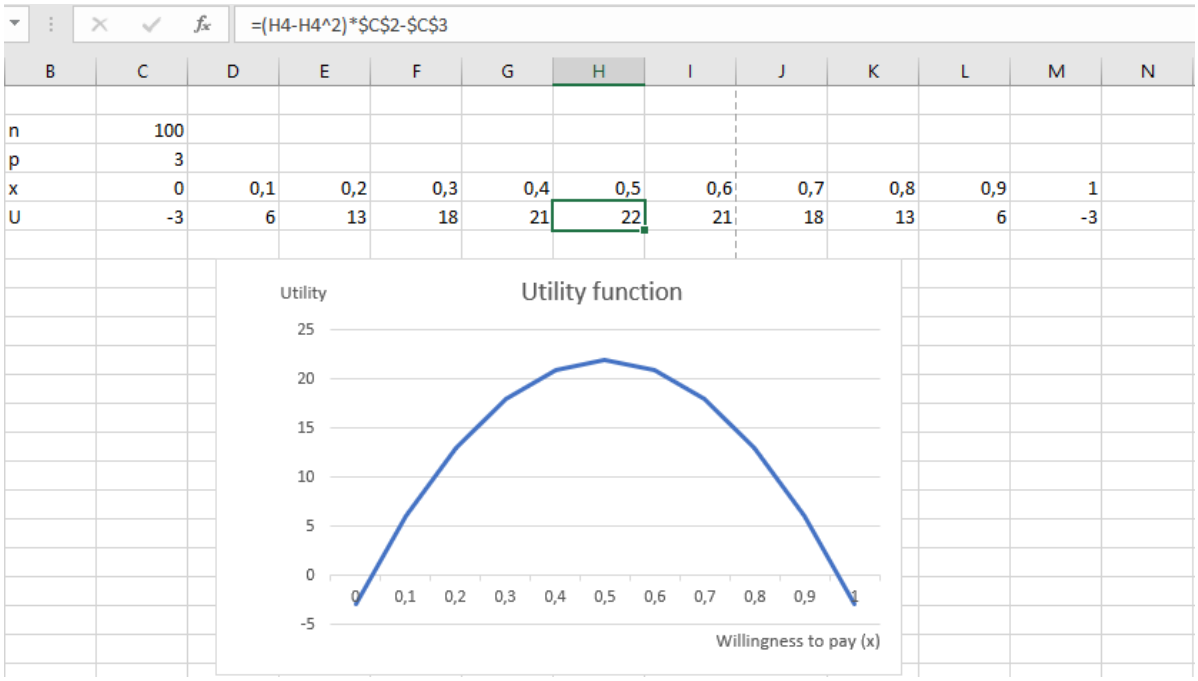
[38] Which depends on the preference shock as explained before.
[39] This expected value is positive if $V_m-V_0-C > 0$, zero if $V_m-V_0-C = 0$, and negative if $V_m-V_0-C < 0$.
[40] In the actual paper, only currency is shown. However, it is straightforward that the expected value for accepting bitcoin is similar and as described above. Therefore I included it for reasons of clarity when showing the equilibria in the next paragraph.
[41] Like currency; the expected value is positive if $V_b-V_0-C > 0$, zero if $V_b-V_0-C = 0$, and negative if $V_b-V_0-C < 0$.
[42] Note that I use money here because the following applies to both currency and bitcoin in the exact same manner. So you can read currency for money or bitcoin for money if that suits you.

probability of accepting money if the expected value is exactly zero. If the actual fraction of agents accepting money is above this threshold value, then everyone accepts money in equilibrium. If the actual number is below this threshold than nobody accepts currency. If the fraction is exactly equal to this probability, some agents will accept money and others do not[43]. How to calculate the threshold value can be found in the appendix.

If the fraction of agents that accepts money is equal to or larger than the threshold value ($\pi \geq \pi^*$ for currency and $\theta \geq \theta^*$ for bitcoin), there exists an equilibrium[44] where money is accepted.

Chapter 4

Excel sheet for discussion on utility function.



[43] Note that the fraction of agents accepting money is then equal to the threshold probability (π^*). So if π^* is 0.4, then exactly 40% of the agents accept bitcoin.

[44] With an equilibrium it is meant that there is no favourable deviation possible from the optimal strategy (=best response).

Chapter 6

Calculating the tax level for which hackers have zero utility from hacking (derivation equation 12).

The utility for hackers is given in equation 11, which is

$$U_h = \frac{(1-\mu(\sigma))*\lambda*b*\varepsilon-\dagger*V_b*S}{H}$$

We are interested in the tax level for which the hackers' utility is zero. This is the case if

$$0 = \frac{(1-\mu(\sigma))*\lambda*b*\varepsilon-\dagger*V_b*S}{H}$$

We can rewrite this as

$$\frac{(1-\mu(\sigma))*\lambda*b*\varepsilon}{H} = \frac{\dagger*V_b*S}{H}$$

Now we want to know the tax level for which this holds, which is

$$\dagger * V_b = \frac{(1-\mu(\sigma))*\lambda*b*\varepsilon}{S}$$

Which is the tax level for which the utility of hackers is zero.

Calculating the tax level for which private agents are indifferent between holding bitcoin and producing (derivation equation 13).

A bitcoin holding agent is indifferent about using bitcoin or producing if

V_b-V_0-C=0

In this case the agent is indifferent between producing and holding bitcoin, which means that the utility from using bitcoin (V_b) is equal to the utility from producing (V_0) plus the cost of producing a good (C).

The utility from producing (rV_0) is the same as in Hendrickson, Hogan, and Luther (2016);

$V_0 = a_m \pi *(V_m - V_0 - C) + a_b \theta *(V_b - V_0 - C)$

The utility function for bitcoin holders is given in equation 10. This is

$V_b = a_b\theta* (U + V_0 - V_b) - \delta_b - (1-\mu(\sigma))*h_s - \dagger*V_b - \mu(\sigma) * \sigma$

If we substitute the formula for V_b and V_0, we get

$a_b\theta*(U + V_0 – V_b) – \delta_b – (1-\mu(\sigma))* h_s – \tau*V_b – \mu(\sigma) * \sigma - a_m \pi *(V_m – V_0 – C) + a_b \theta *(V_b – V_0 – C) – C = 0$

We can rewrite this to

$a_b\theta* (U - C) – (\delta_b+C) – (1-\mu(\sigma))*h_s – \tau*V_b – \mu(\sigma) * \sigma - a_m \pi *(V_m – V_0 – C) = 0$

We want to know the tax level for which this holds, so we rewrite the equation to

$\tau*V_b = a_b\theta* (U - C) – (\delta_b+C) – (1-\mu(\sigma))*h_s - \mu(\sigma) * \sigma - a_m \pi* (V_m – V_0 – C)$

Which is the tax level for which agents are indifferent between using bitcoin or not.

Calculating the cost of security for which private agents are indifferent between holding bitcoin and producing (derivation equation 15).

A bitcoin holding agent is indifferent about using bitcoin or producing if

$V_b-V_0-C=0$

In this case the agent is indifferent between producing and holding bitcoin, which means that the utility from using bitcoin (V_b) is equal to the utility from producing (V_0) plus the cost of producing a good (C).

Similar to calculating the tax for which bitcoin utility is zero, we substitute the formula for V_b and V_0, which gives

$a_b\theta* (U + V_0 – V_b) – \delta_b – (1-\mu(\sigma))*h_s – \tau*V_b – \mu(\sigma) *\sigma - a_m \pi* (V_m – V_0 – C) + a_b \theta *(V_b – V_0 – C) – C = 0$

We want to know the cost of security for which this holds, so we rewrite the equation to

$\mu(\sigma) *\sigma +(1-\mu(\sigma))*h_s = a_b\theta* (U - C) – (\delta_b+C) - \tau*V_b - a_m \pi* (V_m – V_0 – C)$

Which is

$\mu(\sigma) * (\sigma-h_s) + h_s = a_b\theta* (U - C) – (\delta_b+C) - \tau*V_b - a_m \pi* (V_m – V_0 – C)$

Which results in

$$\mu(\sigma) = \frac{ab\theta * (U - C) - (\delta_b + C) - \dagger * V_b - am\,\pi * (V_m - V_0 - C) - h_s}{\sigma - h_s}$$

Which is the probability of buying security for which bitcoin holders are indifferent about using bitcoin.

Calculating the probability that bitcoin holders buy private security for which hackers have zero utility from hacking (derivation equation 16).

Utility function of hackers is

$$U_h = \frac{(1-\mu(\sigma)) * \lambda * b * \varepsilon - \dagger * V_b * S}{H}$$

We want to know where the utility of hackers is zero, so

$$0 = \frac{(1-\mu(\sigma)) * \lambda * b * \varepsilon - \dagger * V_b * S}{H}$$

Which can be rewritten as

$$\lambda * b * \varepsilon - \dagger * V_b * S = \mu(\sigma) * \lambda * b * \varepsilon$$

Which leads to

$$\mu(\sigma) = 1 - \frac{\dagger * V_b * S}{\lambda * b * \varepsilon}$$

Which is the probability of buying security that makes hackers' utility equal to zero.