Effective Cryptocurrency Regulation Through Blacklisting

Malte Möser and Arvind Narayanan
Princeton University
{mmoeser,arvindn}@cs.princeton.edu

Abstract

Anti-money laundering regulation aims to prevent illicit proceeds from being reintroduced into the legal economy. Existing regulation targets financial intermediaries with record keeping and reporting requirements, enabled by the verification of customers' identities (KYC). These strategies fall short in cryptocurrencies, where transactions can be conducted without the involvement of regulated intermediaries.

Transaction blacklisting is a complementary regulation approach, incentivizing users and requiring intermediaries to check coins against public blacklists of illicit funds before accepting them. Blacklisting works on top of many existing cryptocurrencies today, improves anti-money laundering outside of regulated intermediaries and protects innocent users from inadvertently accepting illicit funds. In this paper, we discuss the intricacies of blacklisting, how it would change the Bitcoin ecosystem and how it can remain effective in the presence of privacy-preserving cryptocurrencies. We hope this paper provides a starting point for discussions among researchers, regulators and the cryptocurrency ecosystem around blacklisting.[1]

1 Introduction

Bitcoin, currently the most valuable cryptocurrency, is an open financial transaction system that allows anyone to participate pseudonymously, facilitates global payments with small per-transaction cost, and doesn't rely on a central entity [47]. This unique value proposition, however, comes at a price. Cryptocurrency exchanges, where users can trade fiat currency for bitcoins, get hacked on a regular basis [40]. Dark web marketplaces [12, 61] and ransomware [27, 50] (software that encrypts users' computers and demands a ransom for decryption) almost exclusively use cryptocurrencies for payment. It should come as no surprise that a decentralized, unregulated and pseudonymous financial transaction system attracts illegal activity.

Though the Bitcoin system itself evades regulation through its decentralization, the ecosystem around it is seeing more and more interest from regulators. These have begun enforcing existing financial regulation for intermediaries, such as anti-money laundering (AML) regulation for exchanges or securities laws for companies conducting token sales. As a result, companies or individuals violating securities laws may pay fines in USD and be imprisoned [28]. Activity solely within the cryptocurrencies, however, remains largely unaffected. Perhaps the most direct influence on the Bitcoin system itself had recent action by the Office of Foreign Asset Control (OFAC), a US regulator responsible for enforcing trade and economic sanctions against foreign countries. OFAC added Bitcoin addresses used by two Iranian nationals in a ransomware scheme to their "Specially Designated Nationals And Blocked Persons List" (SDN) [62], effectively forbidding any Bitcoin user in the US to interact with these addresses.

Blacklisting Bitcoin addresses is, however, not effective [44]. In contrast to the banking system, where a single account is tied to a person's identity, Bitcoin addresses can be created anonymously, in unlimited quantities, and without central oversight. This renders address-based blacklists largely ineffective: criminals can create fresh addresses to receive funds (which cannot be easily linked to existing addresses), and a static blacklisting of addresses (as done by OFAC) can easily be evaded by transferring funds to and through newly-generated addresses.

Instead of blacklisting addresses, an effective blacklist needs to contain individual transaction outputs (think coins)—e.g., all outputs sent to the Iranian addresses—and recursively enforce such blacklisting [44]. As transfers in Bitcoin reference the origin of the funds they are spending, it is possible to follow money derived from illicit activity from one transaction to the next. By requiring intermediaries in the Bitcoin ecosystem to check the origin of coins against the blacklist before accepting them, money laundering and other criminal activity can be addressed more effectively.

[1] We invite feedback on these ideas and may revise this paper in response. Last update: October 3, 2019.

Transaction blacklisting in Bitcoin has been discussed both from a technical [1, 2, 3, 9, 22, 44] and legal [2, 9, 22, 26, 56] perspective, and was recommended as an effective regulation approach for virtual currencies in [9]. However, it hasn't seen much traction in policy discussions about regulating cryptocurrencies yet. Regulators so far have followed an optimistic approach of waiting for the ecosystem to mature, and abstained from regulation that could potentially hinder innovation. Cryptocurrency advocacy groups have also advocated for such a path, often highlighting how Bitcoin's transparency already enables post hoc law enforcement investigations [48].

However, supplementing existing regulation with a blacklist-based approach could increase the effectiveness of anti-money laundering in cryptocurrencies today, and will become even more important once cryptocurrencies get more widely used outside (i.e. without the involvement) of regulated intermediaries. Blacklisting could at some point also start to occur organically through regulators' actions or court decisions (e.g., [26]), but in order to make it effective a holistic regulatory approach is necessary. In this paper we provide a comprehensive overview of how blacklisting would change the cryptocurrency ecosystem in order to facilitate more discussion around these issues.

In the remainder of this paper, we first show how blacklisting fills current gaps in AML regulation of cryptocurrencies and protects users from receiving funds derived from illicit activity (Section 2). Next, we discuss the practical aspects of setting up and using transaction blacklisting in a cryptocurrency like Bitcoin (Section 3). Once blacklisting is in place, users face an elevated risk of accepting funds that might get blacklisted in the future, for which we discuss mitigation strategies (Section 4). Then, we discuss the importance of choosing a blacklisting policy and review five policies that have been proposed in the literature (Section 5). Acknowledging that blacklisting may not be feasible in all cryptocurrencies, we describe how blacklisting could still be effective in the presence of more privacy-preserving cryptocurrencies (Section 6). Finally, we address some common concerns around blacklisting (Section 7) and conclude with a brief outlook (Section 8).

2 Combating Money Laundering in Bitcoin through Blacklisting

"Criminals are early-adopters of new technology" — this colloquial statement about the tug of war between criminals and law enforcement readily applies to cryptocurrencies like Bitcoin. Since their inception more than ten years ago, cryptocurrencies have been associated with money laundering [17, 43, 59, 62], the sale of narcotics and illegal goods [12, 61], extortion and ransomware [27, 50, 51, 62], investment fraud and scams [23, 65, 66] or human trafficking [55]. Fighting the criminal use of cryptocurrencies meanwhile faces unique challenges. Traditional ways of combating money laundering are ineffective due to cryptocurrencies' decentralized nature: enforcing the Know-your-customer principle and other cornerstones of traditional AML regulation is fruitless in a system where anyone can create accounts in a matter of seconds, without any regulated parties being involved. Due to the lack of a comprehensive regulation approach, regulated entities such as cryptocurrency exchanges have started using proprietary blockchain analysis services to screen incoming funds. As a result, Bitcoin users are at risk of accepting bitcoins that they cannot spend at exchanges.

In the remainder of this section, we first review the current state of AML regulation as it applies to regulated Bitcoin intermediaries such as exchanges. Then, we discuss the shortcomings of this approach, specifically how the focus on accounts and regulated intermediaries misses money laundering happening outside of exchanges and how it puts users at risk of receiving money they cannot spend. Finally, we sketch a more effective solution: how making information about money laundering public would make combating money laundering more effective and better protects users.

2.1 Background: AML Regulation in the US

Anti-money laundering (AML) regulation aims to prevent and disincentivize the (re-)introduction of money derived from illegal activity into the legal economy. In the United States, money laundering is prohibited through multiple, complementary laws, the most important ones being the Bank Secrecy Act (BSA) of 1970, the Money Laundering Control Act of 1986, as well as Title III of the USA PATRIOT Act of 2001 (also known as Title III: International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001).

The Bank Secrecy Act of 1970 (BSA) requires financial institutions to fulfill record keeping obligations and to report large or suspicious transfers. The original intention of the BSA was to make the placement of cash proceeds of drug sales harder by creating a paper trail that investigators could follow [38]. The BSA however did not make money laundering itself illegal: money laundering was considered to only be a by-product of the actual crime from which the proceeds were derived, which would be prosecuted. The BSA also did not make (attempted) evasion of the reporting requirements illegal. Criminals were able to structure transactions in a way that would avoid reporting requirements, e.g., by making cash deposits slightly below the reporting threshold.

The Money Laundering Control Act of 1986 made money laundering a federal crime and applies to any US person (not just financial institutions). It also fixes loopholes of the BSA by explicitly making evasion of reporting requirements a crime. 18 U.S. Code § 1956 prohibits the transfer of funds derived from "specified unlawful activity" with the intent of promoting specified unlawful activity. In addition, 18 U.S. Code § 1957 prohibits monetary transactions above $10,000 derived from specified unlawful activity and conducted by,

through or to a financial intermediary, without requiring intent of promoting unlawful activity [10]. Both sections feature a knowledge requirement: a person must know that the money is derived from unlawful activity in order to be guilty of money laundering – just a suspicion that the money might be derived from unlawful activity is not sufficient.

The International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 (Title III of the USA PATRIOT Act) further strengthened these money laundering regulations. It requires companies to have an AML compliance program, including at a minimum the development of internal AML policies, procedures and controls, the designation of a compliance officer, employee training as well as independent audits of the program (31 U.S. Code § 5318 (h)). The act also classified Money Services Businesses (MSB), i.e. businesses that transmit or convert money, as financial institutions, making it easier to apply existing financial regulations to them (Section 359). The Patriot Act furthermore widened the scope of anti-money laundering regulation by including the support of foreign terrorist organizations as a money laundering offense.

2.2 Existing AML Regulation's Focus on Accounts is Ineffective in Cryptocurrencies

Banks constitute centralized entry points to the traditional financial sector, making them a convenient target to enforce AML regulation. Cryptocurrencies like Bitcoin however operate fundamentally different from traditional financial systems. Often described as open and "permissionless", cryptocurrencies allow account creation independent of any financial institution and without the ability to enforce identity verification requirements. Instead of maintaining accounts as entries in a centralized database (allowing to enforce KYC), cryptocurrency "accounts" are represented by cryptographic keys. The public key of such a pair is used as the account identifier (referred to as "address"), and digital signatures created with the private key authorize payments. As anyone can create new key pairs and use them to receive coins, the system works completely without a central authority. Because creating keys is fast and cheap, many cryptocurrencies (such as Bitcoin) encourage one-time use of addresses. For every time a user receives money they can create a new key pair, increasing their privacy as their transactions are split among many different accounts. Without any special knowledge, addresses belonging to the same user that are not used simultaneously cannot easily be identified.

Without any oversight over account creation, cryptocurrencies lack a leverage point to enforce KYC or other record-keeping requirements. Identities can only be acquired and verified when users cross the boundary to the traditional financial system by interacting with regulated intermediaries, such as exchanges or payment providers. But even if identities can be acquired at these intersections, regulators won't gain a complete picture of an individual's transactions as these could be facilitated using many different addresses, only a small subset of which become known to the intermediary. As a result, much activity in the system is not attributable.

Right now, many cryptocurrency transactions are likely driven by speculation [54]. But in the future, cryptocurrencies could enable large volumes of decentralized commerce that takes place between individuals only, facilitated by the decentralized network, and without the involvement of a regulated intermediary. Cryptocurrencies also do not distinguish between national and international payments. As anyone can join the network, some share of payments will cross national boundaries. National regulation efforts that depend on sensitive private information about users' identities and their spending habits are ineffective in such an environment.

2.3 The Effectiveness of Regulating Exchanges is Limited and Users are at Risk of Accepting Money they Cannot Spend

Cryptocurrency exchanges currently constitute the major interface between the traditional financial sector and the Bitcoin ecosystem. Exchanges allow users to deposit bitcoins or fiat currency and convert them from one to the other. They are usually custodial, as they hold users' funds in their own wallets (in the case of cryptocurrency) or bank accounts (for fiat currency). In the United States, custodial exchanges are considered to be MSBs and therefore must comply with previously discussed AML regulations [18].

To fulfill the abstract requirements of these regulations, including the development of an effective AML compliance program that has "reasonable" measures to prevent money laundering, many exchanges have adopted the use of blockchain intelligence services to screen customers' transactions.

Blockchain intelligence companies, such as Chainalysis or Elliptic, offer services to exchanges that are designed to detect transactions that originate from illicit sources, such as dark web markets or illegal gambling sites. Exchanges use these services to screen customers' incoming funds before depositing them into the respective accounts. If these tools detect suspicious transactions, accounts may be frozen and customers asked for additional information about the origin or purpose of funds, or customers might be prevented from further using the service altogether.

As (to the best of our knowledge) no detailed technical information about how these services work exactly is publicly available, the following description is based on informal blog posts (e.g., [29, 60]) and discussions. To detect suspicious transactions, these companies are building large databases mapping Bitcoin addresses to known identities. Their ground truth comes from interaction with various platforms and marketplaces in the Bitcoin ecosystem (e.g., by depositing money into the wallet of a dark web market), from the use of their products by exchanges, as well as from law enforcement and

other sources. The identified entities may then be grouped into risk classes. To derive a risk score for a specific transaction, it is checked for originating from or being destined for a known entity.

These current practices raise three concerns. First, the existence and use of such databases is a potential privacy concern for Bitcoin users. While exchanges do not send customers' identities to the third-party services [29, 60], the collected data may still allow to re-identify users when combined with address clustering [37] and external datasets or specific knowledge of an individual's activity.

The second, more general issue that we discussed before, is that this type of transaction screening at exchanges is not sufficient to combat money laundering in Bitcoin. While currently most exchanges rely on these services to identify money derived from illicit activity in order to comply with rather unspecific AML regulation, it does not prevent money laundering that occurs outside of regulated exchanges. And intermediaries in countries with less strict AML regulation have little incentive to implement such measures in the first place.

Third, individual users who make payments outside of exchange platforms generally don't have access to those services to perform their own due diligence before accepting coins. As a result, whenever they accept coins from anyone but exchanges (i.e. the original use case of Bitcoin) they are at risk of receiving illicit funds that, unknowingly to them, they won't be able to spend.

2.4 Public Blacklists of Funds Derived from Illicit Activity Make AML More Effective and Protect Innocent Users

We identified three key areas in which the current regulatory landscape can be improved: reducing the dependence on knowledge of account ownership, improving the effectiveness of AML outside of regulated intermediaries, as well as providing more transparency to protect innocent users. A regulatory approach based on the idea of public blacklists for illicit coins [9, 22, 44] would address all three of these issues.

Blacklists are a well-known tool in a regulators toolbox to prevent interaction of regulated parties with certain outside entities. For example, OFAC's SDN lists the identities of foreign nationals that US entities are forbidden from interacting with, in order to prevent those listed from participating in the global economy. In the context of Bitcoin, a blacklist would contain specific coins that are known to be derived from illicit activity. By tracing these coins from one transaction to the next, they can be separated from the legal economy [9, 44].

Blacklisting coins works on the basis of transactions and is recursively applied when an illicit coin is spent in a new transaction. The advantage of a transaction-based approach is that it is not necessary to know any identities behind addresses. Anyone can check whether coins of a particular transaction are illicit by checking the blacklist. Whenever illicit coins are spent, coins in the new transaction inherit the illicit status, ensuring that it is impossible to launder coins by moving them through a chain of transactions to an unknown address.

Public blacklists are also effective at fighting money laundering outside of regulated intermediaries. Since anyone can check the coins they are about to receive, those holding illicit coins won't be able to spend it. While only regulated intermediaries would be legally required to reject or confiscate illicit coins, *every user* has an incentive to check the blacklist, since they wouldn't be able to spend listed coins themselves. At the same time, since it is now public knowledge which coins are derived from illicit activity, the ability to check coins before accepting them reduces the danger of receiving coins that the user cannot spend at an exchange.

Public blacklists enable public scrutiny: while there's currently a lack of transparency about exchanges decisions' to accept coins, any incorrect or malevolent blacklisting of coins (e.g., for political censorship) would be detectable, and could then be openly questioned (or challenged in court). Having a standardized process to list funds will furthermore improve regulators', law enforcements' and courts' effectiveness at combating crime in cryptocurrencies. And if blacklists effectively deter crime, they can even reduce current reliance on the privacy-invasive practice of blockchain intelligence companies mapping out the Bitcoin ecosystem.

Of course, implementing public blacklists for cryptocurrencies is not a panacea. It requires additional infrastructure and makes sending and receiving cryptocurrency more involved as users will want to check the blacklist before accepting coins. And to make blacklists effective for a global payment system, some degree of international coordination is necessary to prevent criminals from routing their funds through countries that don't enforce the same blacklists. Regulators and law enforcement might be reserved towards a regulatory solution that requires them to make information about illicit activity public. And the cryptocurrency community itself might object such an approach, since it introduces centralized control that cryptocurrencies were envisioned to evade in the first place. In the rest of this paper, we describe how such a system can work in practice and address these issues in more detail.

3 How Blacklisting Would Work

Enforcing transaction blacklisting changes the way payments are conducted in a cryptocurrency. In this section we recall how recursive transaction blacklisting works, discuss the role regulators would need to take on and how blacklisting affects exchanges, merchants and normal users. We provide a summary of the anticipated changes in Table 1.

3.1 Recursive Blacklisting

The goal of AML regulation is to prevent money that was acquired through illegal activity from entering the legal econ-

Table 1: How blacklisting would change the Bitcoin ecosystem

Stakeholder	Aspect	Change	Description	Section
Ecosystem	Decentralization	Decrease	Centralized entities may be better able to offer more convenient solutions for users to handle blacklisting compared to decentralized alternatives	3, 4
	Privacy	Mixed	Centralization could reduce privacy, less reliance on privacy-invasive blockchain intelligence services can increase privacy, payment networks and privacy overlays can increase privacy	6
All users	Taint check	Major change	Users are incentivized to check coins against blacklists before accepting payments	3.1, 3.6
	Risk of future blacklisting	Major change	Requires use of mitigation strategies	4
MSBs	Existing AML requirements (KYC, reporting, etc.)	No change	Potentially reduced reliance on privacy-invasive identity-based measures if blacklists are effective	2.1
	Taint check	Major change	Required to check incoming funds against blacklists and freeze/reject tainted funds	3.5
	Risk of future blacklisting	Objective change	Risk assessment to protect against future blacklisting of high-risk transactions	4
	Additional services	New	Exchanges can provide insurance against future blacklisting	4.4
Wallets	Taint check	Voluntarily	Integration of automated blacklist checks	3.6
	Risk of future blacklisting	Voluntarily	Integration of mitigation strategies	4
	Coin selection	Minor change	Depends on taint policy and objectives	3.6
Payment Channel Networks	Channel establishment	Minor change	Taint check + risk assessment as for normal payments, preference for trusted counterparties	4.3
	Risk of future blacklisting	Minor change	Only immediate channel hop poses risk	4.3
Decentralized protocols	Taint check, risk of future blacklisting	Voluntarily	May incorporate signaling or coin negotiation into protocol	6.2
Regulators / Law Enforcement	Blacklists	Major change	Issue cryptocurrency-specific blacklists, define taint propagation policies and specify actions cryptocurrency intermediaries and users need to implement, define standardized API for clients to query blacklists	3.3
	International cooperation	Major change	International cooperation and coordination required (e.g., through FATF or Interpol)	3.3
	Reporting crimes	Major change	Users can submit evidence of crimes to law enforcement to blacklist coins	3.4
	Contesting listings	Major change	Legal process to object unreasonable or incorrect blacklisting of coins required	3.4
Courts	Forfeiture	Minor change	Able to blacklist known funds that cannot be seized by LE	[26]

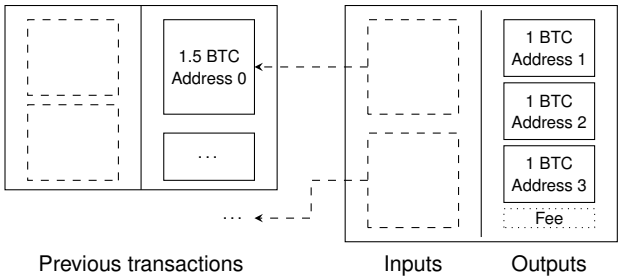


Figure 1: The structure of the Bitcoin transaction graph allows to follow coins from one transaction to the next

omy. A blacklist-based approach can achieve such separation, requiring users to check coins before accepting them and refusing those with illicit origin. In the context of Bitcoin, a blacklist would include specific outputs of transactions that are associated with illegal activity, such as theft, extortion, money laundering or trade of illegal goods [9]. When those outputs are spent, their illicit status (commonly referred to as taint) is inherited by the transaction spending it. That means that even when coins that originate from an address known to be involved in illicit activity are moved through other addresses multiple times, they retain their taint and can be identified as illicit. By recursively assigning taint to all following transactions it is made impossible to launder illicit coins.

Figure 1 shows the structure of a typical Bitcoin transaction. Transactions contain outputs that associate an amount of bitcoins with an address[2] and spend value from previous outputs that are referenced by inputs. By mapping taint from the inputs to the outputs (discussed in Section 5), taint of a former transaction is retained and applied to new outputs [44].

Blacklisting outputs effectively freezes the value contained within the output when regulated entities are forbidden to accept these coins. When coins are transferred to a different address, the link between inputs and outputs allows to follow the coins and recursively apply the blacklisting to the new transactions. Intermediaries would not be allowed to accept coins that stem from these blacklisted outputs, or would need to ignore or seize the part of the funds that are tainted.

A Note On Terminology Fox [19] discusses the difference between the terms "following" and "tracing" in the English law literature. Following implies that the same asset is being followed, whereas tracing means identifying a new substitute for the original asset. In many cryptocurrencies (e.g., Bitcoin), every transaction effectively destroys the value present in its inputs and recreates the value in its outputs. Since there is no inherent mapping from value in inputs to value in outputs, it cannot be followed, only traced.

In the context of cryptocurrencies, however, the term "tracing" has also been used to describe the deanonymization of patterns or techniques designed and employed to obfuscate payment flows. Privacy-focused cryptocurrencies like Monero use the term "untraceable" to describe a specific form of unlinkability: between the input in a transaction and the output that is being spent by this input [46]. In a way, there can be two types of tracing: identifying the output (of a previous transaction) that is spent by an input (taking a backwards look), and identifying which output (in the same transaction) receives value from an input (taking a forward look).

To make the distinction between these two types of tracing clear, we will use the following terminology in this paper. First, we are primarily interested in the flow of illicit value. We call such value "tainted". A "taint policy" defines how taint is "traced" from inputs to outputs (within one transaction), but we use the term "mapping" instead. When such mappings are applied recursively, we say that taint is "propagated" through the transaction graph.

Second, we use the terms "traceable" and "untraceable" as used in the cryptocurrency privacy literature, i.e. referring to the degree of anonymity provided by a cryptocurrency through means of providing unlinkability between outputs and the inputs in which those are spent.

3.2 Legal Grounds

The legal status of a cryptocurrency determines the degree to which recursive blacklisting can be applied. In many legal systems, the "nemo dat rule" holds that when something was stolen, the ownership stays with the original owner, no matter how often the item was resold and whether subsequent purchasers acquired the items in good faith [3]. This allows to recursively blacklist coins in a blacklisting regime.

A notable exception to this rule is legal tender, in order to allow for unrestricted economic exchange. To this date, no cryptocurrency has, however, been declared legal tender by a country. Furthermore, blacklists enable users to efficiently check whether coins have been marked as stolen, thereby reducing the danger of disrupting the economy.

At the same time, blacklisting won't necessarily be able to provide remedies similar to those of traditional enforcement. While blacklisting provides a strong disincentive against money laundering by rendering the holdings of criminals worthless, when it does take place the pseudonymous and decentralized nature of Bitcoin prevents law enforcement from seizing these coins, or learning the identity of the responsible person.

In this paper we assume that the law permits the recursive blacklisting of coins. We refer the interested reader to more in-depth analysis of these issues by Fox [19] for English law, and to the analysis of German law by Grzywotz [22].

[2] More precisely, they associate value with spending conditions specified in a simple scripting language. Most commonly, they require a signature corresponding to a public key, demonstrating ownership of the private key. A specific hash of the public key or the script that specifies the spending conditions represents the "address".

3.3 Blacklist Governance

In practice, a blacklist would be published by a regulatory agency that is tasked with the prevention of financial crime. The regulator would be responsible for adding entries to the blacklist as well as defining the terms of how it is to be followed. For example, they'd specify how taint propagates from one transaction to the next (cf. Section 5) and how regulated intermediaries should act when receiving tainted coins.

While the abstraction of a single blacklist is useful to reason about blacklisting (e.g. [2, 44]), in practice it is likely that there will be multiple blacklists issued by different regulators. In the US, financial regulation is split between a variety of different agencies. State regulators, such as the New York Department of Financial Services, exist alongside federal regulators such as FinCEN. Different regulatory and law enforcement agencies have oversight over different areas or jurisdictions and it is thus conceivable that they would issue their own blacklist, with potentially different rules regarding how blacklisted coins should be handled by users. For example, FinCEN might maintain a list for bitcoins stemming from illegal activity while OFAC maintains their own list relating to economic sanctions, and the DEA could provide another list relating to the illegal sale of drugs and narcotics.

Similarly, other countries would maintain their own blacklists, and entities that conduct business in different countries would need to adhere to those blacklists, too. To make blacklisting effective and prevent criminals from being able to cash out money that was stolen in the US on a European exchange, there should be international coordination between the different countries. As with traditional financial regulation, or criminal enforcement more general, blacklisting inherits the challenges typical in international cooperation. Countries need to synchronize their blacklisting efforts, such that cross-national transactions (one important use case of cryptocurrencies) are not inhibited by a highly fragmented landscape of blacklists and policies.[3] Information sharing could be carried out by existing structures for international cooperation, such as the Egmont Group of Financial Intelligence Units, the Financial Action Task Force on Money Laundering (FATF) or the International Criminal Police Organization (Interpol). In order to limit the complexity for end-users, these blacklists would require a standardized API and machine-readable rules such that client software can automatically parse and adhere to the different requirements.

3.4 Adding an Entry to the Blacklist

Entries would be added to the blacklist as a result of a criminal investigation, for example when investigators were able to locate a criminals bitcoins but are not able to seize it (cf. [26]), or could be added as a direct reaction to a crime, such as the payment of a ransom. We note that regulators and law enforcement may in specific instances choose not to list assets if they are part of an ongoing investigation, e.g., if they hope to identify a specific criminal when they attempt to cash out their proceeds on a specific exchange. In such a scenario, listing the assets could compromise the integrity or confidentiality of the investigation.

A user whose coins have been stolen, or who was blackmailed and paid a ransom, would need to submit supporting evidence to the operator of the blacklist (e.g., through a law enforcement entity such as the FBI's Internet Crime Complaint Center). To prove ownership of the coins at the time of the incident, the user would create a digital signature with the keys that held the coins. In case of a theft on an exchange (e.g., due to phishing) where the user does not hold the keys themselves, the exchange operator could create such a proof for the user. In addition, the user would submit supporting evidence that their coins were indeed stolen or extorted and a statement of good faith under penalty of perjury. Making incorrect claims would hence be a crime that can be challenged through traditional enforcement channels.

Due to the decentralized nature of Bitcoin and a lack of a central registry, regulators are unable to inform the holder of coins of a listing of their funds. Instead, users have to regularly check their coins against the blacklists (which could be done automatically by their wallet software).

As the listing of funds effectively corresponds to a freezing of assets, there must be a legal process in place to contest unreasonable listings as well as a way for incorrectly affected persons[4] to complain and take legal action against it [22]. Such a process could be modeled based on existing processes, such as OFAC's license application to release blocked funds [49]. Affected users would submit an application to the regulator to remove the listing of coins from the blacklist, along with details about the transaction as supporting evidence that the coins were acquired legally (e.g., bought from a reputable exchange). Depending on the type of crime, some of these steps could be automated.

3.5 Regulated Intermediaries

A blacklisting of coins is only effective if users and businesses take it into account when accepting coins. However, since Bitcoin is an open system, compelling users, developers or miners to enforce a blacklist is hard due to their geographic dispersion and limited legal options to do so. Intermediaries in the Bitcoin ecosystem, such as exchanges or payment providers, however, do have a clear jurisdiction in which they already follow existing financial regulation. They are responsible for a significant amount of the transaction volume on the Bitcoin blockchain (cf. [32]) and provide the

[3] If different jurisdictions select different taint policies, outputs would have different legal status across countries.

[4] Note that objecting to a listing would only be feasible for the immediate holder of the illicit coins.

onboarding process for most users acquiring bitcoins. Requiring these intermediaries to follow a transaction blacklist could be achieved by amending existing anti-money laundering regulations. If exchanges and payment providers follow the rules in a blacklisting regime, any user who at some point in the future wants to interact with them, either to convert fiat currency into cryptocurrency or vice versa, or to buy goods from a merchant with bitcoins, is thus incentivized to also adhere to the blacklist. Otherwise, they might accept coins that are worthless when being traded in at an exchange.

Depending on the legal implications of blacklisting, regulated intermediaries would either accept blacklisted coins, freeze them and report such an incident to the responsible authorities, or be forbidden from accepting them in the first place. If the coins get tainted while in control of the exchange, exchanges can potentially sanction the user who deposited the coins, nominally reduce their holdings on the exchange as well as report the user to law enforcement (depending on how far away the blacklisted coins were in the transaction graph). In such an investigation, users might be forced to reveal from whom they received their bitcoins in the first place.

Intermediaries might offer customers a quality guarantee for coins, i.e. if coins a customer receives are retroactively blacklisted the exchange will compensate the user for the difference in quality or exchange the coins for clean ones [44]. They could achieve such higher quality either by holding coins long enough (i.e. they use more of their reserves to facilitate payments), or by adding a risk premium to deposits.

Not all intermediaries in the Bitcoin ecosystem are centralized or operate within a identifiable jurisdiction. There's a trend to decentralize services such as exchanges [8] or privacy services [42]. While in most cases such decentralized intermediaries may not be targetable by regulation, users still have an incentive to adhere to blacklisting if they want to spend their coin at a regulated intermediary in the future (or want to transfer it to a user who does) [1].

3.6 Making and Accepting Payments

Whenever a user receives funds, they need to verify that the coins they are about to receive are not (significantly) tainted. In order to do so, they need to know which coins they'll receive. Here, we sketch three different options.

Returning Coins A simple solution would be for a payee to return funds to the payer when the coins received are tainted. However, the address from which the coins were originally sent might not allow the payer to receive them back. For example, when sending money from an exchange, the coins might come from an address under the control of the exchange that is not directly linked to the user's account. Another disadvantage is that a refund transaction incurs additional transaction fees and adds "unnecessary" transactions to the blockchain. Finally, it is undesirable that the payer has to hand over control of their bitcoins to the payee in order for the payee to check and accept or reject the payment.

Multisig Accounts To address the last issue, the payer could lock funds in a 2-of-2 multisig transaction that contains a time-locked refund. To spend these funds, both the payer and the payee need to sign a spending transaction. If the payee signs such a transaction, it would indicate their willingness to accept the coins. Going further, the payer could lock more funds than nominally requested by the payee and have the payee create a transaction with an amount that they deem equivalent to the risk of future blacklisting. The payer can then choose to agree or reject the transaction by signing or refusing to sign it. If at any point the payee becomes unresponsive, the payer can reclaim their coins after a short period of time. While this solution provides more flexibility and the coins stay under the payers control until the payment is finalized, it always requires two on-chain transactions.

Extending the Bitcoin Payment Protocol The Bitcoin Payment Protocol is a standardized protocol that allows a merchant (or payee) to specify details of a Bitcoin payment, such as the destination address and the amount, and make these programmatically available to the user's wallet [4]. The user's wallet receives a link to the payment request (e.g., by opening a URL or scanning a QR-code) and retrieves the payment details from the merchant's website. This protocol could be extended to include specific details for the handling of blacklisted coins and the risk of future blacklisting. For example, it could specify whether tainted coins are accepted by the merchant and how these would be discounted. It could also specify a set of blacklists (e.g., as API endpoints) that the customer must check their coins against.

Most of the evaluation could happen on the payer's side, preserving privacy as the merchant will only see the final set of coins chosen. If the user chooses coins in a way that violate the rules set by the merchant, the merchant can reject and refund the payment or, if legally required to do so, freeze the funds they received.

Wallet Support Both the multisig solution as well as the extension of the Bitcoin payment protocol require end-users' wallets to support these specific protocols. Wallets furthermore need to modify their coin selection algorithms to take the taint of coins into account. Currently, coin selection is often optimized to reduce transaction fees or increase users' privacy (cf. [16]). In a blacklisting regime, wallets need to take the taint status as an additional constraint and furthermore optimize depending on the taint policy (cf. Section 5).

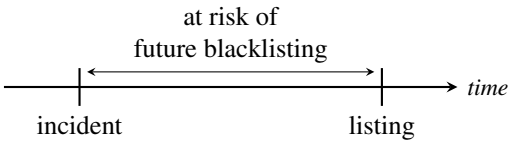


Figure 2: In a blacklisting regime users are at risk of receiving coins that might get blacklisted in the future

4 Managing the Risk of Future Blacklisting

While it is straightforward to check whether coins are tainted at the time a user accepts them, in a blacklisting regime users also need to account for the risk of receiving coins that might get blacklisted in the future [44]. After any illicit activity that warrants a listing of coins on the blacklist has taken place, there will be a time delay until those coins are actually listed on the blacklist (cf. Figure 2). During this time, a user might accept such unlisted coins, only to later discover that those originate from illicit activity and have been listed, leaving them with coins they cannot spend. While this risk seems similar to the current risk of receiving coins that an exchange may not accept, the reduced time frame and the availability of public blacklists enable a number of mitigation strategies.

4.1 Time-Delayed Payments

The time since a coin was created is a useful indicator of its risk in the context of future blacklisting. Assuming that criminal activity is associated with some transfer of funds (e.g., payment of a ransom, theft of coins, illegal payment to a terrorist group), then blacklisting of the particular coin should happened after the transaction has been put on the blockchain. The criminal hence wants to get rid of their illicit coins quickly, before they get listed. A coin that has been sitting in a users wallet for a long time has thus, when spent, a much lower risk of future blacklisting than a coin that has been moved recently. The longer a coin has been in a user's possession, the less likely it should be that it will get blacklisted in the future.

One way to systematically reduce the impact of future blacklisting would be to limit the time frame in which blacklisting can occur. If blacklisting would need to happen within, say, two weeks of an incident, then users could mitigate the risk of blacklisting by preferring coins that have been sitting unspent sufficiently long. (If the coins haven't moved since the crime occurred, they could still be listed after the blacklisting period expired since there is no collateral damage to the rest of the ecosystem). However, many blacklists (e.g., assets blacklisted by OFAC) might not permit such restrictions. Users who do not hold a variety of coins of different ages would also be at a disadvantage.

Using the coin age as a proxy for risk is inapplicable when a criminal is able to steal a user's private keys but does not immediately transfer the coins away. The coins would appear to be idle, but once they are spent they could become subject to blacklisting. Private key theft however appears to be less common than other forms of theft, such as funds stolen from an exchange [3]. Furthermore, this risk can be reduced by using storage options that are more secure than a regular software wallet. Larger amounts of bitcoins can be stored in more secure wallets (e.g., cold storage or hardware wallets), and software solutions such as Bitcoin vaults could help address the issue of private key theft [7, 45].

Even without having a limited time period in which blacklisting occurs, increasing the time delay between coin transfers is still an effective way to reduce the risk of future blacklisting. To this end, users can make use of two features of the Bitcoin protocol to enforce a time-delay until coins can be spent: time-locked transactions, and time-locked outputs. Time-locked transactions are invalid until a future point in time (as specified by the `nLockTime` field) and will be rejected by the network until the time-lock has expired. A user could give such a time-locked transaction to a merchant, who waits until the time-lock expires and then submits it to the Bitcoin network. If coins get blacklisted until the transaction becomes valid, the transaction can simply be disregarded. A slightly different mechanism to create an artificially delay is to make use of the `CheckLockTimeVerify` opcode that allows to specify a time before or after an output can be spent by different public keys. This opcode can be combined with the aforementioned techniques to check the coin status before making a payment, where the payee would effectively receive a specific time window in the future in which they can claim the funds. It has the advantage of producing an on-chain transaction, addressing the issue of stolen public keys mentioned above: the user whose keys were stolen would be alerted by the move of their coins on-chain (similar to [45]) and could blacklist the funds before they are accepted by the merchant.

We note that delaying payments is a common risk mitigation strategy in the financial sector today, and is used in the cryptocurrency space as well. Exchanges may delay the conversion or transfer of currency if additional compliance checks are necessary, and so they may adopt similar procedures when they deem funds to be at high risk of blacklisting. In scenarios where delays are undesirable, charging a risk premium or using insurance may be viable alternatives.

4.2 Risk Scoring

While the age of a coin is a potentially strong indicator for the risk of future blacklisting, it is not the only feature that can be used to assess this risk [44]. A risk score can potentially be constructed based on a variety of indicators, including structural features of the transaction graph or private information on the ownership of addresses or address clusters. Such a score is similar to traditional fraud detection for credit card payments or the risk assessment that banks are required to

perform prior to conducting large payments [22]. However, in order to construct a precise risk model, relevant data must first be made available [44].

As previously discussed, cryptocurrency exchanges are already using risk scores provided by blockchain intelligence companies to screen incoming payments. Chainalysis, for example, offers a "Know Your Transaction (KYT)" API that allows to "identify high risk transactions on a continuous basis" [11]. To compute these scores, blockchain intelligence companies make use of private information about the identities behind addresses, e.g., collected by interacting with various intermediaries in the ecosystem. Once suspicious wallets, such as those belonging to mixers or dark web markets, have been identified, these services can monitor other wallets interacting with these services and specify risk scores based on the type of activity.

Currently, these scores are primarily available to enterprise customers such as exchanges. However, they could easily be offered to a larger group of users in order to be useful to supplement risk scoring in a blacklisting regime.

4.3 Payment Networks

The Bitcoin protocol is inherently limited in the number of transactions that can be processed, as all transactions need to propagate throughout the network and be verified by miners and full-node operators [14]. Currently, multiple groups are working on solving this issue with payment networks, a network of payment channels between individual users that can facilitate chains of payments, similar to credit networks [53]. The future use of payment channels raises two important questions: can money laundering be facilitated through payment channels, and is blacklisting still effective if they become commonly used?

Off-chain payment networks allow to conduct a large number of transactions "off" the chain. Instead of committing every transaction to the blockchain, users can open payment channels [15, 53] to other users. Once a channel is open, they can conduct a potentially unlimited amount of transfers between each other, limited only by the amount of coins locked into the channel, by locally updating the state of the channel (i.e. increasing or decreasing the individual shares). Only when they no longer want to use the channel, the final balance (i.e. the settlement of all intermediary transactions) is committed to the blockchain.

Payment channels can be combined into payment networks that allow to route payments across multiple payment channels [35, 53], similar to transactions in credit networks (but without the risk of a party defaulting). This allows mutually distrusting parties to pay each other through payment channels without needing to open their own, direct channel.

Perhaps the most relevant question is whether blacklisting can be done within payment networks themselves, or whether criminals can evade blacklisting in Bitcoin by moving their operations into a payment network. For example, a ransomware operator could require users to send the ransom through the Lightning network rather than as a normal Bitcoin transaction. In general, payment networks are not very attractive for large-scale money laundering since the bandwidth available (i.e. the amount of funds that can be sent or received) is significantly lower than in a normal cryptocurrency. For a user to pay another user, there must be a path with sufficient bandwidth available to facilitate the pairwise payments. Normal users might not be willing to make too many funds available through these channels (every channel effectively locks up some capital that cannot be used otherwise). Larger players, who could provide higher bandwidth and are running their payment hub commercially, will likely need to register as money transmitters and thus be subject to AML regulation, enabling follow-up investigations that could reveal the criminal's coins on the Bitcoin blockchain.

Payment channels are not only unattractive for money laundering, they also remedy some of the drawbacks of blacklisting in Bitcoin for small payments. Channels are opened infrequently, hence parties only need to check the taint of the counterparty's funds when a channel is opened. Opening a channel however increases the impact of potential future blacklisting as channels are intended to be kept open for long periods of time. This gives payment networks characteristics similar to credit networks: while there's no direct risk of losing funds (the primary risk in a credit network is a defaulting counterparty), there remains the risk that at the time the channel is closed the funds in the channel have been listed. This incentivizes users to only engage in payment channels to highly trusted counterparties, such as friends or reputable and regulated intermediaries. Moving high-frequency transactions into off-chain networks also improves the effectiveness of on-chain transaction blacklisting, as coins are less likely to mix with each other and the overhead of checking blacklists and assessing the risk of future blacklisting is reduced.

4.4 Identity and Insurance

Blacklisting would introduce notions of trust into Bitcoin and increase the benefit of knowing the identities of counterparties. While many intermediaries in the Bitcoin ecosystem are already required by AML regulation to verify identities, normal users could be inclined to conduct similar identity checks prior to interacting with other users, e.g., to better assess the risk of future blacklisting or to be able to involve traditional enforcement in case of future blacklisting. This could decrease privacy for individual users or reduce the utility of Bitcoin as a whole when enough people stop using it. On the other hand, when large payments are conducted through Bitcoin they are often already governed by a contractual relationship that is aware of the counterparties' identities. For small payments, a small risk premium might be sufficient for intermediaries to protect themselves against future blacklisting.

Another potential remedy could be to make use of optional co-signing of transactions by well-known intermediaries. Co-signing is today mostly used for enhanced security, but some intermediaries are using it as a mechanism to prevent double-spending (by having the assurance of a trusted third party to not double-spend a co-signed transaction, exchanges can accept payments that haven't yet been confirmed by the network) [21]. In the context of blacklisting, co-signing could either indicate the ability for the regulated party to reveal the user's identity in the case of funds getting blacklisted, to signal that the intermediary determined the coins to be of low risk, or even to provide assurance that the third-party provides some form of insurance against such blacklisting. Insurance of this type could dramatically reduce the impact of long chains of transactions that become effectively invalidated due to retroactive blacklisting of funds in the first transaction.

5 Blacklisting Policies

To make blacklisting effective, taint must propagate through the transaction graph. A blacklisting policy specifies the exact mechanism with which taint is mapped from incoming coins (inputs) to outgoing coins (outputs).

Several blacklisting policies have been discussed in the literature. Möser et al. [44] propose two policies. In the *poison* policy, any tainted input completely taints all the outputs in a transaction. In the *haircut* policy, any taint associated with an input is distributed equally among all outputs such that the total amount of tainted value does not change. They also suggest that more granular blacklisting policies (e.g., FIFO) could even be negotiated on a per-transaction basis. Abramova et al. [1] introduce the *Seniority* policy, in which taint is assigned to outputs in ascending order. Here, any taint in the inputs is assigned to the first output until all of its value is tainted, followed by the second output and so on. Anderson et al. [2, 3] discuss the *FIFO* policy in detail, where taint is mapped to outputs in the order that it enters the inputs. They show that there is legal precedent for using FIFO in English law and discuss some of the advantages of using FIFO over the poison and haircut policies. In addition to these existing policies, combining ideas from the FIFO and the Seniority policy, we also analyze an *Output-based Seniority* policy, where taint is assigned to outputs similar to FIFO, but aggregated towards the beginning of each output. Such a policy allows a more granular distribution of taint in transactions with potentially many inputs and outputs. Figure 3 provides a visual explanation of these five policies.

Note that in contrast to account-based systems the order in which payments are made to an *address* is irrelevant for the application of the taint policies. Taint is propagated on the level of individual transactions only, based solely on the order of inputs and outputs in the transaction.

5.1 Characteristics

In the remainder of this section we explore the design space for blacklisting policies and discuss the advantages and disadvantages of the individual policies. To this end, we put forward a set of characteristics to evaluate them. We call a characteristic *global* if it affects either other users or impacts the overall system (e.g., by changing incentives), whereas *local* characteristics are only relevant to individual users sending or receiving funds in a transaction.

5.1.1 Local Characteristics

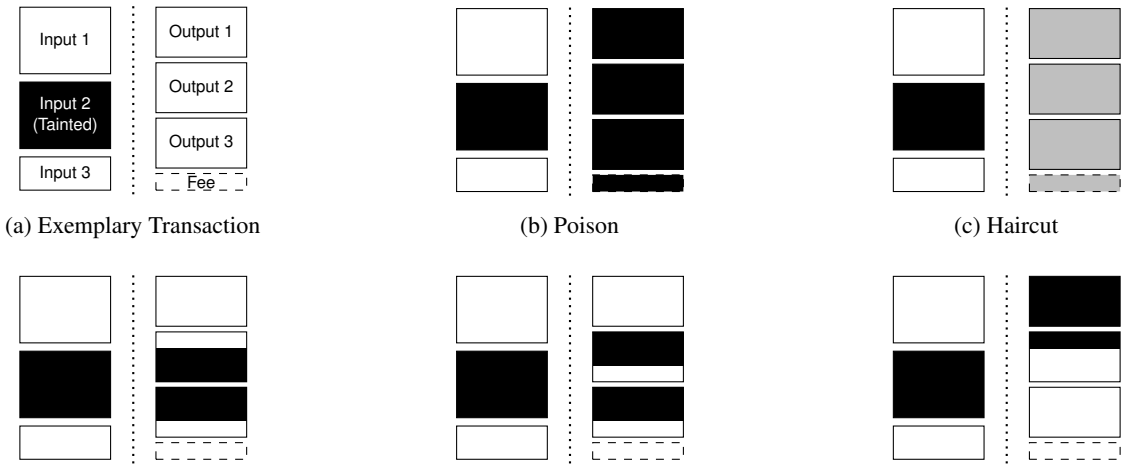
We start with two basic properties. A policy *preserves value* if the total amount of tainted value is the same before and after a transaction involving tainted coins. The poison policy does not preserve taint, since any infinitesimal amount of tainted value in the inputs completely taints all value in the transaction's outputs. All other policies preserve taint, though the haircut policy requires to pay special attention towards the potential occurrence of rounding errors.

A policy is *deterministic* when at the time of creating the transaction it is clear how a blacklisted input would affect the distribution of taint to the outputs. All previously discussed policies have this property as their taint propagation does not depend on any outside circumstances. A counterexample would be a policy where the order in which outputs of a transaction are spent determines the distribution of taint, which could create perverse incentives for the recipients of coins.

Blacklisting policies can change the way users construct and agree on payments. Most importantly, the risk of future blacklisting of inputs can be managed by changing the structure of a transaction (i.e. the order of inputs and outputs), as it determines which and to which degrees outputs are affected.

In a normal setting, the user creating the transaction (i.e. spending their own funds) may have an advantage in the form of additional information about the origin of the coins, and hence about the risk of future blacklisting. For example, they might know that a coin came from a reputable exchange, or rather from a shady mixing service. Large intermediaries like exchanges or payment providers, on the other hand, may have access to additional private information that the user creating the transaction does not. For example, they could have access to a proprietary blockchain analysis software that provides more accurate risk estimates than public sources. Furthermore, a merchant or exchange receiving money usually has a stronger bargaining position to enforce a transaction structure that limits their risk exposure. The construction of a transaction hence depends upon these potential information asymmetries and power imbalances.

A policy may allow users to *distribute risks* of receiving blacklisted coins, e.g., by allocating taint not equally among all outputs, but to specific outputs instead. Both the poison policy and the haircut policy do not allow to distribute risk since all outputs are affected equally (either completely tainted with



(a) Exemplary Transaction (b) Poison (c) Haircut

(d) FIFO (e) Output-based seniority (f) Seniority

Figure 3: How different tainting policies propagate taint from inputs to outputs

poison, or tainted relative to their value). All other policies assign taint to specific outputs rather than uniformly. The Seniority policy, especially, assigns all taint to outputs in order. This enables users to direct the risk by choosing which output to put first and potentially overfund that output to add some buffer before taint is assigned to the other outputs.

To address the issue that the transaction creator may have private information about the quality of inputs, a policy can be considered *ungameable* only if modifying the order of inputs cannot influence a potential taint distribution in their favor. Any policy that does not allow to distribute risk is ungameable, and so is the Seniority policy where the distribution of taint only depends on the total amount of taint in the inputs.

In a traditional Bitcoin transaction, users may arrange inputs and outputs in any order they choose. This could change in a blacklisting regime, as users may construct transactions such that they achieve some desired outcome based on the specific policy. As a result, more information about the origins and recipients of funds is revealed, reducing users' privacy. Generally, a more even distribution of taint is more *privacy-preserving* than a concentration of taint, as it reduces the concern for which counterparty receives the taint.

A typical Bitcoin transaction has two outputs: a spend output and a change output. The Seniority policy allows one user to take over a larger share of the risk of receiving blacklisted coins by putting their output first. In a scenario where the buyer may have less bargaining power than the seller, they might be responsible for taking over the risk of receiving blacklisted coins. As a result, it's more likely that the change output is the first output rather than the second, which hurts privacy. In a FIFO policy, taint is not concentrated, but the order of inputs may reveal information about the expected risk for each output, which allows similar considerations about identifying the change output to be applied.

5.1.2 Global Characteristics

Enforcing blacklisting policies not only changes how users construct transactions, but can also more generally affect the whole cryptocurrency.

Blacklisting has the potential to impact many users once taint gets sufficiently diffused among coins as they change hands. One strategy to reduce this diffusion is to *aggregate* taint in each transaction: rather than distributing taint equally among all outputs or splitting it up in small chunks, taint entering a transaction is combined. Consider the FIFO policy, where every small chunk of taint entering a transaction in the inputs is mapped identically to the outputs. Instead, the Seniority policy allocates all taint in the transaction towards the first outputs, thereby reducing diffusion. Output-based seniority, in comparison, aggregates taint in individual outputs.

Blacklisting policies also need to take transaction fees into account and can thereby affect mining incentives. Tainting fees is important, as otherwise any complicit miner could launder stolen coins through a transaction that designates all of its value to the transaction fee. When tainting fees, the taint of individual transaction fees must thus be directed into the coinbase transaction of the block that includes the transaction, even though no direct reference exist. If the mechanism chosen to taint fees minimizes the risk for miners to receive tainted fees and does not disincentivize them from including transactions, the policy is *miner-friendly*. In practice, one may not be able to prevent transaction fees from ever be tainted or the miners from ever be affected. However, the policy should allow to minimize such interference with a miner's incentive to include transactions based on the fee they pay.

To consider transaction fees in such a way, two design choices must be made: the position of the fee as a "virtual output" in a transaction, and the position of the fee as a "virtual input" in the coinbase transaction. The choice of the output

Table 2: Properties of different blacklisting policies

Property	Poison	Haircut	FIFO	Output-Seniority	Seniority
Value-preserving	○	◐	●	●	●
Deterministic	●	●	●	●	●
Risk is distributable	○	○	◐	◐	●
Ungameable	●	●	○	○	●
Privacy-preserving	●	●	◐	◐	○
Aggregating	○	○	○	◐	●
Miner-friendly	○	○	◐	◐	◐
Backtrackable	○	○	●	○	○

Provides property ● fully, ◐ partially, ○ not

position is most important for both the Output-based and regular Seniority policy. Setting the fee first would increase the likelihood that a miner receives tainted fees, setting it last makes the policy more miner-friendly. With regards to the order of coinbase reward and fees in the coinbase transaction, putting the fees last would allow a miner to not claim transaction fees but still include transactions when using the FIFO or Output-based seniority policy (as miners can choose to claim less than the sum of coinbase reward and total amount of fees in a block). Putting the fees first denies miners this flexibility.

Anderson et al. [2] highlight that with the FIFO policy taint can be followed backwards: starting from a tainted output one can map the taint back to previous transactions. While this *backtrackability* potentially allows for a more efficient calculation of the taint status of outputs in a database system, it makes no difference with regards to the application of the policy in practice.

5.1.3 Summary

We summarize the properties of the five different blacklisting policies in Table 2. The Seniority policy has the most desirable global properties, but does not necessarily preserve privacy well. Poison and Haircut preserve privacy, but have other undesirable properties such as not aggregating taint. FIFO or Output-based Seniority may provide a middle ground, with both being harder to reason about than Haircut and Seniority.

5.2 Empirical Evaluation

Historic data is not indicative of how a blacklisting policy would affect transactions on a blockchain once it is put into place, as users might change their behavior in response. Nevertheless, it can still be useful in order to get a better understanding of the overhead they *could* impose. To this end, we implement the five blacklisting policies on top of BlockSci [30] and evaluate them using data from the Bitcoin (BTC) blockchain until 30 June 2019. As such, this analysis could be seen as a worst-case analysis where no attention is given to the blacklist status of a coin.

We evaluate the impact of the different policies on three datasets: ransomware payments for the Cerber and Locky ransomware [27], payments to the addresses blacklisted by OFAC [62] as well as a list of addresses from blackmail (sextortion) scam emails collected by us (listed in Appendix A). For each of these datasets, we mark the outputs as tainted and then propagate the taint through the transaction graph, up to height 583236 of the Bitcoin blockchain.

We are interested in the total number of outputs tainted as well as the their age and the distribution of value among those. In initial testing, both the poison policy and the haircut policy were quickly deemed impractical due to the large number of outputs they affect (cf. Table 3 – while in theory Haircut should affect the same total number of outputs, in practice very small taint values and rounding often led to only a subset of those outputs actually receiving taint). Due to the large number of outputs tainted by those policies, we will only focus on the FIFO and Seniority policies in the remainder of this section.

Between FIFO, Seniority and Output-based seniority, FIFO consistently tainted less outputs than the Seniority policies. This is surprising since Seniority merges chunks of taint spread among many inputs into a single output. Inspecting the tainted outputs, we discovered that structural properties of the current transaction graph are likely responsible for this. Funds often ended up in places where small outputs were used to confer additional metadata in a transaction (cf. [6]). We also hypothesize that the prominence of peeling chains could lead to a higher number of tainted outputs. To test the effect of transaction graph structure on the Seniority policy, we implemented a reversed Seniority policy, assigning taint to outputs starting from the last to the first. Interestingly, this reduces the number of tainted outputs roughly in half, confirming that graph structure has indeed an influence on the total number of outputs tainted. While this behavior isn't indicative of how the Seniority policies would perform in a blacklisting regime, we cannot empirically confirm their benefit of merging taint.

With FIFO, an output can contain multiple chunks of taint. The difference between the number of outputs and the number of chunks varied considerably between the datasets, with the number of chunks sometimes exceeding the number of outputs tainted with the other policies. A large number of chunks would make reasoning about the selection of inputs for a transaction complicated in practice.

In Appendix B we provide value and age distributions for these analyses. Comparing the share of taint within tainted outputs we find that most outputs tend to either be fully or barely tainted. Inspecting the creation time of the tainted outputs, we see that they are skewed towards more recent times, but distributed over the entire time frame.

Table 3: Total number of outputs tainted with different datasets on 06/30/2019

Dataset	Poison	Haircut	FIFO	FIFO (Chunks)	Output Seniority	Seniority	Reversed Seniority
Blackmail	22562097	7582173	1609	1988	6110	12513	6665
OFAC	–	–	236919	680317	398038	777248	439014
Ransomware	–	–	471589	1863619	700805	1386267	562153

6 Blacklisting and Privacy

Blacklisting is enabled by the ability to follow coins from one transaction to the next. At the same time, this transparency can be a privacy issue, and a variety of designs for more private cryptocurrencies have been proposed [39, 58, 64] and are being deployed. This raises the question about the privacy implications of blacklisting, how blacklisting interacts with various privacy techniques, and whether adopting blacklisting in Bitcoin can be effective or would simply push illicit use towards systems where regulation of this form is not possible.

6.1 Compatibility with Privacy Techniques

There are a different techniques that can be applied to increase the privacy of Bitcoin transactions. On a structural level, it is currently possible to distinguish transactions from each other based on a variety of inherent properties. For example, users can receive payments to a single address, or to a combined address of multiple addresses for which multiple of the owners then need to agree to spend the funds (so called multisig). These different types of transactions can easily be distinguished from one another. Multiple proposals are currently in the process of being evaluated and implemented that could unify the appearance of transactions [25]. However, since they do not change the general existence of inputs and outputs, they are fully compatible with blacklisting.

Arguably the biggest privacy issue in Bitcoin right now is address reuse [24, 37]. Address reuse allows to link multiple payments to or from the same user together, potentially revealing transaction patterns and other related addresses that are owned by the same user. Done iteratively, this may allow to associate large parts of the ecosystem with specific identities.

Since blacklisting does not depend on addresses, it is compatible with techniques that provide remedies against address reuse, such as the use of one-time addresses [13]. So far, these techniques have seen limited use in Bitcoin due to their complexity and performance overhead [41], but they could be added on top of Bitcoin (or other transparent cryptocurrencies) without any impact on blacklisting.

Another possible privacy improvement is hiding the values of transactions. Unique values may allow to infer the purpose of transactions or perform re-identification through other datasets [20]. Hiding the values in transaction reduces the choice of a blacklisting policy to the poison policy. All other policies make use of the amount of taint in order to map it proportionally to the outputs.

6.2 Incompatibility with Privacy Techniques

There exist a number of privacy overlays for Bitcoin, the most popular being CoinJoin (e.g., [33, 36, 41, 42, 57]). In a CoinJoin transaction, multiple users facilitate a joint transaction by combining multiple sets of inputs and outputs into a single transaction. Such a transaction makes it hard to determine which inputs correspond to which outputs, and it breaks a popular deanonymization heuristics used by blockchain intelligence companies that assumes that all inputs to a transaction belong to the same user. In a blacklisting regime, users face the risk of their outputs being tainted by other users, which would lead to a decline in the use of CoinJoin in the absence of signaling or coin negotiation [1, 42].

In Section 3.1 we highlighted the difference between tracing coins and tainting coins. Tainting is concerned with mapping taint from inputs to outputs, whereas tracing is concerned with the ability to identify which coins are spent in a transaction. The latter is useful to efficiently verify the validity of a transaction, and so far we've assumed perfect traceability of coins. But while Bitcoin's traceability provides great transparency and enables blacklisting as an effective regulatory approach, being able to tell which coins are spent in a transaction is also a potential privacy issue. Other cryptocurrency designs, such as Zerocash [58] or Cryptonote [46, 64] are designed to obfuscate this connection and increase privacy by making coins untraceable. In such cryptocurrencies there no longer exists a unique link from one transaction to the next, rather, there is an anonymity set of possible links (the size of which varies between these designs). In the Monero cryptocurrency (based on Cryptonote), transactions select a small number of possible origins for coins spent.

While perfect traceability makes tainting coins straightforward, it is not necessary to give up all privacy in order to achieve effective tainting. The goal of blacklisting is to separate illicit coins from the legal economy. In order to achieve this, it is necessary to identify illicit coins, but not which coin exactly a user is spending. It only matters that they are not spending a tainted coin. In principle, users could still enjoy an anonymity set of potential coins that they are spending from, as long as these don't include any tainted coins. Figure 4 visualizes this distinction: by excluding the tainted coin from the set of possible coins being spent one shows that their coins

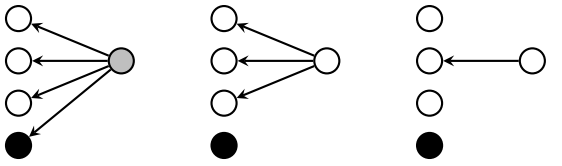


Figure 4: Limited untraceability does not preclude taintability

Privacy technique	Viable taint policies
Transaction uniformity	All
+ address unlinkability	
+ encrypted amounts	Poison only
+ transaction unlinkability	None

higher degree of privacy

Figure 5: Applicability of taint policies given levels of anonymity in the cryptocurrency

don't have illicit origin while still including other, untainted coins in order to achieve (slightly reduced) untraceability.

In cryptocurrencies based on the Zerocash design, the entire set of outputs can make up the anonymity set. So far, users have been slow to adopt these privacy features [31], but a widespread use would make the coexistence of untraceability and taintability difficult. The major practical challenge in enabling blacklisting for untraceable cryptocurrencies is to develop an efficient mechanism that allows users to dissociate their coins from tainted coins. For coins with large anonymity sets, it is necessary to recursively prove this for all coins that were created after the tainted coin. Whether this could somehow be incorporated into the cryptographic zero-knowledge proof systems these cryptocurrencies are built upon is an interesting open research question.

In Figure 5 we summarize the effect of the different privacy mechanisms on the choice of a taint policy.

6.3 Towards Regulation that Balances Privacy with Regulatory and Investigatory Needs

As the cryptocurrency ecosystem matures, more and more technical solutions are being developed that increase financial privacy (e.g., [39, 52, 58, 64]). Privacy is important: individual users don't want their everyday purchases to be identifiable on the blockchain, and companies prefer to hide their financial activity from competitors. At the same time, private, decentralized cryptocurrencies raise challenges for regulators to investigate crimes such as money laundering, corruption or tax evasion and to enforce relevant laws. While regulators shouldn't (and likely cannot [63]) hinder the development and distribution of such systems, they may be able to steer their development and adoption towards a cryptocurrency landscape that balances privacy with regulatory needs.

In the following, we attempt to sketch one option for a potential middle ground, combining blacklisting with privacy-preserving payments. Users should be able to transact privately for everyday purchases (e.g., buying medications at a pharmacy), while payment systems would, at the same time, provide transparency and accountability for larger payments (e.g., significant financial donations to political parties) with the ability to blacklist funds from illicit origins.

We divide payment activity in cryptocurrencies along these lines (cf. Figure 6). High value transactions and the storage of large amount of coins is done in transparent cryptocurrencies such as Bitcoin. Large cryptocurrency holdings are usually accessed infrequently, and can be securely stored, e.g., using hardware security modules or by implementing additional fail safes [34, 45]. Large transactions are also facilitated in this layer. If any of those coins are stolen or used for illegal purposes, they could be effectively blacklisted due to their low frequency of use.

More frequent, low value transactions are facilitated on a second layer. These could involve payment networks or other overlays, e.g., those focused on increased privacy protections. The value that can be moved through this layer would be limited, either organically (e.g., channel capacity and number of open channels in payment networks) or through technical means. For example, these systems might cryptographically ensure that users can only transact up to a certain limit without regulatory oversight [67], or more rigid KYC requirements could be enforced by more centralized overlays. A third approach could be to enforce regular movement of coins out of the private overlay layer into the transparent base layer.

Blacklisting or technical limits at the intersection between the two layers prevent structuring, i.e. splitting up large amounts into smaller ones to launder them in the second layer. With payment channel networks, blacklisting creates a disincentive for money mules to open channels with illicit funds, since they would be stuck with tainted coins. The same applies to more centralized solutions, where coins need to be checked when moved in and out of the system.

7 Discussion of Common Concerns

In this section we address some explicit concerns around blacklisting that have surfaced in discussions about the topic.

7.1 Concern: Blacklisting Destroys Bitcoin

A common concern is that blacklisting could potentially make Bitcoin unusable as a whole. If coins mix too quickly

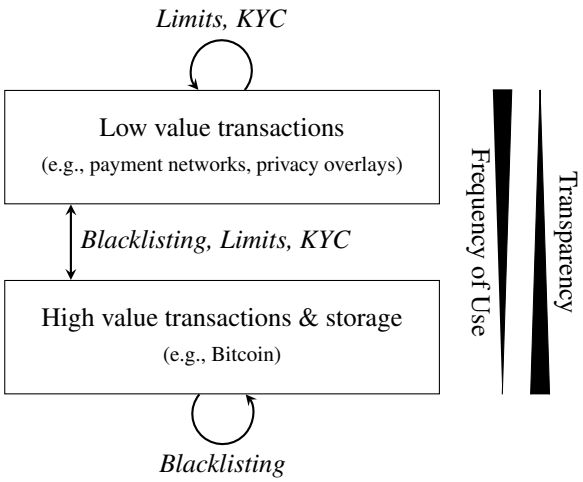


Figure 6: Framework for Effective Cryptocurrency Regulation

with other coins, especially on exchanges that process large amounts of value, then a large numbers of coins could become tainted. Similarly, users could become afraid of accepting illicit coins or simply turn to alternative payment methods due to the overhead that blacklisting imposes.

A related concern is that of reduced fungibility. Fungibility describes the ability to exchange one coin for any other coin of the same denomination. It is reduced if users are able to discriminate between coins of different quality. Bitcoins are by design not fungible. The ability to discriminate between coins based on their history is a core aspect of Bitcoin's design: the ability to uniquely identify and keep track of unspent coins enables the efficient verification of transactions.

To address these concerns, it is first of all useful to point out that no regulation option will always achieve perfect results. There can always be cases where money laundering succeeds and retroactive blacklisting could affect a large number of (innocent) users, which might deter regulators from blacklisting those funds. While the threat of blacklisting even in those situations is (to a certain degree) required to make users check blacklists in the first place, in practice regulators will likely seek a balance between these two competing interest. As discussed in Section 5, more granular blacklisting policies than Poison or Haircut also help to significantly reduce the impact of such listings.

Given today's importance of centralized platforms such as exchanges, their ability to provide more user-friendly solutions for dealing with blacklisting (cf. Sections 3.5, 4.2 and 4.4) might initially drive more users towards centralized solutions, reducing decentralization in the cryptocurrency until sufficient tools are available for normal users to manage the overhead of blacklisting effectively.

7.2 Concern: Blacklisting Destroys Privacy

In a blacklisting regime, outputs with illicit origin are tainted in order to prevent them from being mixed with legitimate coins. Tainting an output does not require any information about the holder of the coin and also does not reveal any additional identifying information (unless the regulator chooses to make such information public). In the long term, blacklist-based regulation could reduce the importance of current widespread address-based deanonymization attempts for money-laundering detection, yielding an overall benefit for normal users' privacy.

When users decide whether to accept coins, there are two potential impacts on privacy. While the blacklist allows users to check coins for potential taint, they might ask for the counterparty's identity in order to assess the risk of future blacklisting, or to enforce claims through the legal system if the coins get blacklisted in the future. However, in many e-commerce scenarios such information is exchanged anyways, and this information usually stays private between the two parties involved in the transaction.

The choice of the policy also affects privacy (cf. Section 5). For example, with the Seniority policy some outputs can be more likely to be change outputs than others. This should be an important consideration when deciding on a policy, with FIFO and Output-based seniority providing potentially more privacy.

7.3 Concern: Criminals Will Use Anonymous Cryptocurrencies Instead

Another concern is that money laundering can be evaded by using more anonymous cryptocurrencies. However, ease of use and the ability to quickly convert into or out of a cryptocurrency are desirable features for criminals, too. Compared to Bitcoin, privacy-focused cryptocurrencies are currently more difficult to use and enjoy less acceptance, making them less attractive for criminals.

Furthermore, it is unclear how regulators will approach fully anonymous cryptocurrencies once they gain traction for illegal use. That Bitcoin's transparency enables certain types of criminal investigations might be one of the reasons why regulators haven't acted more aggressively yet [48]. The regulatory landscape for anonymous cryptocurrencies might thus see change as their adoption increases.

7.4 Concern: Blacklisting Will Turn into Whitelisting

In a blacklisting regime, users are exposed to the risk that a coin might get blacklisted in the future. To manage this risk, intermediaries might only accept known "good" coins, effectively creating a system in which only such "whitelisted" coins are accepted.

Regulated intermediaries might indeed exchange information about coins they hold to make risk scoring easier. As long as whitelisted coins are determined based on their transaction history, and not on the identity of the coin holder, it would retain the open and permissionless properties of the Bitcoin network. However, a purely whitelist-based system would have significant overhead over a blacklist-based system. Tracking and constantly verifying the set of all whitelisted coins would have much worse performance than tracking blacklisted coins – after all, illicit activity only constitutes a small share of activity in cryptocurrencies. Requiring intermediaries to make their coin holdings public could also create significant privacy and confidentiality issues.

7.5 Concern: Blacklisting Can be Avoided by Moving Coins Across Chains

If criminals were able to easily convert their coins into another cryptocurrency, then blacklisting would need to potentially occur across different chain, making it a lot harder to apply and manage in practice.

However, blacklisting across chains is only necessary when the original coins do *not* retain their value. In most cases, users will sell their coins to a counterparty and receive new coins in a different denomination in return. Similar to normal purchases, the counterparty is incentivized to check the taint and risk of future blacklisting before accepting coins, hence there's no need to track taint across currencies. This not only applies to centralized exchanges, but also to most atomic swap protocol, where users can swap their coins with another user without counterparty risk.

In a few scenarios coins may actually (temporarily) lose their value on the original chain. With a sidechain, coins are locked on the original chain, effectively transferring their value to the sidechain [5]. Users accepting coins on the sidechain would need to check the taint of the coins that were locked up on the original chain. Other mechanisms could include "burning" coins on one chain (i.e. making them unspendable) in order to receive coins of equal value on another chain. In such cases, the taint of the original coins would need to be applied to the newly minted coins on the other chain (this is quite similar to how transaction fees are mapped into the coinbase transaction). This could be automated if redeeming coins on the new chains involves a (transparent) proof of the coins being destroyed/locked up on the original chain.

7.6 Concern: Blacklists will be Abused for Political Censorship

Another concern is that governments can use blacklists to block funds outside of money laundering, for example, for the purpose of political censorship. However, blacklisting should not significantly increase the potential for such actions.

First, blacklisting needs to identify concrete outputs on the blockchain. Since addresses can be created anonymously to receive funds, there's no easy way for a government to identify outputs belonging to a specific entity. Second, the transparency of the system also increases accountability. A public listing can be discussed and objected much more easily than an account closure at a bank for undisclosed reasons. Blacklists do not enable censorship beyond what is already possible, e.g., through political pressure on exchanges to not accept certain funds.

8 Conclusion and Outlook

In this paper, we have laid out how cryptocurrency regulation through blacklisting would change the Bitcoin ecosystem. Blacklisting can be an effective regulation approach that works on top of existing cryptocurrencies, improves AML outside of regulated intermediaries and protects users from inadvertently accepting illicit funds. While blacklisting also puts additional burden on users and intermediaries to check coins for taint before accepting them and to assess the risk that those might get blacklisted in the future, recursive blacklisting of funds remains effective if cryptocurrencies gain further adoption and more payments are facilitated without the involvement of regulated intermediaries. Blacklisting does not substitute existing AML measures, but rather complements them and reduces current reliance on the imperfect knowledge of identities behind pseudonymous account identifiers.

Improving AML in Bitcoin through blacklisting introduces some of the inefficiencies from the traditional financial sector, such as in the case of delayed payouts to protect against future blacklisting. Regulators shouldn't be afraid to trade off some of cryptocurrencies widely touted advantages in order to reinforce existing AML efforts through new regulation strategies. While blacklisting comes with some overhead and a degree of central control, it retains cryptocurrencies' openness, decentralized infrastructure and transparency.

In writing this document we hope to provide a useful starting point for discussion around the feasibility of blacklist-based regulation of cryptocurrencies. If cryptocurrencies are to become more popular, effective means of addressing financial criminal activity will be desperately needed.

Acknowledgments

We thank Rainer Böhme, Mihir Kshirsagar, Danny Yuxing Huang and Kevin Lee for their feedback on an earlier draft of this paper, Johanna Grzywotz and Aljosha Judmayer for helpful discussions, and Harry Kalodner for his help with implementing the taint policies in BlockSci.

This work is supported by NSF Award CNS-1651938 and a grant from the Ripple University Blockchain Research Initiative.

References

[1] Svetlana Abramova, Pascal Schöttle, and Rainer Böhme. "Mixing Coins of Different Quality: A Game-Theoretic Approach". In: *Financial Cryptography and Data Security*. Ed. by Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson. Cham: Springer International Publishing, 2017, pp. 280–297.

[2] Ross Anderson, Ilia Shumailov, and Mansoor Ahmed. "Making Bitcoin Legal". In: *Security Protocols Workshop*. 2018.

[3] Ross Anderson, Ilia Shumailov, Mansoor Ahmed, and Alessandro Rietmann. "Bitcoin redux". In: *17th Annual Workshop on the Economics of Information Security (WEIS)*. 2018.

[4] Gavin Andresen and Mike Hearn. *BIP 70: Payment Protocol*. URL: https://github.com/bitcoin/bips/blob/master/bip-0070.mediawiki (visited on 01/13/2019).

[5] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille. "Enabling blockchain innovations with pegged sidechains". In: (2014).

[6] Massimo Bartoletti and Livio Pompianu. "An analysis of Bitcoin OP_RETURN metadata". In: *Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers*. Springer. 2017, pp. 218–230.

[7] Bryan Bishop. *Bitcoin vaults with anti-theft recovery/clawback mechanisms*. 2019. URL: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2019-August/017229.html (visited on 09/25/2019).

[8] *Bisq - The decentralized Bitcoin exchange*. URL: https://bisq.network/ (visited on 02/13/2019).

[9] Rainer Böhme, Johanna Grzywotz, Paulina Pesch, Christian Rückert, and Christoph Safferling. *Bitcoin and Alt-Coin Crime Prevention: A Recommendation for the Regulation of Virtual Cryptocurrencies*. 2017.

[10] Danton Bryans. "Bitcoin and money laundering: mining for an effective solution". In: *Indiana Law Journal* 89 (2014), p. 441.

[11] *Chainalysis – Blockchain analysis*. 2019. URL: https://www.chainalysis.com/ (visited on 02/19/2019).

[12] Nicolas Christin. "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace". In: *Proceedings of the 22nd World Wide Web Conference (WWW'13)*. Rio de Janeiro, Brazil, May 2013, pp. 213–224.

[13] Nicolas T Courtois and Rebekah Mercer. "Stealth Address and Key Management Techniques in Blockchain Systems." In: *ICISSP*. 2017, pp. 559–566.

[14] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, et al. "On scaling decentralized blockchains". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2016, pp. 106–125.

[15] Christian Decker and Roger Wattenhofer. "A fast and scalable payment network with Bitcoin duplex micropayment channels". In: *Symposium on Self-Stabilizing Systems*. Springer. 2015, pp. 3–18.

[16] Mark Erhardt. *An Evaluation of Coin Selection Strategies*. Master Thesis. 2016.

[17] Y Fanusie and Tom Robinson. "Bitcoin laundering: an analysis of illicit flows into digital currency services". In: *Center on Sanctions & Illicit Finance memorandum, January* (2018).

[18] Department of the Treasury Financial Crimes Enforcement Network. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*. FIN-2013-G001. 2013.

[19] David Fox. "Cryptocurrencies in the Common Law of Property". In: (2018).

[20] Steven Goldfeder, Harry Kalodner, Dillon Reisman, and Arvind Narayanan. "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies". In: *Proceedings on Privacy Enhancing Technologies* 2018.4 (2018), pp. 179–199.

[21] *GreenAddress Bitcoin Wallet*. URL: https://greenaddress.it/en/ (visited on 02/20/2019).

[22] Johanna Grzywotz. *Virtuelle Kryptowährungen und Geldwäsche*. Vol. 15. Internetrecht und Digitale Gesellschaft. Duncker & Humblot, 2019.

[23] JT Hamrick, Farhang Rouhi, Arghya Mukherjee, Amir Feder, Neil Gandal, Tyler Moore, and Marie Vasek. "The Economics of Cryptocurrency Pump and Dump Schemes". In: (2018).

[24] Martin Harrigan and Christoph Fretter. "The unreasonable effectiveness of address clustering". In: *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. IEEE. 2016, pp. 368–373.

[25] Alyssa Hertig. *Bitcoin's Taproot Privacy Tech Is Ready – But There's a Catch*. 2018. URL: https://www.coindesk.com/bitcoins-taproot-privacy-tech-is-ready-but-one-things-standing-in-the-way (visited on 06/03/2019).

[26] Andrew Hinkes. "Throw Away the Key, or the Key Holder? Coercive Contempt for Lost or Forgotten Cryptoasset Private Keys, or Obstinate Holders". In: *Northwestern Journal of Technology and Intellectual Property (2019 Forthcoming)* (2019).

[27] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C Snoeren, and Damon McCoy. "Tracking ransomware end-to-end". In: *IEEE Symposium on Security and Privacy*. IEEE. 2018, pp. 618–631.

[28] Patricia Hurtado. *Bitcoin Firm Chief Pleads to First-of-Its-Kind Ponzi Scam*. Bloomberg. 2015. URL: https://www.bloomberg.com/news/articles/2015-09-21/bitcoin-firm-chief-pleads-guilty-to-first-of-its-kind-ponzi-scam (visited on 02/21/2019).

[29] *It's Not Personal: How Chainalysis Collects and Uses Service-Level Data*. 2019. URL: https://blog.chainalysis.com/reports/service-level-data.

[30] Harry Kalodner, Steven Goldfeder, Alishah Chator, Malte Möser, and Arvind Narayanan. "BlockSci: Design and applications of a blockchain analysis platform". In: *arXiv preprint arXiv:1709.02489* (2017).

[31] George Kappos, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. "An Empirical Analysis of Anonymity in Zcash". In: *USENIX Security Symposium*. 2018.

[32] Sergej Kotliar. *Another view. This is what a Coinbase outage looks like on the bitcoin network.* URL: https://twitter.com/ziggamon/status/951700118830432257 (visited on 04/17/2019).

[33] Gregory Maxwell. *CoinJoin: Bitcoin Privacy for the Real World*. 2013. URL: https://bitcointalk.org/index.php?topic=279249.0 (visited on 06/30/2019).

[34] Patrick McCorry, Malte Möser, and Syed Taha Ali. "Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough". In: *Security Protocols XXVI: 26th International Workshop, Cambridge, UK, March 19–21, 2018, Revised Selected Papers*. Vol. 11286. Springer. 2018, pp. 225–233.

[35] Patrick McCorry, Malte Möser, Siamak F. Shahandasti, and Feng Hao. "Towards Bitcoin Payment Networks". In: *Australasian Conference on Information Security and Privacy*. Springer. 2016, pp. 57–76.

[36] Sarah Meiklejohn and Claudio Orlandi. "Privacy-enhancing overlays in bitcoin". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2015, pp. 127–141.

[37] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. "A fistful of bitcoins: characterizing payments among men with no names". In: *Internet Measurement Conference*. ACM. 2013, pp. 127–140.

[38] Peter E. Meltzer. "Keeping Drug Money from Reaching the Wash Cycle: A Guide to the Bank Secrecy Act". In: *Banking Law Journal* 108 (1991), p. 230.

[39] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. "Zerocoin: Anonymous distributed e-cash from Bitcoin". In: *IEEE Symposium on Security and Privacy*. IEEE. 2013, pp. 397–411.

[40] Tyler Moore, Nicholas Christin, and Janos Szurdi. "Revisiting the Risks of Bitcoin Currency Exchange Closure". In: *ACM Transactions on Internet Technology* 18.4 (2018), 50:1–50:18.

[41] Malte Möser and Rainer Böhme. "Anonymous alone? measuring Bitcoin's second-generation anonymization techniques". In: *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2017, pp. 32–41.

[42] Malte Möser and Rainer Böhme. "The price of anonymity: empirical evidence from a market for Bitcoin anonymization". In: *Journal of Cybersecurity* 3.2 (2017), pp. 127–135.

[43] Malte Möser, Rainer Böhme, and Dominic Breuker. "An inquiry into money laundering tools in the Bitcoin ecosystem". In: *eCrime Researchers Summit (eCRS), 2013*. IEEE. 2013, pp. 1–14.

[44] Malte Möser, Rainer Böhme, and Dominic Breuker. "Towards Risk Scoring of Bitcoin Transactions". In: *Financial Cryptography and Data Security, 1st Workshop on BITCOIN Research*. Ed. by Rainer Böhme, Michael Brenner, Tyler Moore, and Matthew Smith. Vol. 8438. Lecture Notes in Computer Science. Berlin Heidelberg: Springer, 2014, pp. 16–32.

[45] Malte Möser, Ittay Eyal, and Emin Gün Sirer. "Bitcoin covenants". In: *International Conference on Financial Cryptography and Data Security*. Springer. 2016, pp. 126–141.

[46] Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, et al. "An Empirical Analysis of Traceability in the Monero Blockchain". In: *Proceedings on Privacy Enhancing Technologies* 2018.3 (2018), pp. 143–163.

[47] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf (visited on 02/10/2017).

[48] Arvind Narayanan and Malte Möser. "Obfuscation in bitcoin: Techniques and politics". In: *arXiv preprint arXiv:1706.05432* (2017).

[49] *OFAC License Application Page*. URL: https://www.treasury.gov/resource-center/sanctions/Pages/licensing.aspx (visited on 09/17/2019).

[50] Masarah Paquet-Clouston, Bernhard Haslhofer, and Benoît Dupont. "Ransomware payments in the Bitcoin ecosystem". In: *Journal of Cybersecurity* 5.1 (2019).

[51] Masarah Paquet-Clouston, Matteo Romiti, Bernhard Haslhofer, and Thomas Charvat. "Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem". In: *arXiv preprint arXiv:1908.01051* (2019).

[52] Andrew Poelstra. *Mimblewimble*. 2016.

[53] Joseph Poon and Thaddeus Dryja. *The Bitcoin lightning network: Scalable off-chain instant payments*. 2016. URL: https://lightning.network/lightning-network-paper.pdf (visited on 01/14/2019).

[54] Nathaniel Popper. *After the Bust, Are Bitcoins More Like Tulip Mania or the Internet?* URL: https://www.nytimes.com/2019/04/23/technology/bitcoin-tulip-mania-internet.html (visited on 05/02/2019).

[55] Rebecca S. Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz, and Damon McCoy. "Backpage and Bitcoin: Uncovering human traffickers". In: *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. ACM. 2017, pp. 1595–1604.

[56] Christian Rückert. "Cryptocurrencies and fundamental rights". In: *Journal of Cybersecurity* 5.1 (2019).

[57] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin". In: *ESORICS'14*. Proceedings of the 19th European Symposium on Research in Computer Security. Vol. 8713. Lecture Notes in Computer Science. Berlin Heidelberg: Springer, 2014, pp. 345–364.

[58] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. "Zerocash: Decentralized anonymous payments from Bitcoin". In: *IEEE Symposium on Security and Privacy*. IEEE. 2014, pp. 459–474.

[59] Tom Schoenberg and Matt Robinson. *Bitcoin ATMs May Be Used to Launder Money*. URL: https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/ (visited on 02/08/2019).

[60] James Smith. *Elliptic and Financial Privacy*. 2019. URL: https://www.elliptic.co/our-thinking/elliptic-financial-privacy (visited on 04/11/2019).

[61] Kyle Soska and Nicolas Christin. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem". In: *Proceedings of the 24th USENIX Security Symposium (USENIX Security'15)*. Washington, DC, August 2015, pp. 33–48.

[62] U.S. Department of the Treasury. *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses*. 2018. URL: https://home.treasury.gov/news/press-releases/sm556 (visited on 01/11/2019).

[63] Peter Van Valkenburgh. *Electronic Cash, Decentralized Exchange, and the Constitution*. Coin Center Report. 2019.

[64] Nicolas Van Saberhagen. *CryptoNote v2.0*. 2013. URL: https://cryptonote.org/whitepaper.pdf (visited on 01/14/2018).

[65] Marie Vasek and Tyler Moore. "Analyzing the Bitcoin Ponzi scheme ecosystem". In: *The 5th Workshop on Bitcoin and Blockchain Research*. 2018.

[66] Marie Vasek and Tyler Moore. "There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams". In: *International conference on Financial Cryptography and Sata Security*. Springer. 2015, pp. 44–61.

[67] Karl Wüst, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. "PRCash: Fast, Private and Regulated Transactions for Digital Currencies". In: *Financial Cryptography and Data Security*. 2019.

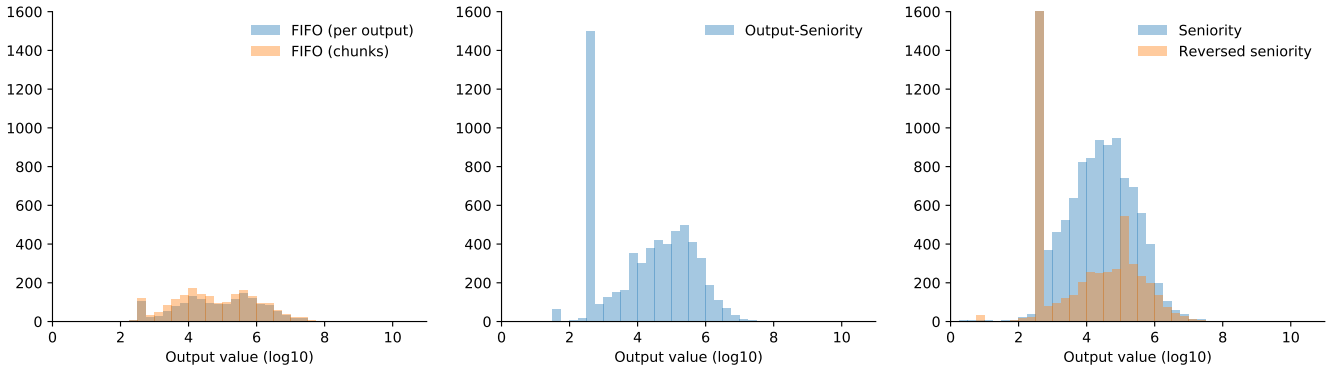
A Blackmail Scam Addresses

The following Bitcoin addresses were extracted from blackmail scam emails (often referred to as "sextortion"). The outputs sent to these addresses make up the "Blackmail" dataset used in Section 5.2.

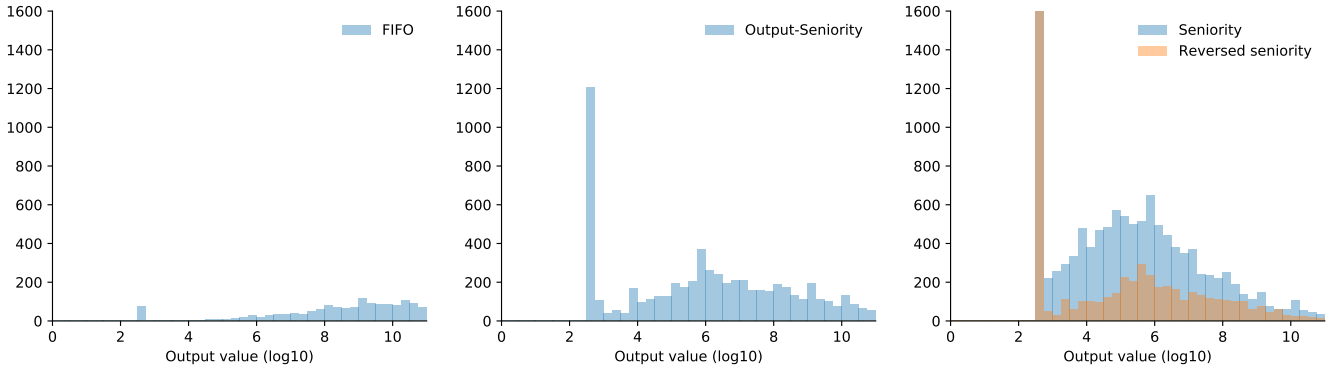
- 16oE4aRiJQvwMvbdfkx6kX8Wg9GLA1uFnz
- 1Agq5LZhY2UgcHoknVU7rZeE1x4gMuJTvf
- 13bpFXeCW6inWQSSgkVKj9rmemtkNvNoD3
- 1GPjEBZvfFRAGwCorR98upF5ByDu2Cq9Ha
- 18921mhD7bedjrgQuDmNh3oFuMQiUry1X7
- 1B3SBdx6ZqhBjUuYTzoMZq4a6Kvk4psKfM
- 19qL8vdRtk5xJcGNVk3WruuSyitVfSAy7f
- 1KzMDhZLokkNd1kcxs2mgwXm97pVvnfRBC
- 1P7bLeCJywaaDRQpT7iwb4qzUHa4CpRFyP
- 1971pHPgLaTmuYtoH4BsGSfFMZaAjotium
- 17EuB8AmyBm81FgCovdr6huCCoSzv2S7nP
- 1WLEChY6S7S97m5voZZtbQcwiEYeSNsja
- 13phdoBirrAtFXKWJQ9HgTYX9b7C2MqXPE
- 1G1qFoadiDxa7zTvppSMJhJi63tNUL3cy7
- 18Pt4B7Rz7Wf491FGQHPsfDeKRqnkyrMo6
- 3ER3byGWbnqgxN4C5amtCXHExPgGaUWsBd
- 19UW5P6PGDA3SWehh8UMGQQC3ezBzN1mDE
- 1H1K8MfLEJgjCCfDEkTJmv9GJjD3XzEFGR
- 39eaJ2Fxbm4KWVu26BzaEH465aK4yrbuzH
- 38KxdSNjge7hdy7zWZuRRC4hN4krQrrA5b
- 12s4cfoNTzT68gSdxLjmSRT3qdvaqwDWNz
- 1GoWy5yMzh3XXBiYxLU9tKCBMgibpznGio
- 15mWFjVymAdqimVim2f1UgX6oSD4TYeGLE
- 1ELgYTbMLmw9vaHADfZmMcKVMWCNmRH8S2
- 1Gm6q6M2TfL4yrL3TnvsUZZ1C5k6wrvBbX
- 34vhBcVUYwfNYjupWHrzef1zogaRZaSFU6
- 3CEx39owi6EeUAoM4ENyYdGhLZj7nAwuYH
- 1DjuN5PM9VLXCeqYrb9nxzpQ8rb2hXZiEt

B Value Distributions for Policy Analysis

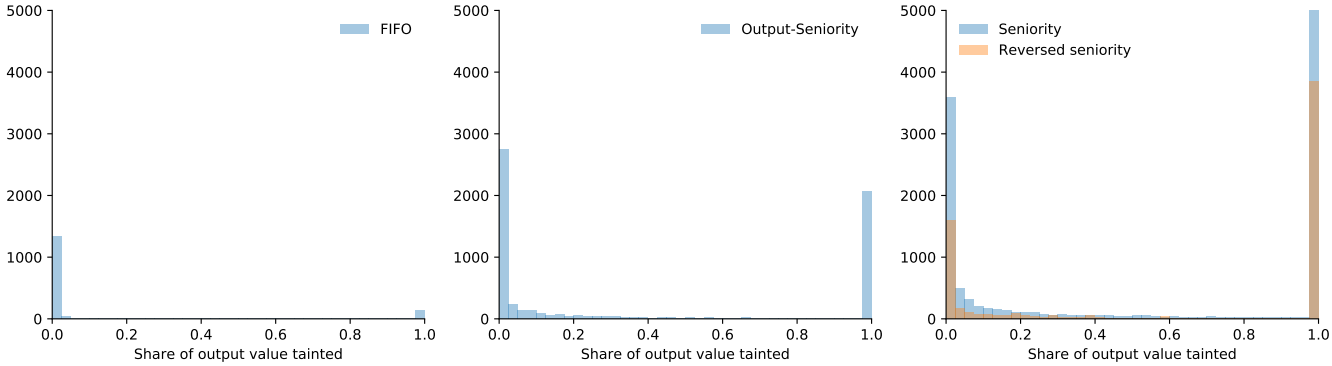
On the following pages you'll find the results of our empirical analysis (see Section 5.2) of applying different taint policies to three different exemplary data sets.



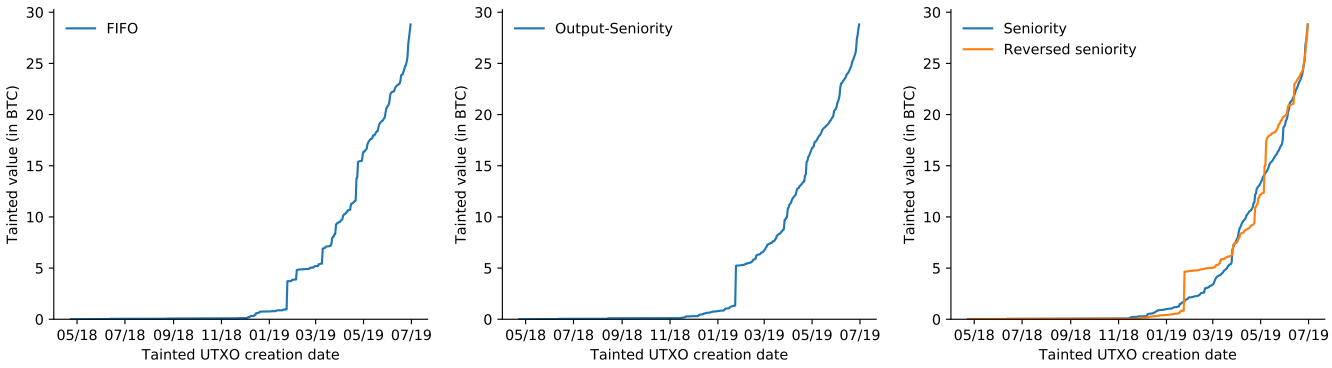
(a) Distribution of tainted value in all tainted outputs



(b) Distribution of (full) output value of all tainted outputs

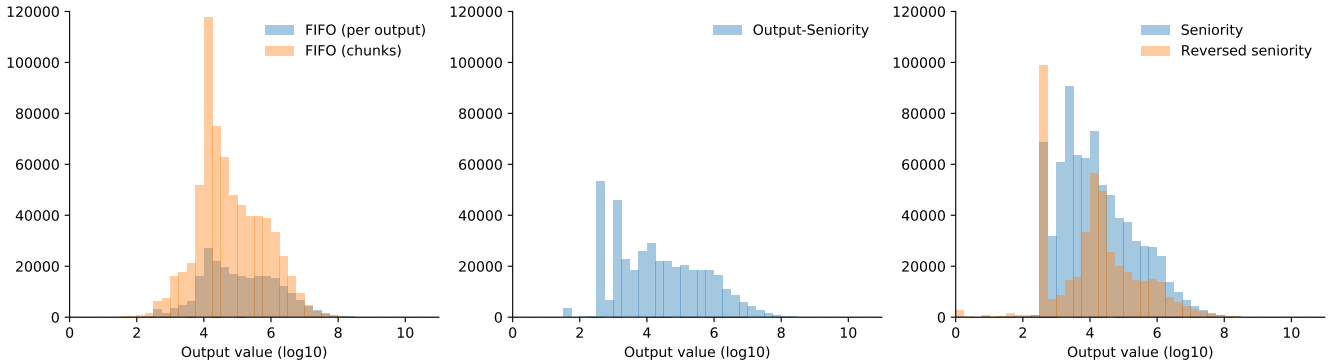


(c) Share of output value tainted

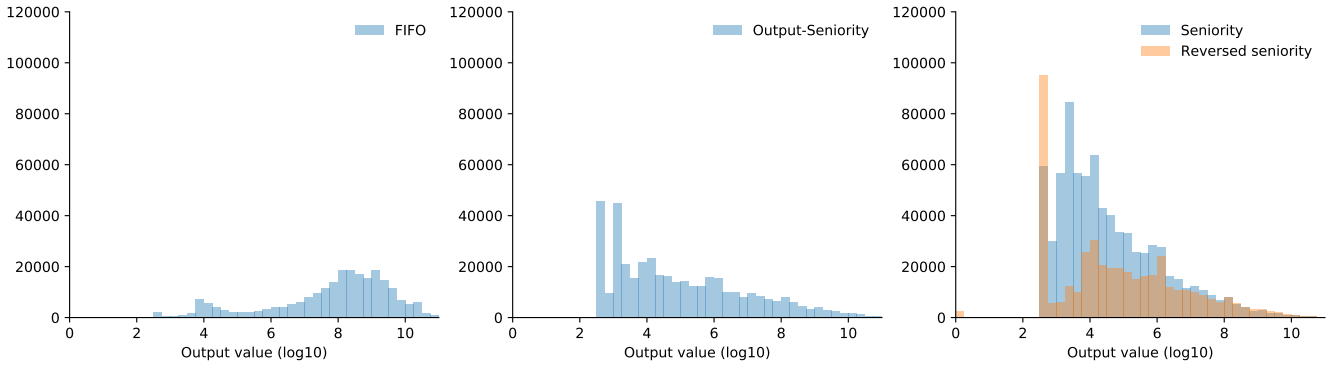


(d) Creation time of tainted unspent transaction outputs

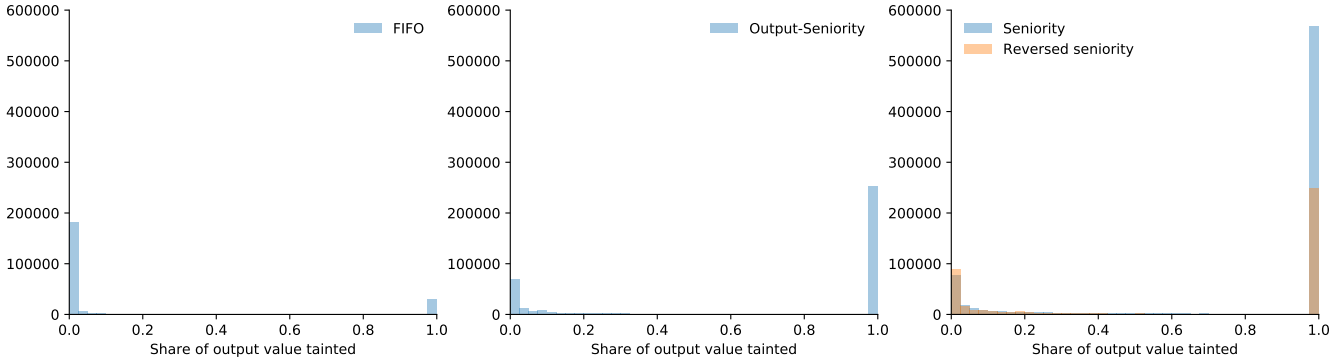
Figure 7: Analysis of the Blackmail data set



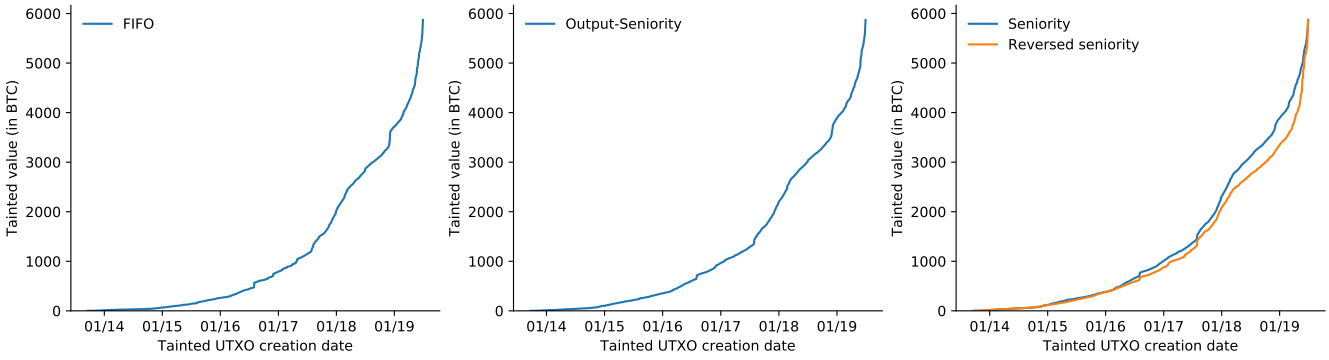
(a) Distribution of tainted value in all tainted outputs



(b) Distribution of (full) output value of all tainted outputs

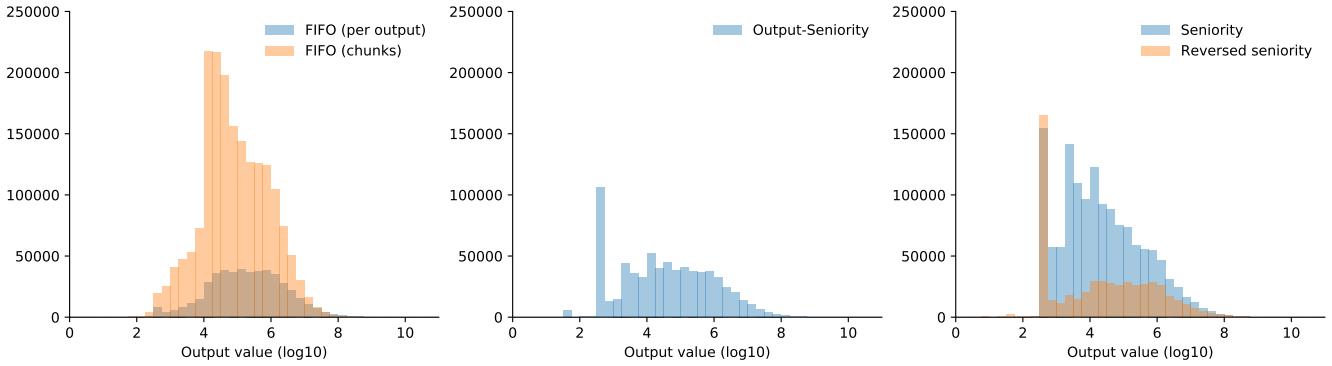


(c) Share of output value tainted

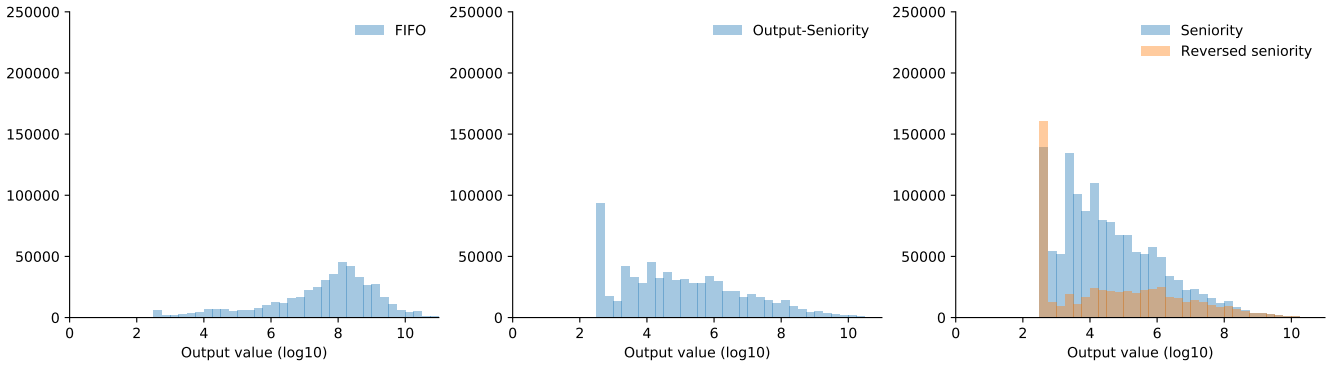


(d) Creation time of tainted unspent transaction outputs

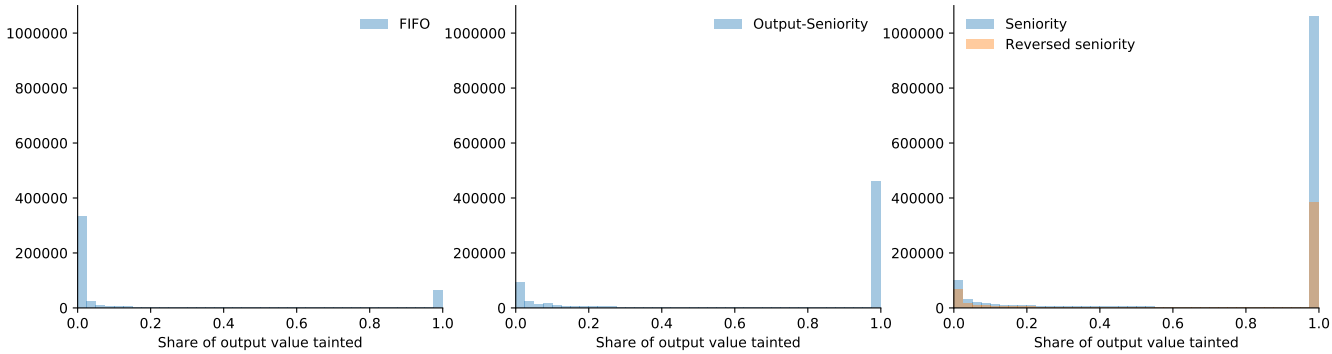
Figure 8: Analysis of the OFAC data set



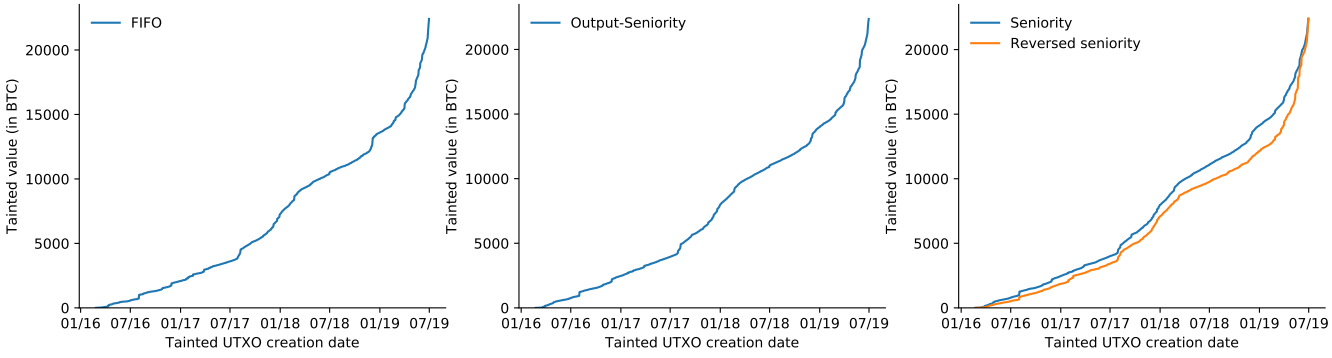
(a) Distribution of tainted value in all tainted outputs



(b) Distribution of (full) output value of all tainted outputs



(c) Share of output value tainted



(d) Creation time of tainted unspent transaction outputs

Figure 9: Analysis of the Ransomware data set