SoK: Money Laundering in Cryptocurrencies

Kartick Kolachala
New Mexico State University
Las Cruces, NM, USA
kart1712@nmsu.edu

Ecem Simsek
Sam Houston State University
Houston, TX, USA
ex059@shsu.edu

Mohammed Ababneh
New Mexico State University
Las Cruces, NM, USA
mababneh@nmsu.edu

Roopa Vishwanathan
New Mexico State University
Las Cruces, NM, USA
roopav@nmsu.edu

ABSTRACT

Money laundering using cryptocurrencies has become increasingly prevalent, and global and national regulatory authorities have announced plans to implement stringent anti-money laundering regulations. In this paper, we examine current anti-money laundering (AML) mechanisms in cryptocurrencies and payment networks from a technical and policy perspective, and point out practical challenges in implementing and enforcing them. We first discuss *blacklisting*, a recently proposed technique to combat money laundering, which seems appealing, but leaves several unanswered questions and challenges with regard to its enforcement. We then discuss payment networks and find that there are unique problems in the payment network domain that might require custom-designed AML solutions, as opposed to general cryptocurrency AML techniques. Finally, we examine the regulatory guidelines and recommendations as laid out by the global Financial Action Task Force (FATF), and the U.S. based Financial Crimes Enforcement Network (FinCEN), and find that there are several ambiguities in their interpretation and implementation. To quantify the effects of money laundering, we conduct experiments on real-world transaction datasets. Our goal in this paper is to survey the landscape of existing AML mechanisms, and focus the attention of the research community on this issue. Our findings indicate the community must endeavor to treat AML regulations and technical methods as an integral part of the systems they build and must strive to design solutions from the ground up that respect AML regulatory frameworks. We hope that this paper will serve as a point of reference for researchers that wish to build systems with AML mechanisms, and will help them understand the challenges that lie ahead.

CCS CONCEPTS

• **General and reference** → **Surveys and overviews**; • **Security and privacy** → **Security requirements**; **Privacy protections**.

KEYWORDS

Cryptocurrencies; money laundering; blacklisting

ARES 2021, August 17–20, 2021, Vienna, Austria

ACM ISBN 978-1-4503-9051-4/21/08…$15.00
https://doi.org/10.1145/3465481.3465774

ACM Reference Format:
Kartick Kolachala, Ecem Simsek, Mohammed Ababneh, and Roopa Vishwanathan. 2021. SoK: Money Laundering in Cryptocurrencies. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021), August 17–20, 2021, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3465481.3465774

1 INTRODUCTION

According to the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN), money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them [42]. Money laundering is closely associated with terrorist financing, where terrorist sponsors take advantage of differences in financial regulatory landscapes and enforcement across various countries to fund and recruit terrorists, and have begun using new payment methods such as Bitcoin and cryptocurrencies to acheive their ends [110]. Broadly, there are three stages in money laundering, *placement*, in which illicit money enters the system, *layering*, in which its sources are obfuscated, and *integration* in which the illicit money is made to appear legal [92].

Money laundering using fiat currency has been pervasive for decades and regulators have devised ways to dissuade and take punitive actions against such malfeasance. Many legal provisions and amendments have been enacted to implement anti-money laundering (AML) measures, such as the Bank Secrecy Act in the U.S., [13] and the U.S.A. Patriot Act, [115] to name two. However, the advent of cryptocurrencies such as Bitcoin [15] and Ethereum [37] has disrupted the banking industry by eliminating the use of a central authority and enabling cashless, anonymous transactions (in an anonymous transaction, the identity of the users taking part in the transaction remains hidden). Since, in cryptocurrency transactions, users use pseudonyms, and the currency itself is not nationally issued or regulated, it becomes harder to track down the origins of illicit money. While a single pseudonym can be linked to an individual, e.g., by examining transaction graphs, a criminal could potentially use thousands of different pseudonyms which makes linking difficult. In reports published by blockchain analytics companies Ciphertrace [22] and Chainalysis [2], money laundering tripled from USD 200 million in 2017 to USD 700 million in 2018 [89], and in 2020, a total of USD 1.3 billion was laundered [76] with USD 41.2 million being laundered using Bitcoin. These significant numbers call for a survey of existing AML approaches, and the challenges in implementing them.

1.1 Related Work

Prior work in cryptocurrency-based AML mechanisms has been sparse. Weber *et al.* [119] recently presented an analysis of Bitcoin transactions from the Elliptic dataset [27] using graph convolution

networks, with the goal of classifying transactions into licit and illicit categories. Shanaev *et al.* [104] analyzed the public reaction to regulatory measures of varying stringency. Fink [43] studied the current U.S. regulations for addressing money laundering in cryptocurrencies and proposed fundamental changes to the underlying Bitcoin blockchain to address regulation-based lacunae. Jacquez [54] analyzed and examined ways in which banks, financial regulatory bodies, and law enforcement agencies can prosecute illicit cryptocurrency asset owners.

To the best of our knowledge, none of the built systems for cryptocurrencies and payment networks in the academic literature take regulatory guidelines and/or AML protections into account in their system design and adversary models [14, 32, 33, 50, 52, 57, 64, 67, 98, 99]. Most current works place a premium on providing user anonymity, which seems to be at odds with AML regulations.

Our Contributions: Our contributions are: 1) We scrutinize a recent technical solution proposed for enforcing AML measures, *blacklisting*, and point out challenges in its enforcement. 2) We examine AML measures in the context of *payment networks* and identify challenges unique to payment networks. 3) We examine global and national regulatory guidelines regarding AML measures and outline potential problems in implementing or enforcing them.

Our study indicates that a lot of work needs to be done and many challenges need to be addressed for implementing effective AML measures in cryptocurrencies and payment networks. Our goal is to focus the research community's attention on these issues and spur more research in this area.

Outline: In Section 2 we describe the technique of blacklisting and detail some of the challenges in enforcing it. In Section 3, we discuss AML measures in payment networks. Section 4 describes the U.S. and global anti-money laundering regulations along with the challenges in enforcing them. In Section 5, we describe our experimental analysis, in Section 6 we make recommendations and suggest ideas towards addressing some of the major AML challenges, and in Section 7 we make concluding remarks.

2 BLACKLISTING

Blacklisting in cryptocurrencies is the process of identifying transactions that have been involved in financial crimes such as theft, money laundering, etc., and "tainting" the coins involved those transactions (marking a coin to prevent it from traded elsewhere). For fiat currencies, the U.S Department of Treasury has published a public blacklist [84] of individuals/groups that are sanctioned due to their illicit activities. Although blacklisting has not been implemented yet for cryptocurrencies in the real-world, it has been proposed in the research literature as a possible AML measure. This is helped by the fact that many cryptocurrencies that rely on public blockchains, e.g., Bitcoins, are not fungible, since the transaction history of every coin is publicly available, and a receiver can refuse to accept coins that have bene involved transactions marked as illegal. Moser et al. [82] defined two blacklisting mechanisms or polices, *Poison* and *Haircut*, among others. *Poison* policy works by tainting all the coins involved in all subsequent transactions in which an account is involved if a single transaction involving the said account's coins gets blacklisted. For example, if a user Alice's coins are discovered to be laundered money, the coins of all users involved in subsequent transactions with Alice will be tainted. The *Haircut* blacklisting policy on the other hand is less drastic, and simply taints the coins involved in the specific blacklisted transactions. There have been proposals to bring Bitcoin within the ambit of regulatory authorities, such as publishing a public "taint-list" of coins that have been known to originate from illegal sources [3]. Blacklisting the transactions recursively, and making the taint-list of coins publicly available ensures that the tainted coins involved in those transactions will be put out of circulation. The users will be disincentivized to purchase or trade in tainted coins involved in the blacklisted transactions since they will eventually taint their "good" coins too. Although the idea of blacklisting seems simple and intuitively appealing, there are several challenges that might inhibit its practical enforcement; we outline some of them below.

2.1 Challenges in Enforcing Blacklisting

1) *Accountability*: One of the issues with blacklisting is that, while it is possible to blacklist transactions, it is harder to enforce punitive action or consequences for attempting to launder money, and circumventing AML regulations. While most academic papers on this topic leave enforcing consequences as outside the scope of their work (and rightly so) [1, 3, 4, 81], we believe that it is important to hold users accountable for their actions. The exact kind of punitive action might be dependent on jurisdiction, but the worrying problem is that *there is no way to trace users*, whose coins have been tainted, since most cryptocurrencies provide anonymity and privacy to their users (users use pseudonyms), and users can create a potentially unlimited number of identifiers/addresses (public keys). These public keys can also be created using stealth addressing that make the payments from the same payee unlinkable [25, 51]. For criminals, it is the certainty of being caught and identified and made to face consequences that act as a disincentive or deterrent, hence, we believe, blacklisting only helps solve half of the problem.

2) *Cooperation*: Another challenge with creating and publishing blacklists is the high degree of cooperation it requires between agencies, in case of cross-border transactions. In the U.S. alone, there is FinCEN at the federal level, and the Attorney General Office of each state typically has its own state-level AML unit. One of the advantages of various cryptocurrencies and payment networks is the ease of conducting global transactions. For a global blacklist to be implemented, we would require a high degree of cooperation between various national AML regulatory bodies, as well as global regulatory agencies such as FATF, Interpol, and more. There are several international treaties [85, 113, 114, 117] that deal with money laundering (both fiat and cryptocurrencies) but none of them talk about or address blacklisting. Getting all stakeholders to agree upon a common minimum criteria for a blacklisting policy might not be easy, and could involve disputes, which would need to be arbitrated.

3) *Future blacklisting*: Future blacklisting refers to the situation where a user accepts coins from other users in good faith, and at a later point of time, discovers that the transactions in which these coins were involved have been put on a blacklist, consequently tainting the coins, by which time these coins could have been traded across multiple transactions. Furthermore, depending on the blacklisting policy used, the user's other coins might get tainted too,

on account of being mixed with tainted coins. One could easily imagine ways and situations in which a criminal deliberately targets a user in such a way. The research community needs to devise ways of insulating honest users from the financial consequences of their transactions getting blacklisted in the future. Delayed payments [82] have been proposed as a solution, but they are far from ideal since they are based on the assumption that the longer a coin has been unspent, the less likely it is to become tainted in the future. In addition to inconveniencing users, and slowing down transaction throughput, there is always the possibility of a malicious user exploiting precisely this (questionable) assumption to launder their coins. Besides the implicit assumption that the most recent transactions carry a high risk of future blacklisting might harm honest users.

4) *Enforce blacklisting in the presence of cold wallets*: The nature of ownership of Bitcoins could influence the enforcement of blacklisting. Several Bitcoin exchanges maintain *hosted wallets* or *cold wallets* [4]. The idea is when a user buys his Bitcoins from an exchange, the Bitcoins belonging to the user are maintained by the exchange itself, such that the user is not in actual possession of his Bitcoins, but can claim a set of coins maintained by the exchange in the exchange's wallet, called the "cold wallet". If a coin were to get tainted, tracing the tainted coin back to the exchange may be possible, but it is much harder to trace the ownership of those tainted coins to a particular user. This had led to several real-world instances of cold wallets being used in money laundering [28, 31, 103].

5) *Compensating honest users in a timely manner*: In the case of possible future blacklisting of transactions, a honest user who accepts a coin in good faith, which is later declared tainted, is at a financial loss. With current blacklisting techniques, it is not clear as to how the honest user would be compensated for her loss.

6) *Cross-chain transactions, unreliable receiver*: Another challenge is cross-chain applicability of blacklisting. If a coin is tainted, say, on the Bitcoin blockchain, what if the user owning the coin simply converts it to Ether or even fiat currency? The taint should ideally prevent the coin from being accepted on any blockchain. This is particularly relevant in the context of payment networks, where users can perform cross-currency transactions in seconds. Tainted coins might go through multiple transactions in the network thereby causing overall loss to the liquidity of the network. One could say that the receiver in every transaction will check for taint before they accept any coins, but how do we ensure this is enforced? What evidence or proof can the receiver (who might later on trade these coins) provide that convinces people that they did check for taint before accepting (and laundering) the coins? Note that this problem persists even when we use Sidechains [106], where coins from the Bitcoin blockchain can be transferred to a different blockchain.

7) *Regulating agency going rogue*: For blacklisting to work in a correct and fair manner, it seems that we would need to trust a regulatory or enforcement authority to honestly create the blacklist. If the authority responsible for creating the blacklist goes rogue, it might attempt to blacklist honest users or avoid blacklisting malicious users, e.g., [29]. To prevent this, a standard of evidence must be established, and the evidence must be made public for accountability.

3 PAYMENT NETWORKS AND MONEY LAUNDERING

Payment channel networks [14, 46, 59, 63, 64, 66, 68, 73, 75, 91, 101, 125] have been proposed as a workaround to the Bitcoin scalability problem (maximum ten transactions/second), where multiple payments are routed over a single payment channel, and blockchain writes are done only when the channel is closed, or if there is a dispute between the (usually two) parties using the channel for transactions. When two parties open a payment channel, they need to write the current channel balance to the blockchain, and if applicable, the current state of the channel's variables. Beyond that, all updates are done between the parties and are not written to the channel, unless either of the parties behaves maliciously. To facilitate transactions between two parties that may not have a payment channel currently open between them, *networks* of payment channels have been proposed [7, 20, 61, 78, 93, 100, 116, 118, 122], where two unconnected users can route payments between them, if there exists a path comprising of several connected users between them, e.g., Alice can route payments to Bob if there exists a path Alice → Charlie → Denise → Bob. Having a path of users also helps Alice and Bob avoid opening a private ledger channel between them (a private ledger channel is defined as a payment channel that exists only between two parties and it maintains a record of all their transactions), and thus incurring expensive blockchain write fees. This can be advantageous, especially in situations where Alice and Bob transact very infrequently.

Conceptually, a payment network can be modeled as a directed graph where users represent vertices, weighted edges represent link balances, and the directionality of the edge represents the direction of the payment flow. A user can route payments to another user over a path in the network that has sufficient balances on its links. Once a payment gets routed from a sender to a receiver, all edges along the path will get decremented by the transmitted amount. One of the advantages of payment networks is that users can perform global, cross-currency transactions in seconds, as opposed to days for traditional bank wire transfers, besides the transaction fees being a fraction of what a bank might charge.

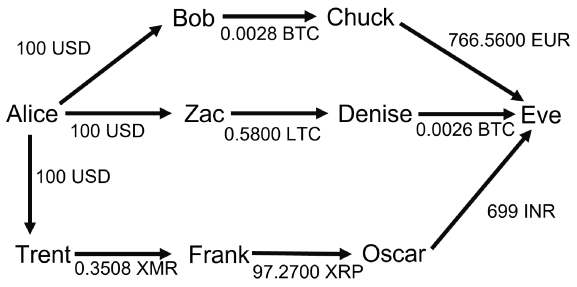

Figure 1: Payment network

Consider a payment network, as shown in Figure 1. Let us assume user Alice is in possession of tainted coins worth USD 300, and she wants to transfer money to Eve. She divides her coins into equal parts of USD 100 each and sends them across three different paths, via Bob, Charlie, and Trent). The coins then get converted into

multiple currencies before eventually reaching Eve. In this example, if all the intermediaries agree to the transaction, and the coins eventually reach Eve, Alice would have successfully laundered her money and has cleaned up her traces. Now let us assume that the transactions involving coins in Alice's possession were reported to be illicit at some point in the future, and the coins are subject to be tainted. The coins in Alice's possession can be tainted, but it would be very difficult to taint the coins spread across multiple transactions and cryptocurrencies. This would amount to tainting the coins of the entire network of users, which is unfair. Besides there is no mechanism in place to compensate the network users promptly, for any unusable (tainted) coins they might now have.

In the real-world, the largest payment network by market capitalization, Ripple, has been fined USD 700,000 by U.S. regulators [95], partly for failing to implement a credible AML program in place to curb financial crimes. Although Ripple has since then pledged to implement stringent AML procedures, payment networks designs proposed in the literature would benefit from proactively building AML controls into their system design and adversary models [35, 38, 48, 56, 66, 79, 102]. Based on the characteristics of payment networks described so far, we now outline a few challenges for implementing stringent and effective AML measures.

3.1 Challenges in Preventing Money Laundering in Payment Networks

1) Transactions in payment networks are split into multiple fragments and spread among different users in a process called structuring [10, 11, 30, 60, 70, 77, 80, 105, 109, 126]. Implementing AML guidelines becomes difficult since the fragmented amounts could be converted into multiple currencies across various geographical locations and we need to take into account the conversion history of all coins. Apart from this, most payment networks offer anonymity [36, 49, 69, 124], by making it hard to link the sender/receiver with the coins being transferred. This would make it hard to identify a coin as originating from illegal sources.

2) Payment channel networks post the final balances to the blockchain and not every individual transaction. How would we track individual transaction amounts between the sender and receiver, e.g., if one coin involved in a particular transaction is reported as illegally obtained?

3) Most of the payment networks have their transaction limits well within the threshold of the U.S. and global regulatory authorities [8, 34, 50, 53, 72, 98, 107, 108, 123], which makes them exempt from following AML guidelines. A user can easily split a large amount into smaller amounts within the thresholds. While the tactic of structuring the money with an intent of laundering it is illegal there is no mechanism to check whether the money is being structured or not. Payment networks only check if a given transaction is within their threshold or not.

4) In blacklisting, the transactions of the users involved in a crime are blacklisted and their coins are tainted. However, if we have a malicious user whose sole purpose is to taint the coins of a dense network of users, he will use his coins to initiate multiple transfers. The coins then travel along the network, tainting the coins of all the honest users in the path. This tainting of coins happens in some magnitude, no matter which policy is used for blacklisting. Hence the net value of the coins lost is *more* than the coins invested by the illicit user. Preventing this is a challenge.

3.2 Virtual Channels And Money Laundering

Each hop in a payment network incurs a routing fee, with longer paths costing more. Virtual channels [32] were developed as a special kind of payment channel that involve an intermediary, to avoid the routing fees paid to different users along the path. The advantage of virtual channels is that an intermediary is not involved in every transaction, rather only when there is a dispute between parties, and when the channel needs to be closed. When the channel is closed, the intermediary writes the final balances of both parties to the blockchain. Let us assume two users Alice and Bob who wish to establish a virtual channel via an intermediary, Ingrid. Alice and Bob open individual payment channel with Ingrid, who locks up some of her own coins in the channels as collateral (to protect against Ingrid going rogue). Alice and Bob can then open a separate virtual channel to transact with each other, which contains coins deducted from Alice and Bob's payment channels with Ingrid. They can change their individual balances on the virtual channel without any involvement from the intermediary. During the closing of this virtual channel, final balances are calculated and are written to the blockchain. This eliminates the need for both Alice and Bob to interact with the intermediary for every transaction, as in they would in the case of regular payment networks. However, this system is vulnerable to money laundering.

3.2.1 AML challenges in virtual channels: 1) The intermediary in the aforementioned scenario could place his illegal coins as collateral in the Alice-intermediary channel, which could have been obtained from the Bob-intermediary payment channel (i.e, either Bob or the intermediary, or both in collusion, want to launder coins). It is not clear how to prevent this. Note that in [32] and other proposals for virtual payment channels [58, 129], the users accept any coins in the intermediary's possession in virtual channels, without checking for taint. Even if the users check for taint, it will not protect them against future blacklisting, i.e., the intermediary's coins may get blacklisted at some point in the future. There is currently no way for honest users Alice and Bob to be compensated in such a case. There have been real-world instances of intermediaries operating unregistered exchanges, without conducting customer due diligence measures, and being aware of, but not reporting proceeds from illegal activities [19].

2) The intermediary in the above case acts as a financial intermediary by transmitting money. Hence according to the FATF guidelines, Customer Due Diligence (CDD) measures are required to be enforced, which entail collecting users' identifying information, examine the nature of the transaction, etc. Unfortunately, the current state-of-the-art in virtual channels directly works against this, by guaranteeing user and transaction privacy. It is not clear how to respect privacy guarantees while also enforcing CDD measures.

3.3 Rebalancing of Payment Networks and Money Laundering

Often certain links in a payment network run short of coins, and as a result, nodes that are connected by the depleted links become dormant. To make these nodes take part in transactions again,

the links need to be *rebalanced*, which refers to the process of replenishing the depleted links. The first such rebalancing scheme for payment networks was proposed in Revive [57]. In Revive, all nodes elect a leader, who accepts rebalancing requests from the other nodes in the network, and facilitates the rebalancing.

Let X $\overset{\$a \quad \$b}{\longleftrightarrow}$ Y denote a bidirectional credit link where "a" represents the balance on user X's end and "b" represents the balance on user Y's end. Consider a situation where three users Alice, Bob, and Charlie are a part of a payment network such that all of them are connected to each other: Alice $\overset{\$100 \quad \$0}{\longleftrightarrow}$ Bob, Bob $\overset{\$100 \quad \$0}{\longleftrightarrow}$ Charlie, Alice $\overset{\$0 \quad \$100}{\longleftrightarrow}$ Charlie. The links with zero balances cannot be used, and need to be rebalanced. In [57], all users elect a leader and submit their rebalancing requests to the leader, who uses links with higher balances to rebalance depleted ones, e.g., Alice $\overset{\$50 \quad \$50}{\longleftrightarrow}$ Bob, Bob $\overset{\$50 \quad \$50}{\longleftrightarrow}$ Charlie , Alice $\overset{\$50 \quad \$50}{\longleftrightarrow}$ Charlie. Other work in this area includes [83], which was designed specifically for rebalancing in credit networks, where nodes act as borrowers and lenders with fixed or variable interest rates. In [83], rebalancing is done as a two-step process, *balance transfer* and *bailout*. During the balance transfer phase, the node with depleted links aims to rebalance them by incentivizing other nodes to establish links with it by advertising a lower rate of interest than other lender nodes in the network. In the bailout phase, capital is temporarily infused into the node requesting rebalancing (to partially make up for the loss incurred by its low interest rates) by a trusted central party such as a bank. Once the node becomes active, and all its links have sufficient funds, the trusted party exits the network. We now cover some challenges unique to rebalancing in payment networks.

3.3.1 Challenges in enforcing AML with rebalancing. 1) If we adopt blacklisting as an AML mechanism, presumably coins will not be tainted until there is convincing evidence that the transactions they were involved in were a part of some financial crimes. In such a case, rebalancing seems particularly attractive to a criminal: he can join a payment network with many dormant links and use his money to rebalance them. By the time he is eventually caught (i.e., when the coins that are in his possession are discovered to be illegal), the net value of the illegal coins he has introduced into the network will be much greater than the value of his own illegally-obtained coins. As an example, in the aforementioned scenario for rebalancing, consider what happens if one of Alice's coins is tainted. Depending on the taint policy, if she helps rebalance Bob and Charlie's links, she can corrupt up to 100% of their coins (of both Bob and Charlie). Some taint policies such as *Poison*, taint all coins that are in a user's possession, even if a single coin is tainted, while other such as *Haircut* will only taint a percentage of the wallet per illegal coin. Regardless of what policy is used, even a single tainted coin from Alice can taint a significantly greater number of coins in circulation in the network, and make many honest users incur a financial loss. It is not clear how this can be prevented.
2) In the case of future blacklisting, if the coins with Alice in the scenario above are found to be tainted at a future point of time, we would need to rollback the rebalancing, but the network topology will likely have changed since the rebalancing took place, e.g., Alice finding new neighbors. Also, it is unclear how to deal with non-cooperative parties, and what should be the role of the leader in implementing AML mechanisms.

4 ANTI MONEY LAUNDERING REGULATORY GUIDELINES

In the U.S, financial crimes, including money laundering are regulated by the Bank Secrecy Act [13], the relatively newer Money Laundering Control Act [74], and the U.S.A. Patriot Act [115]. The Financial Crimes Enforcement Network (FinCEN), within the U.S. Dept. of Treasury, is the agency responsible for enforcing the regulations. Other organizations such as Financial Industry Regulation Authority (FINRA) [44], which operates under the Securities and Exchange Commission [47] too have come up similar guidelines to prevent money laundering. The Financial Action Task Force (FATF) [39] is a global, inter-government body that develops policies to prevent money laundering and curb terrorist financing, to which end it has put forward a set of similar guidelines that member countries must follow. We now briefly cover some of the FinCEN's and FATF's significant recommendations and then point out challenges in their correct interpretation and enforcement.

4.1 Challenges with Enforcing Regulations

1) FATF and FinCEN guidelines recommend that Customer Due Diligence (CDD) measures need to be enforced when carrying out *occasional transactions* above their specified thresholds. It is unclear if "occasionally" refers to the time between two consecutive transactions, or the number of transactions that can be carried out in a specified time frame. FATF and FinCEN guidelines state that AML measures should be applied according to a *risk-based approach*. The definition of risk, the metrics used to calculate it, and the categories which risks fall into need to be addressed in a clear way by the research community. The consequences of not unambigiously defining risks and enforcing CDD measures can be severe, as evidenced in several real-world examples where malicious actors take advantage of ambiguities in, and lax enforcement of CDD measures [16, 21, 97, 111].
2) FATF and FinCEN guidelines require that financial institutions verify the sender and receiver's information in suspicious transactions, or transactions above a certain threshold, as well as verify that the counterpart financial institutions in other countries are compliant with the national and the global AML guidelines and standards. The key challenge here is the gathering of such sensitive information when there is no mutual agreement or any treaty mandated by law between countries involved in such transactions. Criminals have taken advantage of countries not being able to exchange such information, and being unable to keep track of shell banks within their borders [88].
3) FATF requires countries to identify the various risks that can arise from the operation of Virtual Asset Service Providers (VASPs). There is no clear description of the definition of risk and its quantification measures. Malicious users have laundered money exceeding USD 250 million by exploiting this ambiguity [62]. FATF guidelines also say that VASPs should be monitored and scrutinized by a competent authority, while clearly mentioning that a self-reflection

report is unacceptable and non-standard. In the case of a decentralized scenario, it is unclear how parties would be held accountable, give that there is no centralized authority.

4) For cash couriers and wire transfers, FATF recommends a limit of USD 1,000. It is easy, using payment networks, for users to split large transactions into smaller amounts, and route each amount along a separate path using layer-2 protocols such as PR cash [121]. While structuring transactions is illegal, inability to enforce it has led to the practice of "cuckoo smurfing" [26].

5) FinCen and FATF regulations stipulate that if a business is acting as a money transmitter, there has to be an individual in the business who approves an AML program. The manner in which this guideline will be enforced in a decentralized scenario needs to be addressed. The difficulty in putting together an AML program in a decentralized scenario has been exploited by criminals to convert Bitcoin into fiat currency and selling people fake/non-existant goods [94].

6) The FinCEN *travel rule*, which governs international transactions above a certain threshold does not apply to unhosted (cold) wallets. It is unclear how to monitor transactions and enforce AML guidelines if a user tries to launder money using unhosted wallets, e.g., recently criminals have used unhosted wallets to pay kickbacks to each other [31, 103].

7) Standard AML procedures focus on laying down rules to prevent money laundering and financial crimes, but do not provide a framework for building a risk profile to identify people who might have the desire/motives to commit financial crimes. Identifying criminal intent before a financial crime is committed might help in preventing incidents where people with otherwise clean records are found to be involved in money laundering crimes [24, 29].

8) Finally, there seems to significant disparities between almost all systems proposed in the literature in the cryptocurrency/payment network space, and the regulatory guidelines of FATF and FinCEN. For example, both FinCen and FATF require a record of transactions to be maintained and made available to the concerned law enforcement agencies upon request; all known built systems that deal with protecting the privacy of the users do not maintain records of transactions. FATF and FinCEN also state that the sender and receiver names should not be stored in a pseudonymous format. Again, all the known system designed in the cryptocurrency asset and payment network literature violate this guideline. Most built systems also do not take into account AML thresholds. From our findings, this is not just a problem in the systems proposed in the academic literature, but also extends pervasively into the real world, e.g., various financial institutions have been fined heavily for failing to maintain records of customers and transactions, and thus failing to maintain an AML program [12, 23, 90, 120].

5 EXPERIMENTS

We conducted experiments to analyze the effect of different blacklisting policies, and to quantify the effect of tainting coins across a payment network. To this end, we used the transaction datasets provided by a popular payment network, Ripple [96], and extracted the complete transaction set from January 2019 to October 2019. Each individual record in the set includes the sender's public key, the receiver's public key, the amount exchanged as a result of the transaction, the time stamp, the unique identifier (digest) of the transaction, the currency unit used, and a unique marker field.

Table 1: Effect of blacklisting on bottom 100 USD transactions

Tx	Hop count	Poison Taint ($)	Haircut Min Taint ($)	Haircut Max Taint ($)
Tx-1	14	32521.597	0.0021	5000.000
Tx-2	14	32521.597	0.117	5000.000
Tx-3	10	6.005	0.0005	6.000
Tx-4	7	0.01	0.01	0.01
Tx-5	3	100006.343	0.012	60000.0
Tx-6	2	0.358	0.355	0.0032
Tx-7	1	3706746.51	0.01	350000.0

We wrote a Python script to parse this transaction set to extract paths and other details. The Ripple dataset consisted of around 4 million transactions at the time of writing this paper (for our chosen time period). The goal of our experiments is to demonstrate the maximum and minimum monetary effect of money laundering on the transaction sets in the Ripple network. For this purpose we have chosen the top 100 and bottom 100 transactions from the dataset. The top 100 transactions are mostly direct transactions, while the bottom 100 have paths of users between the sender and receiver.

We first extracted the raw sum of funds exchanged by all the accounts for each individual unit of currency in the transaction set. Next, we calculated the maximum amount sent as a result of one single transaction for each unit of currency, e.g., the maximum for Bitcoin represents the maximum number of BTC transmitted from a sender to a receiver as a result of a single transaction. Similarly, we calculated the minimum amount of money sent from a sender to a receiver as a result of one transaction for each unit of currency. We then extracted the sender account public key that sent the maximum and minimum amount of funds for each currency unit, the receiver account public key, and the number of times each account was involved in a transaction as sender or receiver. Finally, we calculated the number of times each currency was involved in a transaction.

Table 2: Effect of blacklisting on top 100 CNY transactions

Account	Tx(s) involved	Poison Taint (¥)	Haircut Min Taint (¥)	Haircut Max Taint (¥)
P_1	553	9024561.5	10.0	289784.0
P_2	525	13824057.0	6.0	1000000.0
P_3	484	123000.0	1.0	123000.0
P_4	211	4609327.0	100.0	400000.0
P_5	188	1748406.0	1.0	319681.0
P_6	153	8158048.66	1.0	702100.0

Using this data, we extracted the top ten currencies (we have found out that there were a total 153 different currencies) that were involved in the most number of transactions (by transaction count). Although the datasets contain transactions in various fiat currencies and cryptocurrencies, we have chosen USD and CNY for our experiments, since they are the two currencies that have recorded the highest amount of transactions.

Taint Calculation: Our experiments analyze the effect of the two most commonly used blacklisting policies, *Poison* and *Haircut* on the Ripple transaction data. The question we seek to answer by conducting our experiments is "what is the monetary loss that can be caused by a single coin being tainted across the transactions of the Ripple network?" We extracted the path taken to route the money from sender to receiver; the path can either proceed through several accounts of different currencies, or be "rippled" through a set of issuers for the same currency. For both cases, we have calculated the total number of accounts and issuers involved in the path, which is essentially the hop count for a given transaction. We then calculated the amount of funds lost when the two blacklisting policies were applied. For *Poison*, as mentioned earlier, the taint propagates through the entire network. Hence, we have calculated the sum total of amounts in which the account public key whose funds might be tainted was involved as the sender.

Table 3: Effect of blacklisting on bottom 100 CNY transactions

Tx	Hop count	Poison Taint (¥)	Haircut Min Taint (¥)	Haircut Max Taint (¥)
Tx-1	12	144700.850	0.001	52400.0
Tx-2	12	2135.634	0.0001	1900.0
Tx-3	11	2000.012	0.001	2000.000
Tx-4	6	5129.264	0.0001	740.894
Tx-5	3	3000.001	0.0001	300.000
Tx-6	2	0.0038	0.0038	0.0038
Tx-7	1	100647.661	0.01	99990.0

For the *Haircut* taint policy, we calculated the least and maximum amount of funds lost as a result of applying this policy. Since *Haircut* taints only the amounts pertaining to the individual transactions, we have extracted the least amount sent by an account in a single transaction (along multiple paths) to get the minimum value, and analogously for the maximum amount. Our results are tabulated in Table 1, Table 3, Table 4 and Table 2. Our results show that even a single illicit transaction can taint a significant number of coins in the payment network, and cause huge financial losses to users.

6 RECOMMENDATIONS

In this section, we propose recommendations which we believe, will aid in mitigating a few of the technical and regulatory challenges that were previously described.

1) *Blacklisting*: One way to approach cross-chain blacklisting is to design a mechanism that enables a user to prove that all the coins they possess are untainted, regardless of the number of times they were converted into various currencies. This would involve some cryptographic mechanisms such as either a zero knowledge proof whose witness is the conversion history of a given coin and the statement/claim to be proven is that the coin is taint-free, or timed cryptographic primitives such as verifiable delay functions [17] or verifiable timed signatures [112] could be explored.

Enforcing uniform blacklisting rules across the board globally is a tricky challenge but by far the most important. A good place to start is, of course, the FATF and the Financial Stability Board [41] at the global level, FinCEN guidelines in the United States, along with other comparable guidelines issued by different national bodies such as the Financial Transactions and Report Analysis (FINTRAC) of Canada [45], the Financial Conduct Authority (FCA) of the United Kingdom [40], the Financial Supervisory Authority of Germany [9], the Australian Prudential Regulation (APRA) [5], the Australian Securities and Investments Commission (ASIC) [6] and many more. There are several treaties in place too such as the Terrorist Financing Convention (1999) [114], the Vienna Convention, the Palermo Convention [85, 117], and the United Nations Security Council Resolution 2462 on countering terrorist financing [113]. These varied regulatory bodies need to come together to formulate a *common minimum criteria* (CMC) that distills the essence of all the regulatory guidelines prescribed up until now. Formulating a CMC is, we believe, relatively easier, than ensuring that it is enforced without fear or favor across various jurisdictions. A *semi-permissioned* blockchain would be useful for law enforcement to post their activities regarding AML enforcement. The blockchain should, obviously only be writable to by law enforcement authorities, but, for accountability and auditability purposes, should be publicly readable. In cases of non-compliance, global watchdogs should have the authority to impose sanctions or other financial costs.

2) *Payment networks*: The hard challenge in payment networks is checking for *structured* transactions (structuring of transactions refers to the process of breaking the total amount to be transmitted into smaller amount, and sending each amount along different paths to the receiver). Example of built systems that enable structuring include [18, 55, 57, 65, 71, 86, 87, 127, 128]. Dealing with structuring requires all stakeholders to accept that some degree of regulatory control is necessary for enforcing AML regulations. A decentralized, but an empowered group of authorities could check transactions originating from a pseudonymous identity, or trace or map multiple transactions made with multiple pseudonymous identities to the same user. This is a delicate problem and needs to be handled without infringing on users' privacy. The challenge here is to find the right balance between complete and conditional anonymity. Complete anonymity might enable money laundering, while conditional anonymity weakens user privacy. A user could be made to use a unique randomly generated string in all their transactions, embedded in all their pseudonymous identities, which could be traced to the said user, if necessary, and only to aid in ongoing investigations. This could be used in conjunction with regulatory enforcement to address the other issues in payment networks, i.e., taint checking of coins, preventing coins across the network from getting tainted, etc.

Table 4: Effect of blacklisting on top 100 USD transactions

Account	Tx(s) involved	Poison Taint ($)	Haircut Min Taint ($)	Haircut Max Taint ($)
P_1	4281	583830521.819	0.01	2895390.15
P_2	428	100020317.232	50.0	99998967.232
P_3	102	588000000.0	5000000	9000000.0
P_4	53	96619133.951	5727.58	14180000.0
P_5	51	104939979.479	24489.8	10000000.0
P_6	50	34977867.760	6122.45	4159575.19

3) *Change in mindset*: For the research community in this space, a change in mindset is required – rather than shun the idea of regulation, and automatic pushback against any kind of "regulatory interference", whether real or perceived, the research community must accept that we would need to rethink or even let go of some of the high privacy, anonymity, and decentralization guarantees we have come to expect from blockchain-based financial services if we want to make progress towards designing and implementing effective AML measures. We believe some degree of cryptocurrency asset regulation is required if we want a clean, trustworthy financial ecosystem that inspires confidence, deters criminal activities, and has the capability to enforce retributive measures when its tenets are violated.

7 CONCLUSION

In this paper we have outlined several practical challenges with implementing and enforcing AML mechanisms in cryptocurrencies and payment networks. Of the enormous research in the past few years that has been done on building systems that support and enable blockchain-enabled financial applications such as mixers and payment networks, to name two, there are hardly any systems that have AML mechanisms as part of their stated design goals. Retrofitting existing systems with something as fundamental as AML mechanisms and regulatory compliance is not easy, and goes against established principles of not adding security as an afterthought. In this paper, we have discussed the main aspects of current U.S. and FATF AML guidelines; analyzing the AML guidelines of other countries might be an interesting direction for future work.

Our findings indicate that no one solution can, in isolation, address the issue of money laundering. The only effective solution would be to build holistic, effective AML mechanisms for blockchain-enabled financial services, from *policy* and *technical* perspectives. The former involves building, from the ground up, systems that reflect and respect global and national AML regulatory guidelines, and the latter involves using techniques such as blacklisting and building risk-models of transactions and users. All of these approaches have several challenges that need to be addressed before they can be put to practical use. We hope that research in the coming years will address all these important challenges, and will yield systems that have built-in AML mechanisms in their system models and adversary models.

ACKNOWLEDGMENTS

Research supported by NSF award #1800088 and the Federal Aviation Administration (FAA). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the NSF and FAA.

REFERENCES

[1] Svetlana Abramova, Pascal Schöttle, and Rainer Böhme. 2017. Mixing Coins of Different Quality: A Game-Theoretic Approach. In *Financial Cryptography and Data Security*, Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y.A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, and Markus Jakobsson (Eds.). 280–297.
[2] Analysis tool 2019. https://www.chainalysis.com/.
[3] Ross Anderson. 2018. Making Bitcoin Legal (Transcript of Discussion). In *Security Protocols XXVI - 26th International Workshop, Cambridge, UK, March 19-21, 2018, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 11286)*, Vashek Matyás, Petr Svenda, Frank Stajano, Bruce Christianson, and Jonathan Anderson (Eds.). Springer, 254–265. https://doi.org/10.1007/978-3-030-03251-7_30
[4] Ross Anderson, Ilia Shumailov, Mansoor Ahmed, and Alessandro Rietmann. 2018. Bitcoin Redux. In *17th Annual Workshop on the Economics of Information Security*. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_38.pdf event-place: Innsbruck, Austria.
[5] APRA 1998. https://asic.gov.au/.
[6] ASIC 1998. https://asic.gov.au/.
[7] Lukas Aumayr, Esra Ceylan, Matteo Maffei, Pedro Moreno-Sanchez, Iosif Salem, and Stefan Schmid. 2020. Demand-Aware Payment Channel Networks. *arXiv preprint arXiv:2011.14341* (2020).
[8] Georgia Avarikioti, Eleftherios Kokoris Kogias, Roger Wattenhofer, and Dionysis Zindros. 2019. Brick: Asynchronous Payment Channels. *arXiv preprint arXiv:1905.11360* (2019).
[9] BAFIN 2002. https://www.bafin.de/EN/Homepage/homepage_node.html.
[10] Vivek Bagaria, Joachim Neu, and David Tse. 2020. Boomerang: redundancy improves latency and throughput in payment-channel networks. In *International Conference on Financial Cryptography and Data Security*. Springer, 304–324.
[11] Titu-Marius I BĂJENESCU. 2020. Libra: first international cryptocurrency. *Technical University of Moldova* (2020).
[12] Banamax scam [n.d.]. https://www.justice.gov/opa/pr/banamex-usa-agrees-forfeit-97-million-connection-bank-secrecy-act-violations.
[13] Bank Secrey Act [n.d.]. https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.
[14] Iddo Bentov, Yan Ji, Fan Zhang, Lorenz Breidenbach, Philip Daian, and Ari Juels. 2019. Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom). Association for Computing Machinery, New York, NY, USA, 1521–1538.
[15] Bitcoin 2009. https://bitcoin.org/bitcoin.pdf.
[16] Bitcoin ponzi scheme 2015. https://www.bloomberg.com/news/articles/2015-09-21/bitcoin-firm-chief-pleads-guilty-to-first-of-its-kind-ponzi-scam.
[17] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. 2018. Verifiable Delay Functions. In *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference (Lecture Notes in Computer Science)*, Hovav Shacham and Alexandra Boldyreva (Eds.). Springer, 757–788.
[18] Joseph Bonneau, Izaak Meckler, Vanishree Rao, and Evan Shapiro. 2020. Coda: Decentralized Cryptocurrency at Scale. *IACR Cryptol. ePrint Arch.* 2020 (2020), 352.
[19] California ML scam 2020. https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and.
[20] Dimitris Chatzopoulos, Mahdieh Ahmadi, Sokol Kosta, and Pan Hui. 2017. Flopcoin: A cryptocurrency for computation offloading. *IEEE transactions on Mobile Computing* 17, 5 (2017), 1062–1075.
[21] Chinese money laundering scam [n.d.]. https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.
[22] Cipher trace tool 2019. https://ciphertrace.com/.
[23] commerz bank scam [n.d.]. https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and.
[24] CostaRica scam 2020. https://www.justice.gov/opa/pr/american-darknet-vendor-and-costa-rican-pharmacist-charged-narcotics-and-money-laundering.
[25] Nicolas T. Courtois and Rebekah Mercer. 2017. Stealth Address and Key Management Techniques in Blockchain Systems. In *Proceedings of the 3rd International*

Conference on Information Systems Security and Privacy, ICISSP 2017, Porto, Portugal, February 19-21, 2017, Paolo Mori, Steven Furnell, and Olivier Camp (Eds.). SciTePress, 559–566. https://doi.org/10.5220/0006270005590566

[26] Cuckoo smurfing 2015. https://www.bbc.com/news/uk-scotland-tayside-central-34289919.

[27] Datasets 2019. https://www.kaggle.com/ellipticco/elliptic-data-set.

[28] DEA report 2020. https://www.theblockcrypto.com/linked/96962/crypto-atms-dea-report-money-laundering.

[29] DEA scam 2020. https://www.justice.gov/opa/pr/former-dea-agent-and-his-wife-plead-guilty-roles-scheme-divert-drug-proceeds-undercover-money.

[30] Christian Decker and Roger Wattenhofer. 2015. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *Proceedings of the 17th International Symposium on Stabilization, Safety, and Security of Distributed Systems - Volume 9212*. 3–8.

[31] Deep-web scam 2019. https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales.

[32] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. 2019. Perun: Virtual Payment Hubs over Cryptocurrencies. In *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*. IEEE, 106–123. https://doi.org/10.1109/SP.2019.00020

[33] Christoph Egger, Pedro Moreno-Sanchez, and Matteo Maffei. 2019. Atomic Multi-Channel Updates with Constant Collateral in Bitcoin-Compatible Payment-Channel Networks. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 801–815.

[34] Enes Erdin, Mumin Cebe, Kemal Akkaya, Eyuphan Bulut, and A. Selcuk Uluagac. 2021. A scalable private Bitcoin payment channel network with privacy guarantees. *J. Netw. Comput. Appl.* 180 (2021), 103021. https://doi.org/10.1016/j.jnca.2021.103021

[35] Huseyin Ergun, Mesut Razbonyali, Erdal Guvenoglu, and Can Razbonyali. 2020. Distributed Atomic Swap on Cryptocurrencies. *Computer Engineering and Intelligent Systems* 11, 4 (2020), 37–45.

[36] Muhammed F. Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph K. Liu, and Dongxi Liu. 2019. MatRiCT: Efficient, Scalable and Post-Quantum Blockchain Confidential Transactions Protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 567–584.

[37] ETH white paper 2013. https://ethereum.org/en/whitepaper/.

[38] Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bharva, Andrew Miller, and Pramod Viswanath. 2018. Dandelion++ Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees. *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 2, 2 (2018), 1–35.

[39] FATF guidelines 2012. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

[40] FCA guidelines 2002. https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing.

[41] Financial Stability Board 2009. https://www.fsb.org/.

[42] FinCen money 2021. https://www.fincen.gov/what-money-laundering.

[43] Adam S Fink. 2018. *Can cryptocurrency be audited to Bank Secrecy Act and anti-money laundering regulations and normalized in the United States*. Ph.D. Dissertation. Utica College.

[44] FINRA 2007. https://www.finra.org#/.

[45] Fintrac 2000. https://www.fintrac-canafe.gc.ca/intro-eng.

[46] Flare 2016. https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf.

[47] Gambling sites for bitcoin [n.d.]. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

[48] Daniel Genkin, Dimitrios Papadopoulos, and Charalampos Papamanthou. 2018. Privacy in decentralized cryptocurrencies. *Commun. ACM* 61, 6 (2018), 78–88.

[49] Graft white paper 2018. https://www.graft.network/wp-content/uploads/2018/10/Graft_White_Paper_3.0_October_2018.pdf.

[50] Matthew Green and Ian Miers. 2017. Bolt: Anonymous Payment Channels for Decentralized Currencies. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 473–489.

[51] M. Harrigan and C. Fretter. 2016. 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)*. 368–373. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0071

[52] Ethan Heilman, Leen Alshenibr, Foteini Baldimtsi, Alessandra Scafuro, and Sharon Goldberg. 2017. TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub. In *NDSS*.

[53] Zhengbing Hu, Ivan Dychka, Mykola Onai, and Yuri Zhykin. 2019. Blind payment protocol for payment channel networks. *International Journal of Computer Network and Information Security* 9, 6 (2019), 22–28.

[54] Todd Jacquez. 2016. *Cryptocurrency the new money laundering problem for banking, law enforcement, and the legal system*. Ph.D. Dissertation. Utica College.

[55] Christian Janze. 2017. Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets. In *23rd Americas Conference on Information Systems, AMCIS 2017, Boston, MA, USA, August 10-12, 2017*. Association for Information Systems, 2110–2120. http://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/2

[56] George Kappos, Haaroon Yousaf, Ania Piotrowska, Sanket Kanjalkar, Sergi Delgado-Segura, Andrew Miller, and Sarah Meiklejohn. 2020. An empirical analysis of privacy in the lightning network. *arXiv preprint arXiv:2003.12470* (2020).

[57] Rami Khalil and Arthur Gervais. 2017. Revive: Rebalancing Off-Blockchain Payment Networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu (Eds.). ACM, 439–453. https://doi.org/10.1145/3133956.3134033

[58] Rami Khalil, Alexei Zamyatin, Guillaume Felley, Pedro Moreno-Sanchez, and Arthur Gervais. 2018. Commit-chains: Secure, scalable off-chain payments. *Cryptology ePrint Archive, Report 2018/642* (2018).

[59] Russell W. F. Lai, Viktoria Ronge, Tim Ruffing, Dominique Schröder, Sri Aravinda Krishnan Thyagarajan, and Jiafan Wang. 2019. Omniring: Scaling Private Payments Without Trusted Setup. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, CCS 2019, London, UK, November 11-15, 2019*, Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz (Eds.). ACM, 31–48. https://doi.org/10.1145/3319535.3345655

[60] Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Sooel Son, and Seungwon Shin. 2019. Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. https://www.ndss-symposium.org/ndss-paper/cybercriminal-minds-an-investigative-study-of-cryptocurrency-abuses-in-the-dark-web/

[61] Peng Li, Toshiaki Miyazaki, and Wanlei Zhou. 2020. Secure balance planning of off-blockchain payment channel networks. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 1728–1737.

[62] Liberty reserve scam [n.d.]. https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

[63] Lightning [n.d.]. Lightning network. https://lightning.network/.

[64] Joshua Lind, Oded Naor, Ittay Eyal, Florian Kelbert, Emin Gün Sirer, and Peter Pietzuch. 2019. Teechain: A Secure Payment Network with Asynchronous Blockchain Access. In *Proceedings of the 27th ACM Symposium on Operating Systems Principles*. 63–79.

[65] Jian Liu, Wenting Li, Ghassan O Karame, and N Asokan. 2018. Toward fairness of cryptocurrency payments. *IEEE Security & Privacy* 16, 3 (2018), 81–89.

[66] Giulio Malavolta, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, and Srivatsan Ravi. 2017. Concurrency and privacy with payment-channel networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 455–471.

[67] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. 2019. Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. https://www.ndss-symposium.org/ndss-paper/anonymous-multi-hop-locks-for-blockchain-scalability-and-interoperability/

[68] Patrick McCorry, Malte Möser, Siamak Shahandashti, and Feng Hao. 2016. Towards Bitcoin Payment Networks. In *In Proceedings of Australasian Conference on Information Security and Privacy*. 57–76.

[69] Sarah Meiklejohn and Claudio Orlandi. 2015. Privacy-enhancing overlays in bitcoin. In *Financial Cryptography and Data Security*. 127–141.

[70] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. A Fistful of Bitcoins: Characterizing Payments among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*. 127–140.

[71] Suat Mercan, Enes Erdin, and Kemal Akkaya. 2020. Improving Transaction Success Rate via Smart Gateway Selection in Cryptocurrency Payment Channel Networks. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 1–3.

[72] Suat Mercan, Enes Erdin, and Kemal Akkaya. 2021. Improving transaction success rate in cryptocurrency payment channel networks. *Computer Communications* 166 (2021), 196–207.

[73] Andrew Miller, Iddo Bentov, Surya Bakshi, Ranjit Kumaresan, and Patrick McCorry. 2019. Sprites and State Channels: Payment Networks that Go Faster Than Lightning. In *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers*. 508–526.

[74] ML control act 1986. https://www.congress.gov/bill/99th-congress/house-bill/5077.

[75] Monero 2014. https://www.getmonero.org/.

[76] Money laundering stats 2020. https://www.aljazeera.com/economy/2021/2/11/cryptos-dirty-side-270-addresses-laundered-1-3bn-in-2020.

[77] Pedro Moreno-Sanchez, Arthur Blue, Duc V. Le, Sarang Noether, Brandon Goodell, and Aniket Kate. 2020. DLSAG: Non-interactive Refund Transactions for Interoperable Payment Channels in Monero. In *Financial Cryptography and Data Security*, Joseph Bonneau and Nadia Heninger (Eds.). Springer International Publishing, Cham, 325–345.

[78] Pedro Moreno-Sanchez, Tim Ruffing, and Aniket Kate. 2017. Pathshuffle: Credit mixing and anonymous payments for ripple. *Proceedings on Privacy Enhancing Technologies* 2017, 3 (2017), 110–129.

[79] Pedro Moreno-Sanchez, Muhammad Bilal Zafar, and Aniket Kate. 2016. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 436–453.

[80] Malte Möser and Rainer Böhme. 2017. Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques. In *2017 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2017, Paris, France, April 26-28, 2017*. IEEE, 32–41. https://doi.org/10.1109/EuroSPW.2017.48

[81] Malte Möser, Rainer Böhme, and Dominic Breuker. 2014. Towards risk scoring of Bitcoin transactions. In *International Conference on Financial Cryptography and Data Security*. Springer, 16–32.

[82] Malte Möser and Arvind Narayanan. 2019. *Effective cryptocurrency regulation through blacklisting*. Technical Report. Princeton University.

[83] Lalitha Muthu Subramanian, Roopa Vishwanathan, and Kartick Kolachala. 2020. Balance Transfers and Bailouts in Credit Networks using Blockchains. In *IEEE International Conference on Blockchains and Cryptocurrencies (ICBC)*. 1–3.

[84] OFAC blacklist 2021. https://www.treasury.gov/ofac/downloads/sdnlist.pdf.

[85] Palermo Convention 2000. https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

[86] Chen Pan, Shuyang Tang, Zhonghui Ge, Zhiqiang Liu, Yu Long, Zhen Liu, and Dawu Gu. 2019. Gnocchi: Multiplexed Payment Channels for Cryptocurrencies. In *International Conference on Network and System Security*. Springer, 488–503.

[87] Dmytro Piatkivskyi and Mariusz Nowostawski. 2018. Split payments in payment networks. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 67–75.

[88] QQAAZZ scam 2020. https://www.justice.gov/opa/pr/officials-announce-international-operation-targeting-transnational-criminal-organization.

[89] Quarterly report q3 2019 [n.d.]. https://ciphertrace.com/q3-2019-cryptocurrency-anti-money-laundering-report/.

[90] Rabobank scam 2018. https://www.justice.gov/usao-sdca/pr/bank-sentenced-obstructing-regulators-forfeits-368-million-concealing-anti-money.

[91] Raiden network 2017. https://raiden.network/.

[92] RAND report 2018. https://www.rand.org/pubs/monograph_reports/MR965.html.

[93] Fatemeh Rezaeibagha and Yi Mu. 2019. Efficient micropayment of cryptocurrency from Blockchains. *Comput. J.* 62, 4 (2019), 507–517.

[94] RICO scam 2020. https://www.justice.gov/usao-edky/pr/fifteen-defendants-plead-guilty-racketeering-conspiracy-international-cyber-fraud.

[95] Ripple Assesment 2015. https://www.fincen.gov/sites/default/files/shared/Ripple_Assessment.pdf.

[96] Ripple datasets 2019. https://github.com/ripple/rippled-historical-database.

[97] Romanian scam 2021. https://www.justice.gov/opa/pr/owner-bitcoin-exchange-sentenced-prison-money-laundering.

[98] Stefanie Roos, Pedro Moreno-Sanchez, Aniket Kate, and Ian Goldberg. 2018. Settling Payments Fast and Private: Efficient Decentralized Routing for Path-Based Transactions. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_09-3_Roos_paper.pdf

[99] Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate. 2017. P2P Mixing and Unlinkable Bitcoin Transactions. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*. The Internet Society. https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/p2p-mixing-and-unlinkable-bitcoin-transactions/

[100] Kyungho Ryu, Wooseong Kim, and Eun-Kyu Lee. 2020. payGo: Incentive-Comparable Payment Routing Based on Contract Theory. *IEEE Access* 8 (2020), 70095–70110.

[101] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *Proceedings of the 2014 IEEE Symposium on Security and Privacy*. 459–474.

[102] Evan Schwartz. 2016. A payment protocol of the web, for the web: Or, finally enabling web micropayments with the interledger protocol. In *Proceedings of the 25th International Conference Companion on World Wide Web*. 279–280.

[103] Serbian ML scam 2021. https://www.justice.gov/opa/pr/serbian-founder-digital-asset-companies-indicted-international-cryptocurrency-scheme.

[104] Savva Shanaev, Satish Sharma, Binam Ghimire, and Arina Shuraeva. 2019. Taming the Blockchain Beast? Regulatory Implications for the Cryptocurrency Market. *Research in International Business and Finance* 51 (08 2019), 101080. https://doi.org/10.1016/j.ribaf.2019.101080

[105] Omer Shlomovits and István András Seres. 2019. ShareLock: Mixing for Cryptocurrencies from Multiparty ECDSA. *IACR Cryptol. ePrint Arch.* 2019 (2019), 563.

[106] Side-chains white paper 2014. https://blockstream.com/sidechains.pdf.

[107] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Mohammad Alizadeh, Giulia Fanti, and Pramod Viswanath. 2018. Routing cryptocurrency with the spider network. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 29–35.

[108] Vibhaalakshmi Sivaraman, Shaileshh Bojja Venkatakrishnan, Kathleen Ruan, Parimarjan Negi, Lei Yang, Radhika Mittal, Giulia Fanti, and Mohammad Alizadeh. 2020. High throughput cryptocurrency routing in payment channel networks. In *17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20)*. 777–796.

[109] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. *IACR Cryptol. ePrint Arch.* 2016 (2016), 1159.

[110] Terrorism finance [n.d.]. https://www.justice.gov/opa/pr/lebanese-businessman-tied-treasury-department-hezbollah-pleads-guilty-money-laundering.

[111] Thailand scam [n.d.]. https://www.justice.gov/opa/pr/alleged-cryptocurrency-fraudster-extradited-thailand-face-charges-multi-million-dollar.

[112] Sri Aravinda Krishnan Thyagarajan, Adithya Bhat, Giulio Malavolta, Nico Döttling, Aniket Kate, and Dominique Schröder. 2020. Verifiable Timed Signatures Made Practical. In *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security*, Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna (Eds.). ACM, 1733–1750.

[113] UN resolution 2019. https://www.un.org/securitycouncil/content/sres24622019.

[114] UN treaty 1999. https://www.un.org/law/cod/finterr.htm.

[115] USA Patriot Act 2001. https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

[116] Sushil Mahavir Varma and Siva Theja Maguluri. 2019. Throughput optimal routing in blockchain based payment systems. *arXiv preprint arXiv:2001.05299* (2019).

[117] Vienna convention 1961. https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XXIII-1&chapter=23&Temp=mtdsg3&clang=_en.

[118] Peng Wang, Hong Xu, Xin Jin, and Tao Wang. 2019. Flash: efficient dynamic routing for offchain networks. In *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*. 370–381.

[119] Mark Weber, Giacomo Domeniconi, Jie Chen, Daniel Karl I. Weidele, Claudio Bellei, Tom Robinson, and Charles E. Leiserson. 2019. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. *CoRR* abs/1908.02591 (2019). arXiv:1908.02591 http://arxiv.org/abs/1908.02591

[120] Western Union scam 2017. https://www.justice.gov/opa/pr/western-union-admits-anti-money-laundering-and-consumer-fraud-violations-forfeits-586-million.

[121] Karl Wüst, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. 2019. PRCash: Fast, Private and Regulated Transactions for Digital Currencies. In *Financial Cryptography and Data Security - 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18-22, 2019, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 11598)*, Ian Goldberg and Tyler Moore (Eds.). Springer, 158–178.

[122] Shengmin Xu, Jiaming Yuan, Yingjiu Li, Ximeng Liu, and Yinghui Zhang. 2019. Super Payment Channel for Decentralized Cryptocurrencies. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 1–8.

[123] Ruozhou Yu, Guoliang Xue, Vishnu Teja Kilari, Dejun Yang, and Jian Tang. 2018. Coinexpress: A fast payment routing mechanism in blockchain-based payment channel networks. In *2018 27th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 1–9.

[124] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt. 2019. XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. In *2019 IEEE Symposium on Security and Privacy (SP)*. 193–210.

[125] Di Zhang, Junqing Le, Nankun Mu, and Xiaofeng Liao. 2018. An anonymous off-blockchain micropayments scheme for cryptocurrencies in the real world. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, 1 (2018), 32–42.

[126] Xiaoxue Zhang, Shouqian Shi, and Chen Qian. 2020. Scalable Decentralized Routing for Blockchain Payment Networks. In *Third International Symposium on Foundations and Applications of Blockchain 2020*.

[127] Yuhui Zhang and Dejun Yang. 2019. RobustPay: Robust payment routing protocol in blockchain-based payment channel networks. In *2019 IEEE 27th International Conference on Network Protocols (ICNP)*. IEEE, 1–4.

[128] Yuhui Zhang, Dejun Yang, and Guoliang Xue. 2019. Cheapay: An optimal algorithm for fee minimization in blockchain-based payment channel networks. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[129] Lin Zhong, Qianhong Wu, Jan Xie, Zhenyu Guan, and Bo Qin. 2019. A secure large-scale instant payment system based on blockchain. *Computers & Security* 84 (2019), 349–364.