Is e-Crime the Future of Cryptocurrencies? A Comparison of Bitcoin and Monero Using Smuggling Theory

***Abstract*—Cryptomining both validates transactions and expands the amount of cryptocurrency in circulation. As long as the value of the cryptocurrency created is, or is expected to increase to be, larger than the cost of mining there will be an incentive for rational parties to invest in mining. Simultaneously criminal participants have the same incentives, but with different production costs from leveraging cryptojacking, botnets, or ransomware. Given both legal and criminal participants in the cryptocurrency ecosystem, we argue that models from criminology which include coexisting legal and criminal participants are applicable. Specifically we use a well-established smuggling theory to seek insights on the interactions of these participant types. Using standard smuggling theory, we illustrate that in some domains legitimate cryptomining can be strictly preferable, although criminal transactions will still exist just as zero crime is rarely the case when legitimate markets dominate. Alternatively, there is an equilibrium where legitimate cryptomining is strictly less utility-creating than criminal mining. In the second case, smuggling theory suggests that criminal mining will dominate (again legitimate transactions still exist). We describe the conditions for the two equilibria and argue that each can be seen in different jurisdictions and marketplaces. We highlight the interactions between cryptocurrency protocols and policies with these equilibria. We estimate the cost of legitimate and criminal mining to explore the distance from either equilibria using Monero and Bitcoin as examples. The results imply that the mining structure of Monero is more closely aligned with the incentive structures of smuggling; thus while much of the focus on cryptocurrency has been on dramatic ransomware attacks using Bitcoin, the long term legitimate viability and criminal threat of Monero may be more worthy of attention. We close by identifying policies targeted at tilting the balance towards legitimate mining.**

***Index Terms*—Economics, Cryptocurrency, Smuggling Theory, Cryptojacking, Botnets, Mining, Monero, Bitcoin.**

I. Introduction

The motivation for this work is found in the history of the Bitcoin ecosystem in both legitimate and criminal markets. Previous work examining cryptocurrencies marketplaces has been primarily empirical; focusing on the use of Bitcoin in other crimes [13]), the theft of resources for cryptomining [39], and the re-integration of the stolen Bitcoins in the blockchain after theft [5], [6].

Here we take a very different approach. We build on the work by Garg et al. [22] which modeled botnets as the criminal smuggling equivalent of legitimate networked services. We apply Garg's model to the cryptocurrency ecosystem. Specifically, we use the same theoretical model initially proposed by Bhagwati et al. [9] to examine if there are equilibria where criminal use of cryptocurrency would dominate the cryptocurrency ecosystem. We were also motivated by work of Clayton and Laurie, showing that anonymous use of Proof of Work to prohibit spam is not possible given the presence of botnets [14].

In addition to discussing Bitcoin, we also focus our analysis on Monero. Monero has a shorter history, lower volatility, and production that aligns with the assumption of the underlying analysis. We were further motivated in this choice by the 2018 publications from a CERT-SEU analyst who identified Monero as particularly "appealing to malicious actors" for botnets, cryptojacking, and click-jacking due to its suitability for mining via general purpose CPUs [31]. We describe the Monero ecosystem, distinguish it from the Bitcoin ecosystem, and review the transactional model.

We start with discussing the motivation behind this research in Section II. In Section III, we briefly discuss cryptocurrencies ecosystem history and review the transactional model in Bitcoin and Monero. Section IV supports our application of theories of smuggling by identifying the similarities between stealing resources for mining purposes and smuggling in the physical world. In Section V, we estimate the cost under each of the malicious acts used for cryptomining and compare it to the costs of legitimate mining. We discuss the smuggling theory in Section VI. Section VII applies the theory to the case of cryptocurrencies. It is in this section where we identify the equilibria based on the analysis done on costs of malicious mining versus legitimate mining. Finally, Section IX is dedicated to the conclusion and discussion of the approach, including the positive valuations and prohibitive tariffs developing in different jurisdictions.

Our primary contribution is to leverage smuggling theories from the economics of crime to examine the production frontiers of cryptocurrencies; then use Monero and Bitcoin as examples for a more detailed focus on mining through this new lens. We identify potential equilibria for legitimate and criminal markets. We note how protocol and policy choices in cryptocurrencies interact with these equilibria and evaluate proposals to alter cryptocurrencies based on these observations.

II. Motivation

Cryptocurrencies which use Proof of Work (PoW) have two primary inputs: electricity and processing power. The amount of either is a function of the selected processor and

the type of PoW calculation required. That the electricity and the processing power are a bundle that is stolen in a machine takeover makes production with stolen resources relatively straight-forward. As a result, there is an incentive for theft of these resources in order to engage in mining.

There is a documented history of malware being used to takeover machines to use the resources for cryptomining. For example, in 2012 Plohmann and Gerhards-Padilla documented that the number of bots reached up to 200,000 computers at one point which means, at the time, the computational power of 200,000 computers was being used to mine Bitcoin for a botnet owner [40]. Two years later in 2014 Huang et al. also found multiple botnets mining up to roughly 600 Bitcoins collectively [25]. More recently, other forms of currency beyond bitcoin have been created using stolen resources [39]. Our analysis is specifically grounded in Bitcoin and Monero but can reasonably be applied to other proof of work (PoW) currencies.

In addition to botnets, it is possible to steal resources using cryptojacking. Cryptojacking websites run scripts that use the viewer‘s CPU/GPU to mine cryptocurrencies. In 2018 a team of researchers at Concordia University searched for websites running cryptojacking scripts and found that in the top one million websites, around a thousand of them were running mining scripts for Monero [21]. This means all of these websites used the viewers‘ CPU power during their visit to the website to mine Monero. Saad et al. and Musch et al. have an extensive analysis of cryptojacking scripts that run on different websites [43], [37].

In terms of eCrime, the focus on theft of resources has been on the power that is required for mining and generating new Bitcoins as well as the Bitcoins transactions that are for the purpose of money laundering. On the economic side, there have been multiple studies on how Bitcoin is and could be used in money laundering schemes because of the anonymity it offers. (We acknowledge that this anonymity is known to be limited, e.g, [42], [27].) Bitcoin famously plays a role in payment for ransomware, for example the role of Bitcoin in WannaCry ransomware has been documented. [29].

In terms of the use of cryptocurrencies in other criminal activities, studies have addressed the use of Bitcoin in ransomware and the use of Bitcoin in illegal transactions [16], [28], [7]. An early evaluation by Christin and his colleagues found that Bitcoin played a potentially essential role in the Silk Road marketplace for illegal goods [13].

A 2018 survey enumerated the different money laundering services available on the dark web using Bitcoin [44]. This built on the work of Möser [33] who had investigated anti-money laundering strategies that could be applied to Bitcoin while respecting the anonymity of the Bitcoin users. Anderson has examined past proposals and solutions on how to deal with tainted Bitcoins present in the system [5], [6]. Anderson examined how Bitcoin known to be stolen (as these are by definition unique identifiable strings) are integrated back into the blockchain after the theft. He calculates the value of Bitcoin generated with these stolen goods, and the result is that were the stolen value removed each Bitcoin would experience a considerable loss in value. As a counter-proposal, he builds upon British precedent to propose using a first-in-first-out standard to separate tainted coins from those with only legitimate provenance.

Monero is built on the Cryptonote protocol, which can use a set of mixins to obfuscate the real source of a transaction in order to enhance the privacy of transactions. This makes following the tainted coins in Monero more complicated than in the Bitcoin blockchain. Still, Möser et. al. estimated that 80% of the transaction could be traced back to their real input with eliminating the mixins using some deduction techniques [35]. Kumar et. al. had more success a year earlier, illustrating the ability to identify the initial inputs of 88% of transactions [30]. In addition to these research projects, CipherTrace has filed two Monero tracing patents in late 2020 and claim they can effectively trace Monero transactions [2]. These show that although Monero protocols would make tracking tainted coins more difficult, policies based on tainted coins could be applied to Monero using additional tools and techniques. In our model the ability to trace and discount an illegally generated coin is implemented as a deterrence cost.

In our extension of the current analysis of cryptocurrency ecosystems for both criminal and legitimate purposes, we note that the classic generalized model of a production frontier in economics uses two inputs of potentially varying costs to determine the optimal choices for producers. Therefore it is straight-forward to model the theft of resources for PoW as changes in the production frontier. We discuss two currencies because the production curve for every cryptocurrency varies. We examine both Bitcoin and Monero. The documentation of these differences in the production frontier is a minor contribution of this work.

III. Cryptocurrencies Ecosystem

Bitcoin was introduced in 2009 as a peer-to-peer form of payment with the promise of being a decentralized anonymous currency. Its fundamental innovation was the creative and insightful combination of previously academic proposals: privacy in public, proof of work, and a method for independently creating value through mining. Essentially Bitcoin leverages a distributed cryptographically validated linked list. The bitcoin-creating blockchain protocol enables the decentralization of the associated ledger of transactions. The transactions are posted publicly. There are logs available for every transaction made on the blockchain. Bitcoin miners who are responsible for confirming transactions are required to solve a mathematical question (which involves finding a number that its hash meets certain constraints) which by Bitcoin design takes around 10 minutes to solve. The design builds directly on the initial work by Dworkin [19], using processing power as the basis for the PoW. The first party to solve the PoW challenge is rewarded with a certain number of Bitcoins . the number of Bitcoins if a function of the Bitcoin ecosystem and the commissions committed to in the transactions they have confirmed. The creation of the Bitcoins and the validation of

the transaction are inherently linked as the resulting block is concatenated onto the end of the chain.

Up until mid-2010, there were no exchanges for Bitcoin so the owners and users were dominated by cryptography enthusiasts who would transfer Bitcoin to each other in a spirit of open inquiry. In May 2010, the first transaction was made with Bitcoin, paying 10,000 Bitcoins in exchange for two pizzas. Note that implies each Bitcoin was valued less than a cent. Soon, the popularity increased, and by the end of 2010, Bitcoin surpassed 1$. However, like every other currency, the existence of Bitcoin depended on its acceptability as a medium of exchange; transferring Bitcoin requires people accepting it as a form of payment. The challenge to cryptocurrencies was that like any currency can only be used if it is accepted and can only be accepted if it is widely used; and the early value of Bitcoin beyond novelty was anonymity. The ability to provide verifiable, non-revocable, remote, and anonymous transactions was the driver for early adopters as Bitcoin became a dominate form of payment in online criminal marketplaces. Silk Road, known as one of the first and most popular market for smuggled and prohibitive goods on the web (mainly used to buy and sell proscribed drugs), only accepted Bitcoin as its form of payment as noted by [13].

With more use Bitcoin gained more value; the Bitcoin price started to rise, even eclipsing $1,000 for a couple of short periods in late 2013. Although the price dropped in response to prohibitions from China on the mining and use of Bitcoin , these prices gave more publicity to Bitcoin. In 2017, the price once again reached $1,000, and this time it did not drop. The rise in the price created more demand for Bitcoin, and eventually, the price of Bitcoin reached its first peak of $19,783.06 in December 2017; a recent peak of $27,109 happened in late 2020 [3]. Following the 2017 year-long surge in the price, the price began to drop, and between 2017 and 2020 the value of Bitcoin fluctuated between $4000-$12000. That volatility of bitcoin outstrips that of other fiat currencies is beyond the scope of current model. (Please see [11], [20] for discussions of Bitcoin volatility.)

As mentioned earlier, the mechanism for expanding the supply of cryptocurrency is expanded by mining. Every 10 minutes, a block is generated, and its miner is rewarded with a certain number of Bitcoins. According to the Bitcoin protocol, the initial reward was 50BTC per block and every 210,000 blocks (roughly four years), the reward is halved (currently the reward is 6.25 BTC per block).

To ensure a block is generated every 10 minutes, the difficulty of the mining challenge is determined by the rate at which recent challenges have been solved. If the recent challenges were solved in less than 10 minutes on average, the challenge will get harder, and if the solution time averaged more more than 10 minutes on average, the difficulty is decreased. Solving these challenges requires computational power rather than mathematical acumen, so anyone with a processor can participate in mining. The more difficult it is to solve the challenge, the more computational power needed to solve the challenge in 10 minutes. Despite the prospect of decreased numbers of Bitcoins as a reward, the remarkable increase in price led to a corresponding increase in mining Bitcoin. Given the relatively straightforward link between having computational power and making money, there was a corresponding increase in investment in computational power. In this work, we examine the investment in computational power as investments in two markets: the legitimate trade of computational power and the use of computation power that is neither owned nor leased by the miner.

In the Bitcoin market there appears to be stabilization of mining and transactions. In terms of mining, the specific requirements for creating a hash collision can be optimized by using Application-specific integrated circuits (ASICs). The availability of ASICs for mining has fundamentally changed the production frontier, so general purpose CPUs are no longer competitive. In our discussion we consider the applicability of our results on the Bitcoin ecosystem before the widespread adoption of ASICs.

Monero mining follows the same overall structure as Bitcoin. A mathematical proof-of-work must be solved to successfully mine Moneros. The time to mine a Monero block is around 2 minutes and each successful instance of mining is rewarded with a grant of roughly 1.25 XMR (Moneros). However, the main difference between mining Monero and Bitcoin is that Monero proof-of-work does not use an ASIC-friendly algorithm and thus the mining will likely remain competitive on CPUs or GPUs. This means even a personal computer with a strong CPU/GPU could be a useful hardware for mining Moneros, in contrast to the hardware chipsets optimized to mine Bitcoin.

The range of legal and illegal sources of computation power underlie this analysis. The large number of computations needed for mining results has resulted in the formation of pools, as individuals share their devices. In pools members contribute computation resources and when cryptocurrencies are awarded after mining, members in the pool are granted a portion of the rewards, relative to the computational power they have contributed.

The need for computational power and the promise of anonymity enable comparison to smuggled, illegal goods. Cryptocurrency criminals seek to steal processing power and electricity for mining to reduce production costs, just as smugglers seek to avoid tariffs.

IV. Mining and Smuggling

Criminology research addresses both criminal and legitimate trade and activities, often finding these in the same market. For many goods the flow of assets between those markets results in demand being modeled as a single curve, with the same demand being served by all producers. Here we treat cryptocurrency as such a market: there is a demand that can be fulfilled by criminal mining or legitimate mining. Despite the nomenclature of currency and the dominate design goal for simple private transactions, cryptocurrency has a contested nature as inherently valuable asset, monetary instrument, or commodity. Here we begin with the assumption that the

Department of Treasury is correct, cryptocurrency is an asset, one that is distinguished by its volatility and unusual risk characteristics [17], [18]. With that as a plausible functional assumption, we can use a standard comparison of goods which can exist in both licit and illicit markets to examine the dynamics of the licit and illicit cryptocurrency markets.

Previously Garg [22] made the argument that botnets could be examined using the model of smuggling. This underlying theoretical structure was used both to propose policies towards the ecrime and to contribute to the explanations for the concentration of botnets, spammers, and other components on ecrime in different regions, just as smuggling of different types is concentrated in distinct regions.

In cryptomining, as with any business, the profitability is primarily a function of long run marginal cost. This the cost of producing one additional unit of production, which is the cost of the electricity. Below we examine two models for legitimate mining, one where processing power is assumed to be a fixed cost (and thus not part of long term marginal cost) and then expand this to try to capture marginal processing cost. For botnets this is the cost of obtaining an additional machine for mining; for ASICs the marginal cost of processing is identified as a source of uncertainty. As a result of the difference in ASICs and botnets, the result is that the smuggling cost is decreasing relative to the legitimate cost. Essentially our core assumption is that any miner can vary the two primary essential factors of production: processing power and electricity.

As a result of the number of computations that these hardware devices do, maintaining the devices can be an issue due to heating, especially for facilities that hold a large number of these devices. We acknowledge this and other maintenance cost is a weakness as we focus on a two input production model. We note that recent work by Collier and his colleagues at Cambridge illustrated that the customer support and maintenance cost in ecrime is quite similar to that of legitimate businesses [15].

To return to the case of mining, a number of computations must be completed in a certain amount of time in order to successfully mine. This number has been increasing in the aggregate in the past years for all of the cryptocurrencies. At times the necessary number of computations is so high that a miner using the best device available would either be experiencing a loss, or face a long term multi-year path to cover the cost of their processing platforms using mining profits unless electricity prices remained under $0.09 per kWh. Recall this is only considering the electricity as marginal cost, and not any overhead such as facilities space or maintenance. An analysis of cross-national production, volatility, and global distribution similarly concluded that electricity cost, coin value, and volatility were the dominant determinants of global supply, supporting this analysis [38].

Another similarity is in the existence of national prohibitions. There are propositions to prohibit cryptomining in multiple jurisdiction around the world (mainly those countries with lower electricity costs). For example, both the Chinese and Iranian governments have made policy statements about the value of removing the drain of cryptomining from their national grid [8], [1]. Iceland continues to have a complex relationship with the cryptocurrency community [24]. Globally the governmental responses range from zero tariffs to prohibition [38].

V. Production Costs

In this section, we define the smuggling model used for our analysis. To begin we discuss the cost models of three different mining methods.

A. Legitimate Mining

1) Bitcoin: Here we are focusing on modeling the two possible marketplaces an abstract model of production is useful. The issues of legitimate and illegitimate production spans different cryptocurrencies. For our illustrative example currency we will include the cost of mining in Monero, which is more suitable for mining with personal computers.

In the earlier days of Bitcoin, miners would use their personal computers for mining purposes; however, general-purpose machines are far from optimal. As a result of this, there are ASICs (Application-specific integrated circuits) that are designed to do the computational work needed for mining optimally. At the time of writing this paper, the best ASIC is AntMiner S9 which can do 13.5 TH/s ($13.5 * 10^{12}$) with a power consumption of around 1.35 kWh. Although the price of ASIC itself and the costs of maintaining the ASIC due to heating are not low, the main cost for mining using ASICs is the electricity cost. The current network hash rate is around 132 million TH/s, which means, if we can hash at this rate for ten minutes (the duration between two successive minings), we can mine successfully and get the associated 6.25 BTC reward. So the number of ASICs needed for a successful mine is as follows:

$$N = \frac{132 * 10^{18}(\frac{Hash}{s})}{13.5 * 10^{12}(\frac{Hash}{s})}$$

Which is 9777777 AntMiner S9s. The electricity costs for one Bitcoin would be:

$$Cost = N * 1.35(kWh) * ElectricityRate(\frac{\$}{kWh}) * \frac{1}{6} * \frac{1}{6.25}$$

The division by 6 is because our power consumption is in hourly rate and each block is mined in ten minutes, and the division by 6.25 is because in each successful mine, the miner is rewarded 6.25 Bitcoins and we are calculating the cost for one Bitcoin. The electricity rate differs in different parts of the world. In the United States, the minimum electricity cost is $0.08 per kWh, and the average rate is around $0.12. So the minimum cost would be $28,160 and the average cost would be $42,240. Considering the fact that the Bitcoin price is currently $31,000, one can see how close it is for mining not to be profitable in the United States even with the lowest electricity rates. It is interesting to mention that Bitcoin value has surged by a %100 during the past couple of months, which means a couple of months ago the gap between the cost and the value was even greater than what it is right now. Also

recall that we are not considering the hardware and heating cost associated with starting and maintaining mining. No one owns this much computing power; however, everyone can contribute to mining pools and get rewarded relative to the computational power they have contributed to the mining pool. The administrators who run these pools charge fees when a Bitcoin is mined, which is another source of cost. You can see the profitability of Bitcoin mining from March 2020 - Feb 2021 in Figure 1.

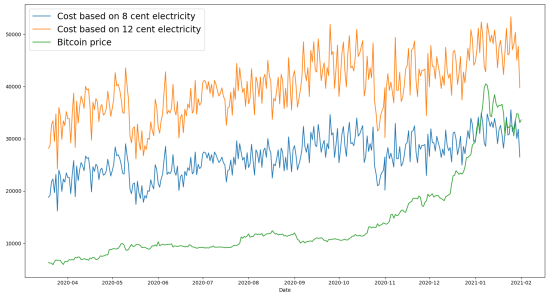

Fig. 1: Comparison between the Bitcoin value and its cost with different electricity costs.

2) Monero: At the time of this paper, the best CPU for mining Monero is AMD EPYC 7742 which can do 44,000 H/s that is a 225W CPU. The current network hash rate is around 1.3 GH/s, which means hashing at this rate for two minutes (the duration between two successive mining operations) results in success and the associated 1.25 XMR reward. The number of ASICs needed for a successful mine is:

$$N = \frac{1.3 * 10^9(\frac{Hash}{s})}{44 * 10^3(\frac{Hash}{s})}$$

Which equals to 29545 CPUs. The electricity costs for one successful mine would be:

$$Cost = N{*}0.225(kWh){*}ElectricityRate(\frac{\$}{kWh}){*}\frac{1}{30}{*}\frac{1}{1.25}$$

The division by 30 is because our power consumption is in hourly rate and each block is mined in two minutes and the division by 1.25 is because each successful mine yields 1.25 XMR. By using the same minimum and average electricity costs that we used in the Bitcoin section, the minimum cost for mining one Monero is \$14 and the average cost is \$21. Comparing with the Monero value which is \$169 at this time, we can see that the reward will outperform the electricity cost, however, considering the fact that these CPUs cost around \$7,000 it would take miners more than 5 years to just pay back the cost of the CPUs (remember this is mined with N CPUs, so the hardware cost is $N * 7000$). On top of that one should remember to consider the costs of maintaining and mining pools to have a more accurate calculation. The profitability for Monero in the past year is illustrated in Figure 2.

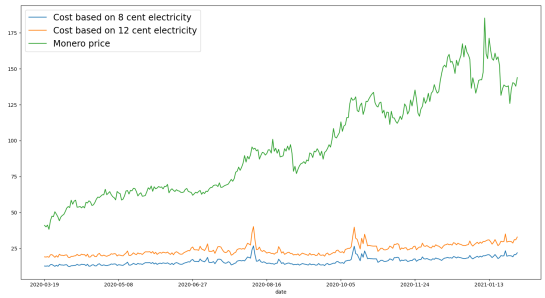

Fig. 2: Comparison between the Monero value and its cost with different electricity costs.

B. Botnets

In this section we look at the profits made by botnets mining Bitcoins and Moneros.

1) Bitcoin: In this model we were informed by the results of Huang et al. in estimating the costs of a botnet and the profitability of these botnets [25]. We specifically examine the botnets mentioned in their research paper: ZeroAccess and BMControl. According to their findings, ZeroAccess mined 486 Bitcoins during the span of roughly 1.5 years with an estimated return of \$8,300. BMControl ran for one year, mining 3,097 Bitcoins with a dollar value of around \$46,300 at that time. These numbers indicate the profits from the use of botnets to mine. Consider that a botnet is a general input, and can be used for multiple activities. For example, consider the cost structure and low marginal returns of spam, where tens of millions of emails (with the interrelated cost of email account creation, target acquisition, and customer service) may result in a handful of purchases [26]. Of course, the processing requirements for cryptocurrencies are orders of magnitude greater than those of spam.

Using a botnet to mine requires building, renting, or taking over the infrastructure. In terms of building a botnet as business, Putman [41] described the spread of malware, including the economics of distribution. We also leverage their pay-per-install model in which botnet masters pay a certain amount of money for every thousand unique infected devices. Caballero et al. [12] described the pricing of the use of botnets, once constructed. Their results documented how the prices for infected devices differ based on their geographical location, with devices in US and UK valued at \$100-\$180 per thousand installs, devices in other European countries ranging from \$20 to \$160 for a thousand installs, and other countries priced below \$10 for every thousand installs. We use the average numbers mentioned in this work, (\$140 for US and UK, \$90 for other European countries and \$5 for other countries) to estimate the cost of the two mentioned botnets. Huang et al. show a distribution by country of the devices enrolled in each of the botnets. Our model uses Huang's density measure and used a weighted mean for costs based on the geographical location of the bots. Using this approach,

we estimate that the cost of ZeroAccess as roughly $750 and the cost for BMControl as $10,400 for the entire lifespan of the botnets.

2) Monero: To calculate the cost of mining Monero on a botnet we use the results of the thorough research done by Pastrana et. al. in late 2019 [39]. They investigate the behavior and gains of multiple botnet campaigns and report their findings. Their research examines Photominer, Adylkuzz, Smominru, Xbooster, Jenkins and Rocke botnets. They report that the top ten botnet campaigns made a total of $38M while all of the campaigns made $58M during their active period. During this time, the highest earning campaign made around $20M in a span of around three years and was still active at the time of publishing the paper. They also show how their reported amount of Moneros mined illicitly summed up to around %4.5 of all the outstanding Moneros at the time.

To compare the production of legitimate and illegitimate mining, we need to estimate long run marginal cost for each. For the case of illegitimate mining, the cost of botnets is dominated by the cost of the malware distribution. This cost tends to be lower than the mining rewards, given historical pricing. Botnets have a higher setup fees due to the need for distribution of the malware, and after that, they face minimal continuing costs, while legitimate miners pay effectively noting but fixed cost of a processor, but have to pay the potentially high electricity costs to keep mining. Long run marginal cost for botnets integrate the cost of enforcement, referred to deterrence cost in smuggling models.

C. Cryptojackers

Cryptojacking refers to the use of scripts on a website that harness the viewers‘ CPU to mine cryptocurrencies for the duration of the connection to the website. This duration may be moments, or an open tab may allow for extended mining. Scripts for mining cryptocurrencies are typically set up in one of two ways. The first method is when a website owner purposefully decides to run these scripts on their own website as an alternative or in addition to ads to monetize its viewership. And the second method is via subversion: when an attacker takes advantage of security vulnerabilities in a website to inject malicious scripts into the website to use the viewers' CPU to mine for their own gain.

Saad et al. [43] illustrated that although many of the top one million websites run cryptojacking scripts, the revenue made from cryptojacking is orders of magnitude less than what they would make from ads. As a result, they argue that cryptojacking could not replace ads as a monetization technique for websites. However, cryptojacking and advertising can coexist on a website; there is no need to forego advertising for cryptojacking. In economic terms, these are not substitutes so that an increase in one does not imply a decrease of the other.

Due to its design, Monero has been the cryptocurrency of choice for cryptojackers. As a result, we focus on Monero mining scripts in our analysis of malicious cryptojacking. In 2018 a security vulnerability was found in Drupal, a content management framework run by 2.3% of internet websites. Attackers started exploiting this vulnerability to inject cryptojacking scripts into vulnerable websites, in attacks called Drupalgeddon 2.0. In May 2018, a researcher from Bad Packets LLC., Troy Mursch, wrote a blog about the websites effected by these scripts (the blog has been updated multiple times since then) [36]. He was able to locate more than 300 websites infected by these scripts, including governmental and university websites. He identified roughly 115,000 websites vulnerable to the attack. Around the same time, Matthew Meltzer and Steven Adair from Volexity, a security firm, wrote a blog on the profits made by Drupalgeddon 2.0 [32]. They found the wallet address linked to the Drupalgeddon 2.0 scripts which had been active for roughly a year. The wallet address had been used in two different mining pools. In one of them, there was $13,400 worth of Moreno mined, and in the other one, there was $105,566.80 worth of Moreno at the moment of the announcement. This shows that this attack was able to mine around $120,000 worth of Monero in a year. We estimate the upper bound of the costs for this attack. We assume that all 115,000 vulnerable websites found by Mursch were infected by a pay-per-install malware service. Based on the average costs discussed earlier in the paper, the cost of such an attack will be around $10,500. These costs are one-time setup costs, and as long as the scripts are running, the attacker is making money from other users‘ resources. This return of a thousand percent on investment is unusual in legitimate commerce.

In contrast to the focus on malware, a comprehensive survey of cryptomining in 2019 found that the cryptomining by third party apps dominated. That is, rather than being the result of malware or web site takeovers, cryptomining was embedded in third-party services and add-ons. The websites were not subverted, but were rather bundling the code as part of the served package with content and services. The results of this large scale study were that such quasi-legitimate mining was three time the size indicated by previous work [10]. In this work we consider this cryptomining software as part of the smuggling category.

VI. Smuggling Theory

In 1973, Bhagwati et al. first proposed the smuggling theory [9] we use here. It was an intellectual innovation in that it recognized that smuggling could be utility optimizing. Before that time, smuggling models presumed that like other criminal activity, i.e. violent crime, smuggling could not attain a stable equilibrium and that legitimate markets need only be nudged into dominance. The foundation of the model is production possibility curve (or production possibility frontier). In production possibility graph, each axis represents the amount of a produced good. The x and y axes are the inputs, which normally are vast simplifications but match the processing power and electricity inputs required for cryptocurrency mining notably well.

The production possibility curve assumes good A and B use the same resources. Different production curves embed different constraints and limitations of each, and shows what is the maximum number amount of the goods A and B can be

produced. We provide a basic production possibility graph in figure 3. In this figure, for point 1, there are unused resources, so production would expand until all available resources are used. Point 2 shows a point on the production curve illustrating optimal use of the resources so that increasing one good would require decrease in the other. In contrast point 3 represents an impossible production given the constraints and resources. In smuggling theory, the two goods under consideration are legitimate and smuggled goods each of which has its own production cost given the available inputs.

Without loss of generalization we can select three points on this curve, which represent production points for free trade, in the presence of tariffs, and smuggling. You can consider them as slight shifts based on different costs of inputs. Note that in this paper we only need to consider two production points: optimal production in the presence of tariffs and optimal production for illicit goods. We use the tariff example rather than the free trade conception, as under Bhagwati et al's model free trade has no associated regulatory nor maintenance cost.

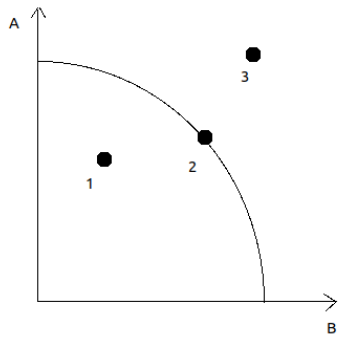

Fig. 3: An example of production possibility graph

In Figure 4 any point on the graph shows how much of a good is produced with inputs A and B. The transformation curve shows the classic abstract production from available inputs. In this case, the cryptocurrency is modeled as produced by processing power and electricity. Smugglers produce from stolen goods, cryptojacking, or using legitimate production to avoid sanctions, money laundering regulations, or other prohibitions that are typically modeled as expensive tariffs. However, they do not pay for electricity or processing power. Legitimate producers pay for electricity, and we extend our model to consider processing power.

Here P_T is the optimum production point in the legal trade and P_S is the desired production point of smuggling. The domestic price is the tangent to curve at P_T. A transformation curve is drawn from each of these points. In a transformation curve the slope at each point shows the cost to produce one more unit of the good at that point. The cost of legitimate production is always constant and thus the transformation curve is a line for the legal trade production point. However, this might not be the case for smuggling in which the costs could be constant, increasing, or decreasing depending on the situation. Figure 4 shows an example of such a curve when the costs for increased legal and illicit production are both constant. In this example, the cost of producing or trading the good legally is greater than the cost of smuggling it. Therefore, its transformation line is steeper than smuggling's transformation line. Note that, neither of the transformation lines are as steep as the domestic price, which is the tangent at P_T. C_T and C_S represent the consumption rate of the consumers.

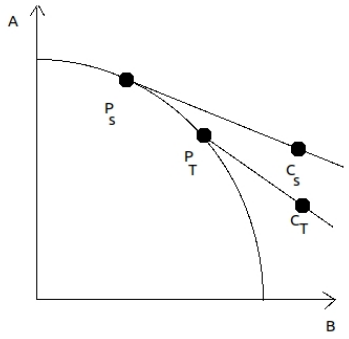

Fig. 4: Transformation curve with constant costs

To continue with our application of the smuggling theory, we need to define utility and social indifference curves. Utility is the satisfaction consumers receive by choosing and using a product. Indifference curves are curves that every point on the curve has the same utility for the consumer. These curves are usually drawn as convex because when a consumer has a large number of good A and a small amount of good B, replacing large amounts of A with small amounts of B will result in the same utility.

Figure 5 shows a set of indifference curves. In this figure, all the points on indifference curve one (IC_1) have the same utility and all the points on indifference curve two (IC_2) have the same utility as well, however, the overall utility on the indifference curve (IC_2) is higher than indifference curve (IC_1). As a result, if one has a budget line of L1, it would be best for them to buy the combination of goods represented by point A to maximize their utility as the line is tangential to an indifference curve. (In this case, the processing and electricity could be used for gaming, other commerce, or in the case of smuggling, spam or phishing.)

In our smuggling theory sample, the consumption rate of the smuggling is found by maximizing the utility given the transformation line. The indifference curve that is tangential to the smuggling transformation curve will highlight the smuggling consumption rate. However, for legal trade, the consumption

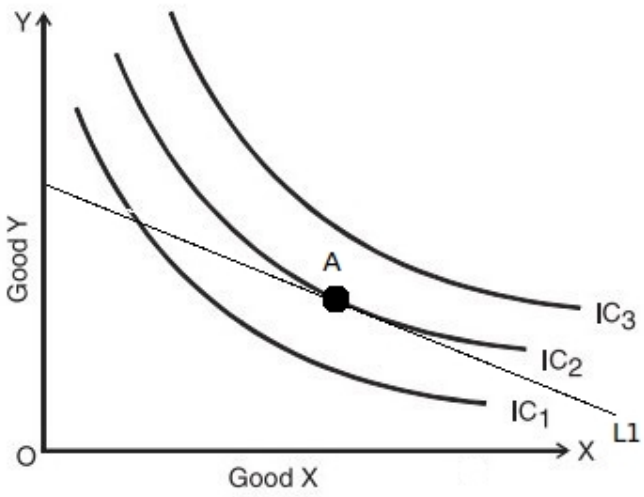

Fig. 5: A sample of indifference curves where the utility of all points on each curve are the same, and the utility of $IC_n > IC_{(n-1)}$

rate is not obvious. Bhagwati et al. would pick two points, one on which the utility will be less than that of the smuggling consumption rate, and one where the utility is an improvement on the smuggling utility and then discuss the feasibility of the two situations. We will use the same process in this paper. It is worth mentioning that utility curve in the legal trade is drawn tangential to the cost line drawn from C_T and not tangential to the transformation curve itself.

VII. Smuggling Approach to Mining

We assume perfect competition in the cryptomining market, which means all of the cryptocurrencies in a system face the same production cost, utility, and price. Same as the model, we assume that the community is indifferent about the origin of the good they receive. In other words, we assume a cryptocurrency user makes no distinction between the cryptocurrencies generated legitimately and those generated criminally.

A. Mining Under the Current State

Our model, or rather our adoption of Bhagwati's model, is depicted in Figure 6 and Figure 7 using the same concave production curve. P_S is the desired production point of smugglers, and P_T is the production rate in a legitimate market. The slope of $P_T C_T$ shows the cost of production under tariffs, which for us is the cost of legitimate mining. The same applies to $P_S C_S$; the shape of the curve illustrates that it is arguable that the marginal costs for stealing resources decreases over time. In other words, an assumption that taking over more computers is easier when botnet is already established is embedded into the model by the negative slope from P_S to C_S. At some point the lowest marginal cost is reached and the cost line approaches constant. Notice that the slopes show the marginal costs and do not include fixed costs, as the model is of the long term state. As a result, the slope for $P_T C_T$ is more than the slope for $P_S C_S$ even before marginal costs become decreasing. Lastly, U_T and U_S show the utility achieved using a tariff-based environment or smuggling-based environment showing utility of smuggling $U_S > U_T$ in Figure 6 and utility of legal trade $U_T > U_S$ in Figure 7. In the first case, the smuggling is welfare-increasing and in the physical world, such a case would result in legal trading ceasing to thrive, as the cost of illicit production is lower, and the utility is higher. In other words, smugglers could provide the good for a price that legitimate importers can not match. However, in our case we focus on the production of a good (cryptocurrency mining) where the value of the good is exogenously fixed in the market, this will not necessarily result in a suppression of legitimate mining.Therefore mining process might be still profitable for legitimate miners (which we discussed in detail in Section V). Thus they will continue to produce. However, should the price fall significantly it is possible that there will be an equilibrium at which legitimate mining becomes unprofitable and only illegitimate mining remain profitable. In the case where legitimate mining is welfare-increasing (Figure 7), you can see that the consumption rate is close to the maximum rate, which means only the maximum rates of consumption in this case can lead to an increase in utility compared to smuggling. Although these consumption rates are possible, in real world they are highly improbable.

In the following discussion we begin with the possibility that under the current state and policies, the equilibrium is the one under which smuggling is welfare-increasing and theoretically could suppress legitimate mining in the long run.

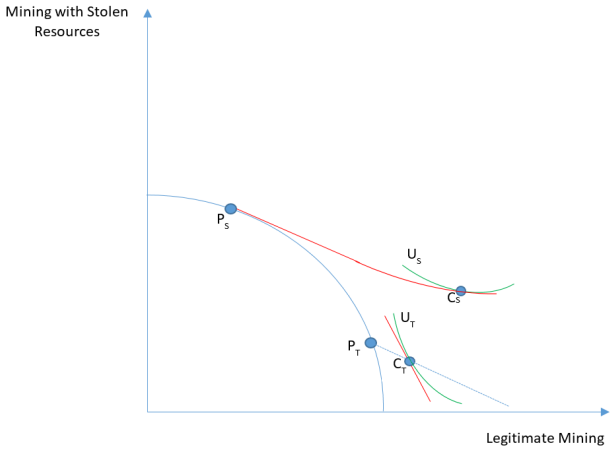

Fig. 6: Perfect competition in cryptocurrency mining at the current state with smuggling having a greater utility

VIII. Tainted Currencies

In this section we discuss the proposed policies which have been recommended to address the criminal production and uses of Bitcoin. While these could be used for Monero or any other cryptocurrency we use Bitcoin as the focus of the discussion due to the richer historical data and wealth of research. As noted above applying such techniques to Monero

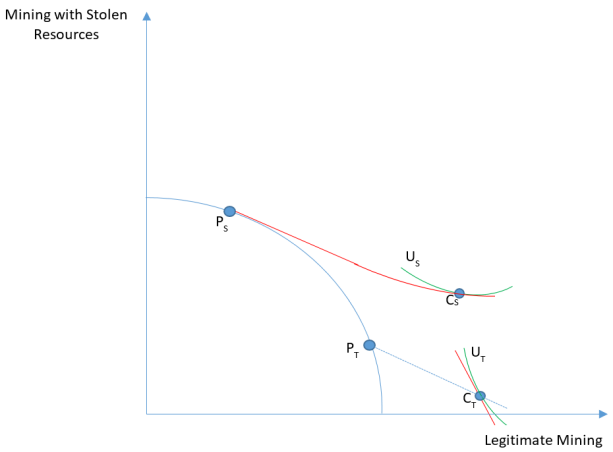

Fig. 7: Perfect competition in a cryptocurrency mining at the current state with legitimate mining having greater utility

would need the use of additional tools to help with tracking of tainted coins.

We start with the work of Anderson, who argues that legalizing the Bitcoin industry should start with tracking known stolen Bitcoins [5], [6]. He begins his analysis with the previous proposals by Möser et al., which suggests two approaches for dealing with stolen and illegal activities: 'haircut' and 'poison' [34].

In the poison approach, if one stolen Bitcoin is added to a wallet then all Bitcoins in the wallet are considered stolen. This approach has the advantage that criminal wallets, not simply individual Bitcoins, are removed. With a poisoning policy one identified stolen Bitcoin added to a wallet results in all the Bitcoins in the wallet becoming worthless and unusable for transactions.

In the haircut approach each Bitcoin in a wallet is decreased according to the number and value of Bitcoins in that wallet. For example, if one stolen Bitcoin is deposited into a wallet which already has four Bitcoins in it, after the deposit, all Bitcoins in the wallet are considered 20% tainted. In this way, moving Bitcoins between wallets to launder them would no longer be feasible. The objection to this proposal was propagation of the dilution. This approach leads to the propagation of the taint when one stolen Bitcoin can lead to many tainted Bitcoins further down the blockchain. Conversely, it also limits the ability of attackers to use pass-through accounts to obfuscate ownership of even large numbers of stolen Bitcoins such as documented in the network analysis of Goldsmith [23]. They illustrated that different groups leveraged distinct identifiable approaches to cashing out and that approaches to identifying one criminal transaction does not match to another.

In contrast, Anderson proposes a FIFO approach in which they propose that the first Bitcoins spent from the wallet are the first Bitcoins that were deposited into it. In this way, one can track the exact stolen Bitcoins, and those are not mixed into other legitimate Bitcoins.

All of these approaches assume that as soon as criminal Bitcoins get identified these can be tracked, and one can embed criminal deterrence into ta cryptocurrency ecosystem. Thus the stolen Bitcoins will start to lose value based on these policies. Here we model this cost as deterrence costs in criminal mining.

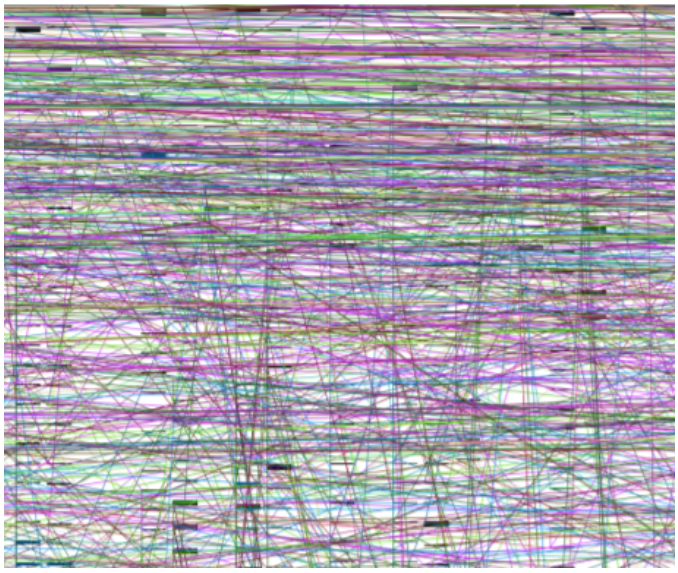

Fig. 8: Ahmed, Shumailov, and Anderson illustrate the complexity of tracing taint through the blockchain, which includes the challenge of identification of criminal actors. The above illustration from [4] that visualizes the remarkable density of taint in the blockchain, also illustrates the coexistence of robust legal and criminal markets.

In this section, we make the admittedly bold assumption that the same tracking systems proposed for theft are applied to illegitimate mining, so if at any time it is understood that a block is mined via stolen goods, the Bitcoins generated for that mining could be considered tainted and can lose value. Arguably, this would align with the identifiability of IP addresses in the blockchain [27], [36] as well as the identification of relative few large-scale cryptojacking operators in [36]. This loss of value acts as a risk and cost for the production of cryptocurrencies. We integrate this cost as a deterrence cost by shifting the production cost, again aligning with classic smuggling theory. The equilibria for these cases are shown in Figure 9 and Figure 10. As a result the marginal cost for illegitimate mining increase. In addition, the marginal costs are no longer considered decreasing because of the increasing likelihood of detection. Recall that deterrence is the product of likelihood of detection, likelihood of enforcement action, and cost of enforcement action. The likelihood of detection increases with scale, although it is easier to add bots to a mature botnet or increase diffusion of widely-installed cryptojacking scripts, expansion leads to increased risk of detection. In addition were any of the FIFO, poison, or haircut approaches to be adopted the enforcement would be integrated into the protocol, so expected cost would be increased as the criminal cryptocurrencies would certainly lose value.

We assume the cost of increased risk of deterrence is equal to the decreased marginal costs of botnet expansion and the result is roughly constant costs for illegitimate production. Note that the poison approach, where the risk is losing all of the generated cryptocurrency, the model would result in greater deterrence costs. Yet the distribution of tainted coins in the Bitcoin ecosystem under the poison model results in a situation where there is such potential widespread loss that we perceive the adoption of this approach to be least likely. The density of taint in transactions in figure 8 from [4] supports this argument.

In contrast, tainting is shown in this case the equilibrium in which the $U_S > U_T$ will only happen when the consumption rate for legitimate mining is already minimal. Such minimal participation of legitimate mining would indicate little to no valid use, and would indicate that the legitimate mining of the cryptocurrency was collapsing. The other equilibrium shows the situation where $U_T > U_S$ and as a result smuggling is welfare decreasing. These models assume that the impact of haircutting or poisoning on legitimately produced coins is negligible. In fact only if FIFO is selected as the mechanism for bringing cryptocurrencies into reliable legitimate commerce could we be confident that the effect on legitimate coins would be negligible. FIFO would result in no impact or loss of value in legitimate production.

These results support the adoption of some form of taint tracking. The high cost of smuggling could lead to legitimate mining suppressing illegitimate mining if the cost of deterrence is increased. Note that this could improve the health of the ecosystem, as the cryptocurrency ecosystem depends on profitability of legitimate mining to thrive.

While the identification of stolen bitcoins from some attacks, such as massive hacks, is straight-forward identification of any coin created by click-jacking, botnet production, or with ransomware wallets that are not detected is a challenge.

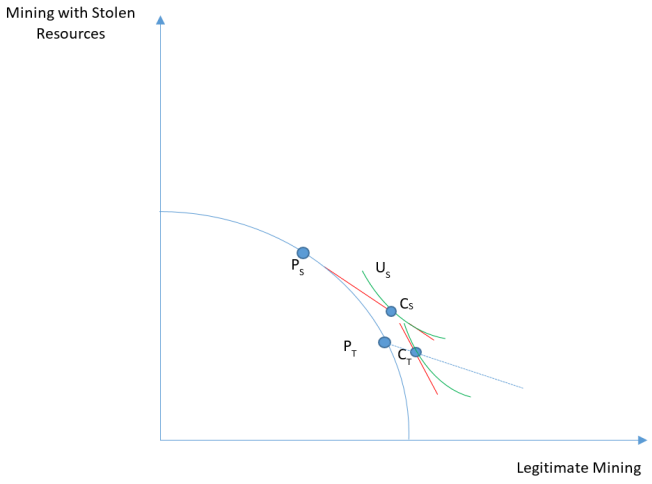

Fig. 9: Perfect competition in cryptocurrency mining with the inclusion of cryptocurrency tracking with smuggling having greater utility

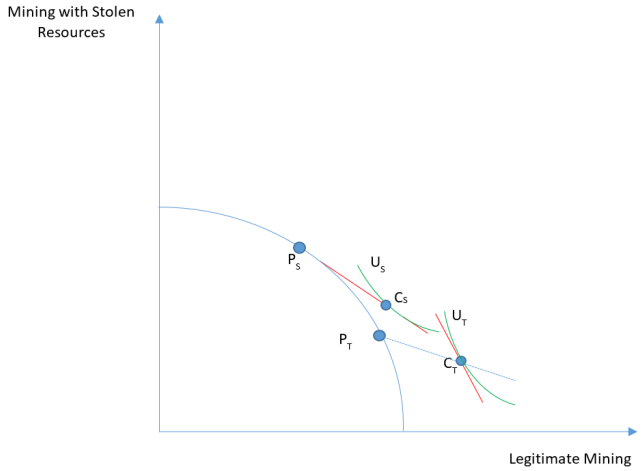

Fig. 10: The model of cryptocurrency mining with the inclusion of cryptocurrency tracking with legitimate mining having greater utility as a result of the loss of utility due to tainting policies.

IX. Conclusions and Future Work

In this work we argue that the theft of resources to lower the costs of mining in cryptocurrencies is analogous to smuggling. Building on that and leveraging smuggling theory, we show that with the current state of cryptocurrencies, there is a possible equilibrium where smuggling forces legitimate mining out of the market. This equilibrium requires either low cost, low expectations of future cost, or the existence of no substitutes. The existence of this equilibria supports the adoption of tracking algorithms such as those proposed by Anderson [5], [6] and Möser et al. [34]. Where only legitimate actors are mining and all of them are at a loss, the reactive nature of the protocol significantly contributes to the survival of cryptocurrencies. Our results both supports the proposals to introduce policies to track tainted cryptocurrencies in order to add deterrence cost to illicit cryptomining while simultaneously identifying the influence of the choice of PoW mechanisms as highly variable in terms of their resilient against such an outcome.

It is important to reiterate that one of the main reasons for Monero becoming the cryptocurrency of choice for cryptojackers is the PoW protocol which is not ASIC-friendly. If Monero were to adopt an ASIC-friendly algorithm for their PoW, personal computers would systematically be less useful for mining Monero and thus cryptojackers would have less profits.

We believe that our results can be supported by examining the history of Bitcoin through a lens of smuggling. In the earliest days of Bitcoin, a considerable share of its transactions were highly concentrated in e-crime transactions. As Christin showed in his research on Silk Road, over a period of 29 days, Silk Road transactions accounted for 4.5% of Bitcoin transactions across all exchanges [13]. This is an example of how criminal use, associated literal smuggling, increased the value of Bitcoin . The use of Bitcoins in illegal transactions

was arguably welfare increasing when both mining costs and Bitcoin values were low. In this paper we examined criminal and legitimate production of cryptocurrencies, including Bitcoin, under different production models.

When the cost of mining was low and the value of the coins was similarly far less the supply of tainted Bitcoin could have been an important component of the Bitcoin supply. However, when there was a lower production curve for illegally produced Bitcoin, it was possible for an equilibrium to exist where legitimate miners were excluded from the mining pools. When it was the case that it was possible to mine Bitcoins using a general CPU, using botnets for Bitcoin mining was a significant problem. However, the use of ASICs changed the production frontier of legitimate Bitcoin such that criminal activity in the actual mining process is no longer common.

For any cryptocurrency exclusion of legitimate miners from the mining pool could be prevented with sufficient deterrence cost; not only on the use of stolen coins but also on the use of stolen cycles. Tracing the wallets used in malware and cryptojacking and applying FIFO, haircuts, or other deterrence costs are feasible approaches to avoid the risk of such an equilibrium.

Beyond policy changes that could be suitable for any cryptocurrency the specific design of PoW for Bitcoin has made it less attractive over time for criminal mining. In contrast to Bitcoin, the PoW of Monero democratizes mining by using a PoW mechanism suitable for CPUs. Conversely, the tremendous cost of carbon associated with mining protocols that use processor-based PoW would then also be associated with Monero. This observation indicates the complexity of modeling the risks and costs of ccs.

For future work, we hypothesize that the reactive mechanisms that exist in Bitcoin and Monero mitigates the risk of a dominant smuggling equilibrium as the price of mining changes as more parties exit the market. One component of future work is expanding these models to include systematic feedback and examining the resulting dynamics. Also examination of global distribution of cryptocurrencies, electricity prices, and deterrence would enable global comparisons to examine potential smuggling havens for various cryptocurrencies. A comprehensive dynamic model of cryptocurrencies that would necessarily include the costs of carbon as well as the cost of theft and ransomware, and thus is a longer term project.

REFERENCES

[1] Iran seizes 1,000 Bitcoin mining machines using subsidized power. https://www.reuters.com/article/us-crypto-iran/, Jun 2019. Accessed : 2020-01-17.

[2] Bitcoin price. https://www.financemagnates.com/cryptocurrency/news/is-monero-still-a-privacy-coin-ciphertrace-files-2nd-xmr-tracing-patent/, Nov 2020. Accessed : 2021-01-05.

[3] Bitcoin price. https://www.coindesk.com/price/bitcoin, Dec 2020. Accessed : 2020-12-28.

[4] M. Ahmed, I. Shumailov, and R. Anderson. Tendrils of crime: Visualizing the diffusion of stolen bitcoins. In *International Workshop on Graphical Models for Security*, pages 1–12. Springer, 2018.

[5] R. Anderson. Making Bitcoin Legal (transcript of discussion). In *Cambridge International Workshop on Security Protocols*, pages 254–265. Springer, 2018.

[6] R. Anderson, I. Shumailov, M. Ahmed, and A. Rietmann. Bitcoin redux. 2019.

[7] T. August, D. Dao, and M. F. Niculescu. Economics of ransomware attacks. *Available at SSRN*, 2019.

[8] G. Barber. China says Bitcoin is wasteful. now it wants to ban mining. https://www.wired.com/story/china-says-bitcoin-wasteful-wants-ban-mining/, September 2019. Accessed: 2020-01-17.

[9] J. Bhagwati and B. Hansen. A theoretical analysis of smuggling. *The Quarterly Journal of Economics*, pages 172–187, 1973.

[10] H. L. Bijmans, T. M. Booij, and C. Doerr. Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pages 1627–1644, 2019.

[11] J. Bukovina and M. Marticek. Sentiment and Bitcoin volatility (no. 2016-58). *Mendel University in Brno, Faculty of Business and Economics*, 2016.

[12] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring pay-per-install: the commoditization of malware distribution. In *Usenix security symposium*, pages 13–13, 2011.

[13] N. Christin. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*, pages 213–224, 2013.

[14] R. Clayton and B. Laurie. Proof of work proves not to work. In *3rd Annual Workshop on Economics and Information Security*, pages 1–9, 2004.

[15] B. Collier, R. Clayton, A. Hutchings, and D. R. Thomas. Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. In *3rd Annual Workshop on Economics and Information Security*.

[16] M. Conti, A. Gangwal, and S. Ruj. On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security*, 2018.

[17] F. S. O. Council. Financial stability oversight council annual report. Department of Treasury, 2018.

[18] F. S. O. Council. Financial stability oversight council 2020 Annual Report. Department of Treasury, 2020.

[19] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In *Annual International Cryptology Conference*, pages 139–147. Springer, 1992.

[20] A. H. Dyhrberg. Bitcoin, gold and the dollar–a garch volatility analysis. *Finance Research Letters*, 16:85–92, 2016.

[21] S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark. A first look at browser-based cryptojacking. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 58–66. IEEE, 2018.

[22] V. Garg, N. Husted, and J. Camp. The smuggling theory approach to organized digital crime. In *2011 eCrime Researchers Summit*, pages 1–7. IEEE, 2011.

[23] D. Goldsmith, K. Grauer, and Y. Shmalo. Analyzing hack subnetworks in the bitcoin transaction graph. *Applied Network Science*, 5:1–20, 2020.

[24] J. R. Hendrickson and W. J. Luther. Banning bitcoin. *Journal of Economic Behavior & Organization*, 141:188–195, 2017.

[25] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Botcoin: Monetizing Stolen Cycles. In *NDSS*. Citeseer, 2014.

[26] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM conference on Computer and communications security*, pages 3–14, 2008.

[27] P. Koshy, D. Koshy, and P. McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *International Conference on Financial Cryptography and Data Security*, pages 469–485. Springer, 2014.

[28] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013, page 11, 2013.

[29] N. Kshetri and J. Voas. Do cryptocurrencies fuel ransomware? *IT professional*, 19(5):11–15, 2017.

[30] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of monero's blockchain. In *European Symposium on Research in Computer Security*, pages 153–173. Springer, 2017.

[31] E. Le Jamtel. Swimming in the monero pools. In *2018 11th international conference on IT security incident management & IT forensics (IMF)*, pages 110–114. IEEE, 2018.

[32] M. Meltzer and S. Adair. Drupalgeddon 2: Profiting from Mass Exploitation. https://www.volexity.com/blog/2018/04/16/drupalgeddon-2-profiting-from-mass-exploitation/, April 2018. Accessed: 2020-01-17.

[33] M. Möser, R. Böhme, and D. Breuker. An inquiry into money laundering tools in the Bitcoin ecosystem. In *2013 APWG eCrime Researchers Summit*, pages 1–14. Ieee, 2013.

[34] M. Möser, R. Böhme, and D. Breuker. Towards risk scoring of Bitcoin transactions. In *International Conference on Financial Cryptography and Data Security*, pages 16–32. Springer, 2014.

[35] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, et al. An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163, 2018.

[36] T. Mursch. Large cryptojacking campaign targeting vulnerable Drupal websites. https://badpackets.net/large-cryptojacking-campaign-targeting-vulnerable-drupal-websites/. Accessed: 2019-09-15.

[37] M. Musch, C. Wressnegger, M. Johns, and K. Rieck. Web-based Cryptojacking in the wild. *arXiv*, 2018.

[38] D. I. Okorie. A network analysis of electricity demand and the cryptocurrency markets. *International Journal of Finance & Economics*, 2020.

[39] S. Pastrana and G. Suarez-Tangil. A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth. In *Proceedings of the Internet Measurement Conference*, pages 73–86, 2019.

[40] D. Plohmann and E. Gerhards-Padilla. Case study of the miner botnet. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, pages 1–16. IEEE, 2012.

[41] C. Putman, L. J. Nieuwenhuis, et al. Business model of a botnet. In *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, pages 441–445. IEEE, 2018.

[42] D. Ron and A. Shamir. Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security*, pages 6–24. Springer, 2013.

[43] M. Saad, A. Khormali, and A. Mohaisen. End-to-end analysis of in-browser cryptojacking. *arXiv preprint arXiv:1809.02152*, 2018.

[44] R. van Wegberg, J.-J. Oerlemans, and O. van Deventer. Bitcoin money laundering: mixed results? an explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2):419–435, 2018.