Aldin Traljic - at3630
Sofia Calatrava - ac3643
Roy Rinberg - rr3426
Mikha Diaz - mvd2131

Privacy When Everyone is Watching

Privacy on the Blockchain in the Presence of KYC laws

IEOR4575 - Policy For Privacy Technology
Professor Rachel Cummings
Final Project
Fall 2021

Blockchain? Blockchain.

If you want to buy a coconut from the bodega, the bodega does not need to know how much money you have in your account – you swipe your credit card, the bank confirms to the bodega that you have the necessary $2.73, then it removes the appropriate value from your account, and moves it to the bodega's account. In order for you to be able to acquire a coconut, both you and the bodega must trust a central party to manage most of the transaction. To remove trust in this interaction, one would need to use cash or directly barter; both of these options are impossible in online transactions.

In 2008, the Bitcoin whitepaper was released which proposed a method to keep a publicly owned ledger that anyone could reference, in order to remove the need for a trusted third-party in a financial transaction [1]. The blockchain's core technology is based on generating *decentralized consensus* about an on-going list of transactions (note: this does not need to be financial transactions, but could be any digital interaction). The core goal of a blockchain is for many parties to maintain computers that all keep track of their own ledger, and the parties seek to actively align those ledgers.

Every node listens to all transactions being shared, then rebroadcasts the order of transactions that they have in their own ledger; nodes that are faithfully executing the blockchain protocol (also called *honest nodes*) will roughly take the history that the most other nodes agree on, to be the ledger that they should take as their own. Different blockchains have different *consensus protocols* for agreeing on history, but in general, this means that so long as at least 50% of the nodes are *honest* (or in some cases, at least 2/3rds are honest), we are able to achieve consensus and share a common ledger, without trusting any one major party. This allows people to come to a consensus even in the presence of malicious actors (usually referred to as Byzantine nodes), who are typically trying to convince other actors that they have more money than they do. [2]

Bitcoin applies these consensus protocols to keep track of a ledger of monetary transactions (of the in-chain currency Bitcoin), however, other cryptocurrencies like Ethereum have used the blockchain to do any kind of transaction: Ethereum allows for people to submit code to the blockchain (called smart-contracts), which can be thought as a tool to guarantee that some transaction will occur. [7]

What's the problem?

In the last 13 years, Bitcoin, and more importantly, blockchain technologies have changed the world; now the global crypto market cap is approximately $2.5 trillion dollars [3]. Still, despite its influence on the world, much of the blockchain is misunderstood. One of the biggest misunderstandings is around privacy, anonymization, and pseudonymization.

Removing centralization is an incredible engineering accomplishment, but it's important to understand the trade-off we have made: we remove the need for centralization by creating a public ledger that anyone with internet access can view. Different blockchains manage their ledgers differently, but in principle people own wallets (secured through cryptographic

techniques such as RSA), and are able to execute transactions with other users on the blockchain. Wallets are typically a randomly generated number, and typically are not tied to a personal identity. However, one of the most important concepts to understand with this, is that such blockchains do not offer anonymity, but rather pseudonymity : transactions cannot be directly linked to a single user, but all transactions initiating from a single wallet, can be tied to the same actor (or really, private key). As a cartoon example: if you commit a crime and are paid for it, and then use the money to buy a personal website with your name, you have not remained anonymous. [2]. Anonymity will be preserved only if the data cannot be linked to a physical identity; however, if your wallets are linked to your real identity, then all of the previous works under that pseudonym will be traced back to you and all anonymity will be lost.

Further, preventing institutions from learning wallet owners' identities is becoming increasingly difficult with the implementation of Know Your Customer (KYC) laws. KYC laws are ethical requirements within the investment and financial services industry [11]. KYC requires the verification of a customer's identity, to ensure that a customer is who she claims to be. The objective of KYC is to prevent illicit activities such as money laundering, financing terrorism, and tax evasion [12]. Typically, KYC requires that exchanges collect a customer's social security number, date of birth, physical address, and at times a government issued identification document such as a driver's license or a passport. [12] The level of transparency required by KYC, applied to cryptocurrencies, results in anyone from government agencies to hackers can track any financial transaction and discover the identity of the persons behind them [13].

There are existing techniques that attempt to provide anonymity guarantees. One is generating a new address for each transaction, but there are serious flaws behind this approach, as reading the blockchain history and looking over network traffic will lead back to the original address. An additional privacy concern is that the Bitcoin network is a peer-to-peer (P2P) network, exposing participants to network level attacks and the risk of the IP address being revealed by intermediaries such as ISPs. In an interview with Bloomberg, Lilita Infante, a member of the DEA's Cyber Investigate Task Force said that "the blockchain actually gives us a lot of tools to be able to identify people," and when asked about criminals, "I actually want them to keep using [cryptocurrencies]" [4].

Bitcoin's Privacy Guarantee

Pseudonymity

Bitcoin is believed to be anonymous because one does not need to use their real name to make transactions. However, Bitcoin is in fact pseudonymous since all transactions are associated with an address linkable to one's identity.

A cryptocurrency transaction begins, for instance, with a Bitcoin wallet – a software application that interfaces with the Bitcoin blockchain. It generates and stores users' addresses (cryptographic equivalent of a bank account number; essentially virtual locations to which cryptocurrency is sent/received) and private keys (cryptographic equivalent of a password, in which a Bitcoin address can only be accessed by a unique corresponding private key). While one does not use their actual name to make Bitcoin transactions, they instead use Bitcoin

addresses (pseudo-identities) to interact with the system. This pseudonymity is inadequate to protect users' privacy, especially as Bitcoin utilizes a public block chain that enables one to look up all transactions associated with any given address. If someone is ever able to link a Bitcoin address with one's real world identity, then all their past, present, and future Bitcoin transactions can be linked back to their real world identity [28].

It is also not difficult to establish a link between a Bitcoin address and a real-world identity. For example if you buy a cookie from a cafe and pay with Bitcoin, while you would not need to reveal your real name, your physical identity gets tied to the Bitcoin transaction, consequently making all other transactions involved to the address used linkable to you. If you purchase from an online shop that accepts Bitcoin as payment, the merchant will need your shipping address or contact information. If you purchase cryptocurrency through an exchange like Coinbase or Binance, they will need your credit card or bank account details. As all this information could be linked back to your personal identity (e.g. through other public datasets, social media, side channels, or indirect leakages of information), we demonstrate that Bitcoin offers minimal privacy guarantee to users [28].

De-anonymization Theory

In this section, we consider how Bitcoin could be de-anonymized through shared spending, transaction graph analysis, and network-layer deanonymization.

Generally, since all Bitcoin transactions are recorded in a public ledger, a combination of several different input transactions into a single transaction could provide evidence of joint control to the public. These transactions are permanently recorded in the blockchain, where it could potentially be deduced that these input addresses are under the control of one user. For instance, if two Bitcoin payments (inputs) are used to purchase a book (output), one can infer that the transactions are likely controlled by the same user. Further, beyond just linking two, three, or more different addresses to a certain transaction, this can be extended transitively as well where any movement of Bitcoin in other transactions to new addresses (e.g. not just the book that was purchased with one of the inputs, but also coffee bought with such in another cafe) can be linked back to a user. This hence shows that shared spending demonstrates joint control, where one's transactions can all be linked together [10].

In "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" by Meiklejohn et al. (2013), the UCSD researchers employed a transaction graph analysis to de-anonymize Bitcoin transactions. To reliably infer addresses as owned by particular identities, the researchers transacted with various service providers through purchasing items with BTC, using Bitcoin exchanges, utilizing gambling sites and wallet services, etc. When there is an exchange of BTC either by buying from or selling to a service provider, the researchers are able to ascertain one Bitcoin address that that merchant owns. These addresses then end up searchable on the Bitcoin public ledger, and all transactions associated with the merchant's address could now be linked to their identity. In Figure 2 below, the analysis conducted by above researchers is illustrated, compromising 344 transactions and attaching real world identities to sets of Bitcoin transactions.

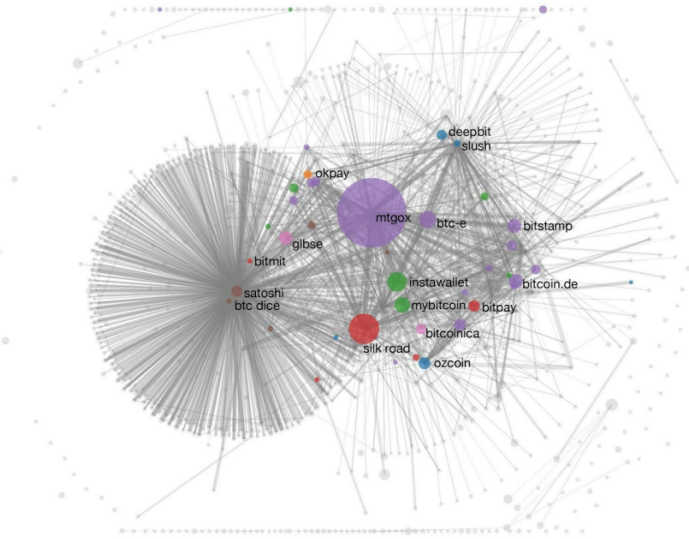

Figure 1. Labeled transaction graph analysis [29]

Lastly, Bitcoin transactions could also be deanonymized through P2P network-layer deanonymization. When a node (computer) broadcasts or creates a Bitcoin transaction, it connects to many nodes at once and broadcasts the transaction to peers in the network. Given sufficiently many nodes on the network, they could cooperate to identify the first node to broadcast the transaction with a consensus, presumably the source of the transaction. The transaction could then be linked to the node's IP address, in which there exists numerous ways to unmask a person's identity behind an IP address, posing another threat to Bitcoin's privacy [28].

Figure 2. P2P network-layer deanonymization [28]

Colonial Pipeline Ransomware Attack

Red flags regarding the privacy issues behind the de-anonymization of cryptocurrency transactions have been highlighted in theory, but these issues are not strictly hypothetical. While some cryptocurrencies like ZCash and Monero have cryptographic tools to preserve privacy, blockchains like Bitcoin have nothing directly protecting the privacy of its users. Here we see an example case of how Bitcoin does not offer privacy guarantees, only a thin layer of anonymity. Qualified blockchain investigators can in fact identify people behind Bitcoin transactions with relative ease and using only publicly available information and tools.

On May 7, 2021, Colonial Pipeline's billing system suffered a ransomware cyberattack.[1] They are the largest fuel pipeline in the US, supplying approximately 45% of the East Coast's fuel, including gasoline, diesel, home heating oil, jet fuel, and military supplies [2]. In response to the cyberattack, they halted all operations as precaution from hackers carrying out further attacks potentially on vulnerable parts of the pipeline. In Colonial Pipeline's 57-year history, this was the first time they had to shut down operations of its whole gasoline pipeline system. This led to fuel shortages and record-spike in fuel prices across the East Coast [4].

Service resumed on May 12, 2021. Colonial Pipeline, with the assistance of the FBI, paid 75 BTC (about $4.4 million) as ransom payment. They identified the hackers as affiliates of the Russia-linked criminal cybercrime group DarkSide. On June 7, a month later, the Department of Justice (DOJ) reported successful recovery of 63.7 BTC (about $2.3 million) from the ransom. This spurred valuable dialogue and numerous headlines that in fact, cryptocurrencies such as Bitcoin "are not as hard to track as it might seem" [5]. This led to large downsized moves for the cryptocurrency market [10].

Bitcoin has been commonly perceived as an "anonymous payment network" where transactions may be conducted unregulated and outside the traditional financial system [9]. As such, criminals "flocked to Bitcoin to do illicit business without revealing their names or locations" [8].

Court documents on the Colonial Pipeline cyberattack indicated that Bitcoin transaction records were traced to a digital Bitcoin wallet where the ransom money was delivered, which was seized under court order.

Colonial Pipeline advised the FBI of the Bitcoin address that they were instructed to send the ransom payment to. Because of the public nature of the Bitcoin ledger, officials were able to connect the criminals to their digital cryptocurrency wallet. Upon review of the Bitcoin public ledger, the FBI found that the ransom payment address received two payments on May 8, 2021 (when Colonial paid the hackers) totaling 75 BTC. Using a Blockchain explorer, an online tool that operates as a blockchain search engine which "allows users to review/search transactional data for any addresses on a particular blockchain," officials were able to collect the addresses where the ransom payment was ultimately transferred and distributed [5]. Then, the FBI was

[1] Ransomware is a "form of malicious software that infects a computer system and restricts access of files contained therein through encryption. By encrypting files on the system, they are made unreadable and unusable until the encryption is reversed, or the information is decrypted" [8].

able to gain possession of the private key to the address which had the majority of the ransom, successfully recovering 63.7 BTC [9].

April Falcon Doss, executive director of the Institute for Technology Law and Policy at Georgetown Law, said that the DarkSide hackers were “overly confident that the money couldn't be traced and that their private key was secure” [9].

Tuan Phan, founder of Zero Friction LLC, authored a paper that reconstructs the FBI’s recovery process using only publicly available information and tools. This demonstrates that Bitcoin transactions can be recovered using a money flow analysis, as was done by the FBI and supported with a seizure warrant [5].

Transaction Hash	Description
6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2	Ransom payment (Item #1)
915fb4f0a030937f2c1d2210996e8eb32b5a41b331965c7ec78961923775bd62	Intermediate #1
fc78327d4e46dac01dc313067b1ac7f274cdb3a07ea9f28f6f71473145f1b264	Intermediate #2
0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7	Intermediate #3
9436dbf0435b15378f309c35754a110db880fa9bb66a062160a25533bb4a212a	Intermediate #4
daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9	Sent to Subject Address (Item #3)
943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a	Sent to FBI ‘s Holding Address (Item #4)

Figure 3: Transactions from the Colonial Pipeline ransomware payment tracking operation [6]

The author started with a query to search the Bitcoin network for all addresses that partially match the partial address provided by the FBI, as can also be done with Ethereum. Immediately, the query returned only one output and the author was able to conclude with a high degree of certainty that the result was the subject address in question. Then, using a Bitcoin explorer, the author found that three transactions belonged to this address, with two being sent and one, the earliest, received. Following the transaction pattern and the money flow, the author was able to produce the transaction hash list. In fact, we tried our hand at following the money flow and finding the final retrieval of 63.7 BTC of the ransom payment and were successful. As stated, the FBI was not able to retrieve the full amount because not all of it was transferred to one account, as can be seen by the transaction hash list and the money flow chart below. Specifically, the transaction hash: 0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7 is the key, as of the 75 BTC sent as a ransom payment, the receiving address, bc1qxu83k5qkj8kcqdqqenwzn7khcw4llfykeqwg45, received only 63.7 BTC. Since DarkSide is a ransomware as a service organization, affiliates pay the service for the use of the ransom tools.

Therefore the payment of 63.7 BTC is likely the fees to the affiliate, and the remaining balance is likely the share for the DarkSide developer.

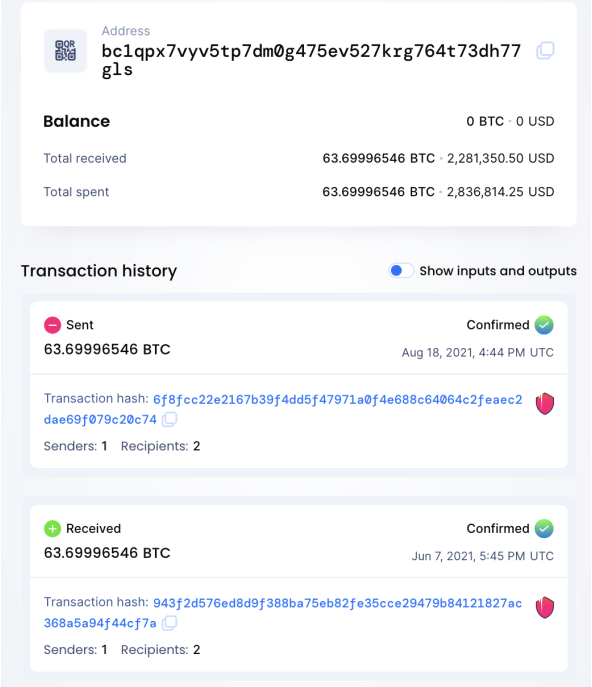

Figure 4: Address the FBI retrieved money from [6]

One of the more technical details behind the FBI's seizure of funds was obtaining the private keys for the subject addresses, but with Bitcoin there is an approach for this as well. Not much is known, or perhaps can be disclosed, about the FBI's specific technique, but it evolves around clustering timestamp and transaction details. On a general level, it is postulated that it is possible to obtain the IP addresses for all Bitcoin nodes by scanning the internet for every host with the port in question. Once known, access can be gained to the host that holds the private keys by monitoring in real time the address and thereby identifying the IP address that first transmitted the transaction of interest [6].

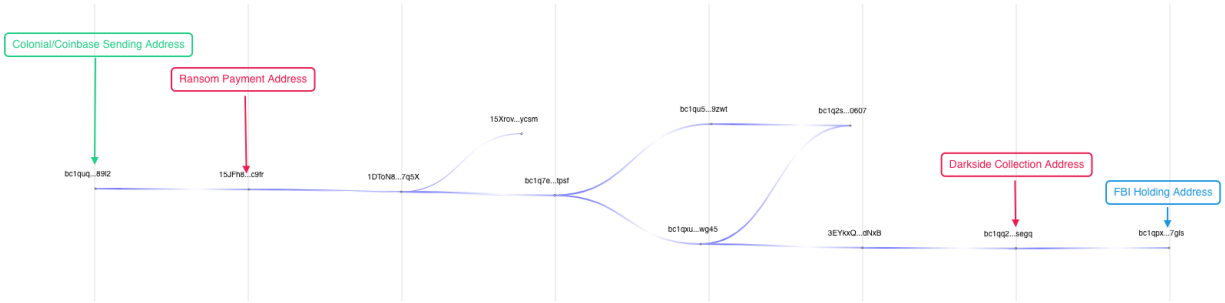

Figure 5: Graph of the flow of money from Colonial Pipeline ransomware payment [6]

There are serious privacy issues on the blockchain, as is abundantly clear from this case, and action needs to be taken immediately. Certain privacy aware individuals are moving ahead of others in identifying this problem and developing particular privacy aware solutions that do currently exist and will be defined in the following sections. These solutions include Anonymizers, Tumblers (a.k.a coin mixers), Stealth Addresses, and Ring Addresses, privacy-aware coins such as Z-cash and Monero, and smart contracts (defined later), however they alone cannot answer all of the concerns present, especially not without the added context of cryptocurrency regulations and KYC laws.

The objectives of KYC laws, deanonymization and traceability of financial transactions are in direct opposition to the goals of tools like privacy-aware coins and the technologies they employ. KYC regulations are also partly responsible for why privacy enabling cryptocurrencies have remained in the shadows of digital finance. In the following sections we will explore the regulations around general cryptocurrency and privacy-aware coins, like KYC, and the implications they have on finance, as well as some of the problems we have identified.

General information on cryptocurrency regulations

There are increasing financial regulations on cryptocurrencies, about what organizations can do. The fundamentally decentralized nature of blockchain and cryptocurrency technologies have led to a patchwork of regulations in different parts of the globe. In the United States, for example, no clear regulatory framework has been implemented, though in September of 2021, the Treasury department announced that it was in the process of making a push for clear regulation. The current level of clarity around cryptocurrencies in the US is made evident by its differering classification in different governmental entities. The US Treasury Department classifies cryptocurrency as a currency, the Securities and Exchange Commission (SEC) as a security, the Commodity Futures Trading Commission (CFTC) as a commodity, and the Internal Revenue Service (IRS) as a property for federal income tax purposes. [14]

For the first several years of early blockchain development, cryptocurrencies governments largely kept away from the market, seemingly letting it fall to the regulations of the *invisible hand of the market*. But as the market for digital currencies has grown so have the potential risks for consumers and financial markets, drawing the attention of regulators. The calls to action have fallen on the back of tremendous profits being made by firms investing in cryptocurrencies, and fears of cryptocurrency destabilizing the world's financial markets and becoming a gateway for massive criminal activities and hiding of assets due in part to the opaque nature of some the nature of some of the most elusive players on the market, privacy-aware coins. [15]

The first push for regulation is more concerned with stablecoins, a type of digital currency that is pegged to well-established traditional currencies like the Euro and USD. First introduced in 2015, stablecoins currently hold a market share worth $120 Billion USD. However, contrary to what its name implies, a 2021 report by the Federal Reserve and The Treasury states that stablecoins pose a risk of causing bank runs and a subsequent financial crisis similar to 2008.[16]

How do Regulations and “Privacy-Coins” Conflict?

Though stablecoins have garnered a fair amount of recent attention on the part of regulators, privacy-aware coins have also been a tenuous topic of conversation. Unlike other more transparent currencies like Bitcoin, privacy-aware coins, like Zcash, Monero, Beam, Dash, and Zcoin, trade transparency in favor of privacy. Privacy-aware coins operate using anonymous peer-to-peer decentralized systems.[13] Privacy-aware coins have two major focuses. The first is anonymity, hiding the identities of people behind transactions. The second is on untraceability, making it difficult or impossible to *follow the money.*[17] In addition to privacy-aware coins, other adjacency cryptocurrency services exist that can be used to obfuscate digital transactions and increase anonymity.

Examples of these features include Coin Mixers, Ring Addresses, Stealth Addresses, and ZK-SNARKS.[17] A Coin Mixer first combines multiple transactions to make a single transaction, and then divides the transaction back up before sending the correct amount to each recipient. A Ring Address connects multiple digital wallets to each other. When one of these wallets makes a transaction, an observer cannot tell which of the wallets in the *ring* made the transaction. Monero is one privacy-aware coin that applies this technique. A Stealth Address is a method of generating a new address for every transaction. Monero also incorporates this into their transactions in the form of a *dual-key stealth address protocol*. This protocol requires two cryptographic keys, a “scan key” and a “spend key”, to create a new address. A Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, or zk-SNARK for short, allows the blockchain to prove that a transaction is valid without requiring either party to identify themselves.[17]

privacy-aware coins and related services are the reason for growing fear around the enablement of criminal activity. Regulators have argued that privacy-aware coins provide a way to finance illegal operations, terrorism, sustain money laundering since individuals engaging in those activities are able to operate in disguise. Advocates argue that privacy-aware coins are essential to individuals who make legal transactions and simply want or require their activities to remain private, and that sweeping regulation infringe upon individual right to privacy, and destroy a necessary sanctuary.[17]

As with virtually all cryptocurrencies, regulation around privacy-aware coins varies from country to country. South Korea and Japan have banned them. The United States has kept their use legal, while the Department of Homeland Security (DHS) has called for creating backdoor methods to retrieve and exploit information hidden by those coins. Additionally, with the help of regulators, most US exchanges have unlisted privacy-aware coins from their platforms. The main argument behind for blacklisting privacy-aware coins from exchanges is that the certains laws such as Anti Money Laundering (AML), Combatting the Finance of Terrorism (CFT), and Know-Your-Customer (KYC) require currency exchanges to collect certain identifying information that is made made more difficult or impossible by privacycoins. The repercussions of violating any of these existing laws disincentivize exchanges from allowing privacy-aware coins onto their platforms.[17]

KYC Considerations

The requirements of transparency attached to already existing financial regulations seem to conflict with the philosophy behind and the implementation of privacy-aware coins. An impasse has been reached between institutions who demand control and surveillance over the flow of currency, and groups who refute regulation in favor of privacy. However, we argue that most of these issues only appear to be in conflict, and in reality, more stringent KYC laws are tools by law enforcement and banks to increase the centralization of power, **not** to protect the security and privacy of citizens.

Strains on financial markets and an influx of socio-political issues have caused an increase in attention by governments on KYC laws. Primarily they have two ostensible goals 1. Identify financial assets for the purpose of taxation, and 2. Track payments across digital markets for the purpose of tracking down criminal behavior (As DeepThroat *indirectly* told the US public, “follow the money” [18]).

Because of these interests, policies that promote strong KYC laws tend to come from organizations that either deal with securities and taxes, like the Securities and Exchanges Commission (SEC) and IRS, or money laundering like the Financial Action Task Force (FATF) on an international level, or the US department of Treasury’s Financial Crimes Enforcement Network (FinCEN). Recent guidance from FATF, FinCEN, and the US infrastructure bill [19] all have elements that are generally incompatible with decentralized finance and financial transactions (and wallets) outside of a third-party financial system [20].

However, overly strong KYC laws are actually quite dangerous for the privacy and security of most people. Additionally, they reinforce the centralizing economic trends of oligopolies and monopolies, by requiring the centralization of data and with limited access to that data. In this section we first describe how strong KYC laws can be damaging; then we look at what KYC laws actually promise, and consider two cases:

1. *If it were 1984:* If KYC laws are incredibly strict, what kinds of technical tools and Decentralized Finance (DeFi) environment can technologists develop to help protect the security and privacy of people
2. *If we were emperors*: If we had total control of KYC laws, what recommendations would we make; and what recommendations do we have on the technical development aspects.

For the point of the rest of our explorations we view the financial markets as having 3 regions: 1. The “real” world, 2. The blockchain world, and 3. Exchanges. Here’s a small diagram representing this ecosystem.

How does money enter and leave the cryptocurrency world?

For most coins, there is only one way to generate new coins : through cryptocurrency mining, which can be thought of as a provably scarce method for producing coins at a given

rate. This means that there are only two ways to acquire a cryptocurrency : either to mine, or to trade with someone who already has one.

This means that if you have USD and you wish to acquire Bitcoin, there are 3 possible ways to do it : 1. Acquiring a mining rig, and mine for Bitcoin, 2. Submitting a transaction on an exchange, 3. Making a transaction with someone in person, handing them a physical or digital good, and then them giving you bitcoin (either physically giving control of a wallet, or submitting a transaction on the blockchain). The diagram below gives a cartoon example of the space of types of transactions.

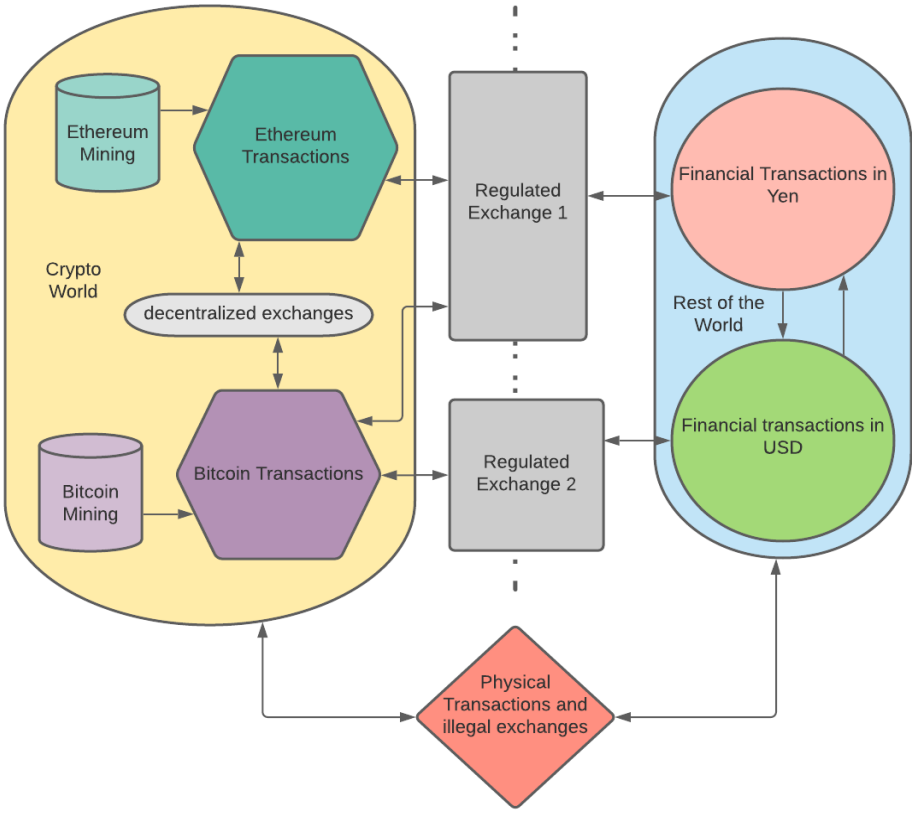

Figure 6: The space of financial transactions[2]

Bitcoin mining is complicated and concerns itself more with the intricacies of running a business, than purely making a financial transaction, so this paper won't focus on this. The regulatory consequences of methods 2 and 3 will be discussed below.

KYC Goal 1 : Accounting for taxes.

One of the main goals of KYC rules is to enable financial organizations to accurately account assets, and report them to tax agencies, like the IRS. We dismiss this claim as a

[2] Figure 6: Chart created on Lucid.app

serious issue because we observe that cryptocurrencies actually do not provide any new issues that didn't exist before. In the current non-blockchain world, we have 2 forms of currency, online currency (e.g. credit cards) and cash. If someone wants to live their life entirely in cash, they can - paying taxes will be inconvenient for them, but they can do it. And outside of the extremely inefficient solution of tracking specific dollar bills, it will be quite hard to track if they are paying the right amount of taxes. However, legal businesses are incentivized under penalty of law to file their taxes correctly, and most people do this.

We note that one notable difference between cash and cryptocurrencies is the scale of transactions : cryptocurrencies enable speed and scale to transactions that simply are not possible with cash. However, this does not matter for accounting for taxes - the only component that contributes to taxes is the total assets held. If someone acquires coins through method 2 (a transaction on the exchange), the assets are fully logged with the IRS and tax-collection authorities. If someone acquires the transactions through method 3 (an off-exchange transaction), this requires an exchange of money from a bank account, physical goods, or cash; IRS and law enforcement already has methods for tracking all three of these sources of money (especially money from a bank account).

The introduction of cryptocurrencies does not introduce new tax evasion methods. Using privacy-preserving cryptocurrencies rather than cash, changes nothing from an accounting for assets perspective. It's illegal to lie about your finances, but it's obviously possible to do.

KYC Goal 2 : tracking criminals. An analogy: immigration

The second major reason for KYC we have found is in order to identify and track criminal activity, and so, much of KYC legislature is expressed under AML (Anti-Money Laundering) laws. Similar to the original arguments against privacy-aware coins for the purpose of preventing tax evasion, we observe that cryptocurrencies do not introduce anything into the market that did not exist previously; instead, overly strict KYC laws are tools for law enforcement and centralized agencies to seize more control.

We observe that the same issues that we have in immigration are actually the same issues that blockchains have. In theory, every person who enters a country's border is documented; this means if a human does something suspicious, law enforcement can point at that person and find whatever documentation exists. This documentation occurs on entry (either into the borders of the country or into the world, by being born). If the system worked perfectly a person would commit a crime, that crime would be tied to the human body that did the crime, and the name of that body would be searchable. Border control and customs works really effectively because we force each person to be responsible for what they bring in and out of the country, regardless of how they got it. KYC in a minimal form would be in this format.

Strict KYC laws that require financial organizations to be able to account for where money comes are the equivalent of requiring shop owners to know where their customers got their money : in theory it would identify financial crimes, but at a complete loss of personal and corporate privacy. Requiring that all transactions be non-private is **not** how law enforcement currently works; and giving governments (and subsequently everyone) a view into all financial

transactions would be a gross reach for power. Until we live in a significantly more just society (which is debatably even possible), enabling governments to do this will invade privacy and erode democratic values.

How can KYC laws be damaging:

On December 23, 2020, FinCEN put out a proposed rule “Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets,” which seeks to put increased requirements on what transaction information is required to be stored by money services businesses and banks, under the Anti-Money Laundering Act of 2020. [21] Many cryptographers and proponents of decentralized systems have put out comments against this proposed rule.

Dr. Mathew Green and Dr. Eran Tromer, a Columbia professor and co-founder of ZCash, put out comments, claiming serious issues with the proposed rule: First, they cite **Security and economic risks to individuals**, as “Even minor data leaks can cause disproportionate privacy harm to customers: this is due to the fact that even a small amount of wallet identifying data can often be combined with public ledger data in order to recover a user’s entire transaction history.” They also identify that this rule **Imposes Excessive Information Security Costs on Small Entities**, and relatedly is harmful to innovation in the cryptocurrency space.” Lastly, they mention a point similar to our previous anti-KYC arguments, that strict KYC requirements are **Ineffective and trivial to circumvent** (for well-resources criminals), as “nefarious parties, such as those engaged in crime, tax evasion or terrorism, would easily circumvent such requirements by relaying their transactions with third parties through their own unhosted wallet. From the perspective of the bank or MSB, only the customer’s own wallet would be involved in the visible transactions, and thus the rule would not be applicable. Regulators’ visibility is thereby decreased, rather than increased.” [22]

What if it were 1984?

We posit a world where preventing anti-money laundering and tracking financial crimes is governments’ top concern, and KYC laws dominate cryptocurrencies. An extremely strict KYC law would require exchanges to only accept transactions if they knew where the money came from, under severe penalty by law enforcement. In theory, this would only put a regulatory pressure on the “on/off” ramps in and out of the blockchain; however, if the exchanges are required to know where the money came from, they would require the parties that seek to take money out of the blockchain network to be able to fully explain where each transaction came from. This would create two forces: 1. This would minimize the amount that people seek to enter/leave the blockchain (if you can live your whole life on the blockchain, KYC laws have no authority over you). 2. This would create an increasingly transparent, non-private financial world.

We think this world is unlikely, because most governments typically succumb to corporate interests, and if every time Apple paid a VR company any amount of money, the whole world knew, corporate secrets would scarcely exist.

If we take strong KYC laws as a premise, the necessity of corporate secrets for capitalism to be successful leads us to think that either blockchains will cease to exist or more services will live entirely on the blockchain. If KYC laws were extremely strict, and we saw an increase in power of centralized governments (like China), KYC laws may end up dramatically reducing the legitimacy and quantity of cryptocurrencies.

However, such an endeavor by the world's governments would be an uphill battle as the world's GDP is ~80 Trillion dollars [23], and cryptocurrencies are ~2.5 Trillion dollars [3], or in other words at least ~ 3% of the worlds' wealth is held within cryptocurrencies (but likely much more, due to the presence of smart-contracts, whose value are not directly measurable). We see good reason to believe that cryptocurrencies are not going anywhere, as they provide genuine value to people, and so conclude that in the presence of strong KYC laws, more services will exist entirely on the blockchain, and specifically, blockchains which as privacy-aware in some relatively strong capacity. This would directly counteract the original goals of the strict KYC laws, and so we do not recommend governments apply incredibly stringent KYC laws.

What if we were emperors? What would be our proposal?

The impossibility of the stated task:

In physics, "Maxwell's Demon" is a thought experiment that theoretically violates the second law of thermodynamics. The second law of thermodynamics states that entropy cannot decrease - informally, this means the global amount of disorder in a system can never decrease. In this thought experiment, a demon could allow cold particles into a chamber through its gate one way, and hot particles through the other, thereby decreasing the total entropy of the system, by taking a well-mixed arrangement, and putting it into a more organized (and less likely) orientation.

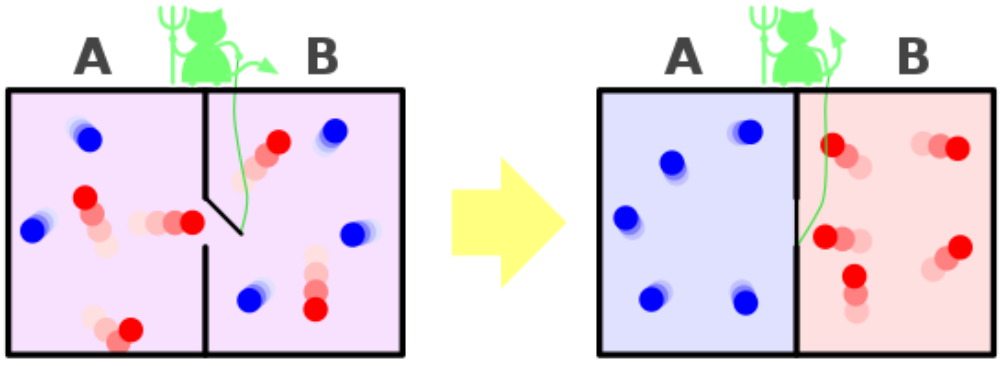

Figure 7: Maxwell's demon [24]

This promise of reversing entropy is critical, and could provide technological solutions to nearly every kind of problem, including the eventual heat death of the universe. [25] Maxwell's demon was proposed in 1867, and year after year, it is shown that Maxwell's demon could not know which particle belongs where and direct them accordingly. Similar to good-samaritans and

criminals, it remains impossible to differentiate cold and hot particles, without expending proportional amounts of energy to investigate their identity.

Similarly, since the 1960s law enforcement has been fighting to have increased centralized power to audit and monitor its people in order to “catch the bad guys”, while cryptographers have been fighting to have increased privacy and security. These legal, technological, and moral debates have been lovingly termed the CryptoWars. [26] We observe that without perfect knowledge of a person, it is impossible to only let the “right” people have privacy; the same way that it is impossible to let Maxwell’s Demon violate the second law of thermodynamics by selectively letting some particles through one way and others another. [24]

Our policy proposal

We first observe that this issue is not cut-and-dry, but remains an ethical consideration. Unless every transaction can be investigated, criminals will be able to thrive in the shadows; at the same time, if every transaction is public, personal and corporate privacy is profoundly breached. Outside of these two extremes, we suggest living in a world of grey, and regulators’ job is not to prevent all crime, but rather to make it difficult enough that most people won’t do it.

We propose a variant of what Goodell and Aste call “Institutionally Supported Privacy Enabling Cryptocurrency” , which seeks to achieve “the benefits of government regulation without creating a central database that irreversibly connects all persons with all their transactions.” [30] We propose that KYC apply relatively strictly to the people who interact with exchanges. Taking money in and out of the blockchain requires a similar degree of financial information that trading on the stock exchange does. However, we explicitly recommend these KYC laws do not extend very deep into the blockchain (see figure below for a diagram of what depth means). We propose a constraint on the reach of KYC, such that KYC information is only required for transactions that directly deal with an exchange, or are 1 step removed. We observe that if we require KYC for the n transactions that lead to/from an exchange, then any motivated party could easily make n+1 transactions with dummy-wallets that they own, and go from a non-anonymous setting to an anonymous setting. This means that to stop all financial crimes, we would need to have an entirely non-private blockchain.

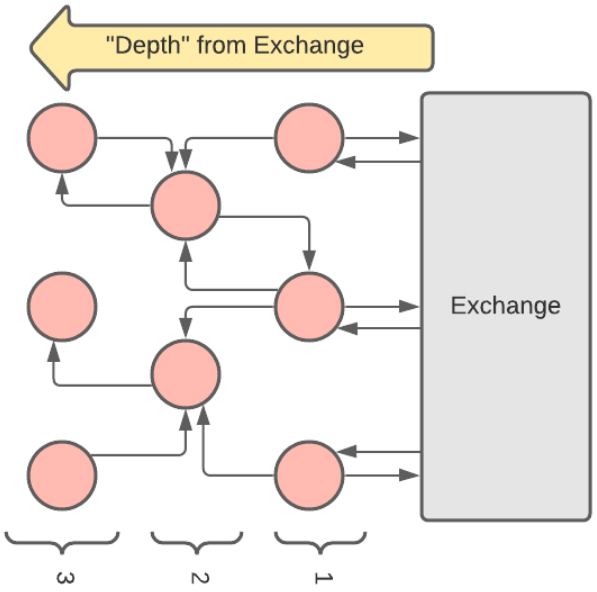

Figure 8: diagram showing depth from the exchange, for the purpose of KYC restrictions.[3]

Again, we state that an entirely non-private blockchain is highly unlikely. If every time Apple paid a VR company, the whole world knew, corporate secrets would scarcely exist; powerful forces at Wall Street and Silicon Valley would issue a financial revolt, if you had to "tweet" every transaction. As discussed in our *What if it was 1984* section, demanding privacy-breaches all the way through the blockchain would likely be counterproductive.

To prevent requiring that all transactions with exchanges be entirely public, we propose that increased development of privacy-aware coins, and in particular ZK-SNARK technology is promoted. In particular, ZK-SNARK with emphasis on "selective disclosure". Exchanges would be regulated entities, and would enforce KYC laws that require users to register their personal information, the way that people do to trade on financial exchanges. Privacy-aware coins would dominate the majority of the crypto market capitalization, and those privacy-aware coins would be ZK-SNARK based, with selective disclosure built into them, and mandated for the one or two transactions that extend to or from an exchange.

ZK-SNARKs (Zero-Knowledge Succinct Non-interactive ARguments of Knowledge)

ZK-SNARKs are a marvel of cryptography. ZK-SNARKs are a short proof that proves that something is true, without letting anyone know what that is. Nearly all (if not all) privacy-aware coins and cryptocurrency tumblers are based on ZK-SNARK technology, where rather than revealing someone's entire account balance to prove that someone has enough money to cover a transaction (as bitcoin and ethereum work), someone computes a ZK-SNARK

[3] Figure 8: Diagram made on Lucid.app

that is a proof that they have enough money in their account, without actually showing anyone their actual account and account balances.

A next step to pursue is the expansion and implementation of selective disclosure, a mathematical tool that can be added onto ZK-SNARKs. Selective disclosure allows the owner of the wallets and the creator of the ZK-SNARK (who are the same person) to selectively share a secret value with another party, that removes the Zero-Knowledge component of the ZK-SNARK. In other words, selective disclosure allows people to conduct entirely shielded transactions for the public, but show specific institutions what transactions they have committed.

Other privacy tools

In today's increasingly digital world, more and more privacy technologies are utilized to provide adequate data protection for consumers and society overall. Some most commonly discussed tools include differential privacy (DP) and secure multi-party computation (MPC). For the problem at hand, these are unfortunately inapplicable. DP is most suitable for tasks where one needs to understand information and trends from the overall group, rather than particular to specific individuals. Here, noise is introduced to a dataset to ensure user's data are privatized and secure. Bitcoin, however, operates as a public block chain that requires a majority consensus vote of honest nodes, so a DP approach to introduce noise to the data would not be appropriate. With cryptocurrency, these transactions need to be broadcast correctly, and agreed upon by all parties. On the other hand, while MPC has been growingly popular as a privacy technology, it is most often used for analyzing aggregate data while preserving the confidentiality of each data contributor. For cryptocurrency, however, the core of the block chain is based on an on-going list of transactions, so each transaction is a vital part of the technology. As such, it would not be appropriate and applicable to study aggregate data in order to protect individual user privacy. Below we discuss a technical proposal we deem most fitting for the problems tackled.

Our Technical Proposal

Our technical proposal is very straightforward: we have spent the majority of this paper arguing for privacy-aware coins and against strict KYC laws. Given some resources allocated into the small, but possible outcome of very strict KYC laws, we recommend technical investment into the support and development of privacy-aware coins.

Currently, only 5% of transactions on ZCash are shielded. [27] Professor Eran Tromer believes this is because "hardware wallet support for shielded Zcash transactions is still under development.... Naturally, a large fraction of the ZEC supply is held in people's hardware wallets, and is therefore unshielded." [20] Devices like Ledger have very weak processors and very little memory, and so cannot currently handle the extra computation required for shielded transactions.[4] Investment into hardware solutions that support privacy-aware coins would likely dramatically increase the privacy of the existing market.

Investing in more developer support and code for privacy-aware coins is a strong step forward as well. In particular, we recommend focusing on the development and support of

[4] https://www.ledger.com

mathematical research and programming libraries for ZK-SNARKs and selective disclosure tools. We also recommend more investment into software support for cryptocurrencies that are not directly privacy-aware (and are ethereum based), through investment into ZK-SNARKs and smart-contract based tumblers (code that can be run on the blockchain)

Measurement of Success and Conclusion

We have one main objective: to increase privacy on the blockchain. Our proposal to achieve this objective is focused on limiting the scope of KYC laws and promoting the use of ZK-Snarks with selective disclosure incorporated. Measuring success is not simple and cannot be boiled down to a single yes or no question. It is also difficult to find a way in which to quantify results in a consistent manner. However, there are a few specific events and trends that would support our overall objective, the first of which being that strict KYC laws do not pass and that, if not the lawmakers themselves, then the general public acknowledges the impact of these laws and advocates for a less strict version of them. In this context, one win would be for random tax audits of blockchains to come back and show that the majority of assets are taxed. Another way in which we would be able to surmise that our proposals are successful would be for improvements to be made to technology that supports shielded transactions and selective disclosures. Examples of such improvements would be hardware wallet support and reduced transaction fees. Additionally, another measurement of success would be if technology that supports other privacy tools for non-privacy-aware coins, like mixers for Ethereum (e.g. Tornado Cash), is developed further and becomes more commonly used.

There is another element to success that is even harder to quantify but could make a significant difference moving forward. It is to raise awareness about the privacy issues that currently exist on the blockchain. Other measurements of success and technological improvements would be fantastic, but first people need to understand what is happening and how they can be affected. The current state of the blockchain combined with proposed KYC laws will likely erode people's willingness to even use the blockchain. We want to avoid the lack of privacy hampering the progress of the blockchain in the future. As long as the ideas we propose address this concern, then we can consider them successful.

We will leave the final word of this report to a person that was well ahead of their time in terms of addressing privacy concerns on the blockchain, Dr. Eran Tromer, who said in an interview with us, "I think that a world devoid of financial privacy is scary, deplorable and unlikely. Cryptocurrencies and decentralized finance will not fulfill their promise until you can buy a book without broadcasting your transaction on-chain. Therefore, for the DeFi vision to happen in earnest and with widespread adoption, privacy solutions *must* become ubiquitous. Our job, as cryptographers, is to help ensure it's the *safe* and *secure* privacy solutions that get used. As for Bitcoin, specifically: for the aforementioned reason, it would have to either evolve to provide privacy (the recent Taproot protocol upgrade is a tiny step in that direction), or more likely: become a reserve asset that people hesitate to directly transact in because who's crazy enough to "tweet" their account balances and transaction, but that can be bridged, tokenized and securitized to other platforms that do provide privacy." [20]

References

[1] Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” *Bitcoin.org*, 2008, https://bitcoin.org/bitcoin.pdf.

[2] Pragmatic Coders. “Is It Possible to Have Anonymous Transactions on the Public Blockchain?” *Software Product Development Services for Startups & SMB Companies*, 2019, https://www.pragmaticcoders.com/blog/anonymous-transactions-on-the-public-blockchain.

[3] “Cryptocurrency Prices, Charts and Market Capitalizations.” *CoinMarketCap*, 2021, https://coinmarketcap.com/.

[4] Bitcoinist. “US Dea 'Actually Wants' Criminals to Keep Using Bitcoin.” *Bitcoinist.com*, 8 Aug. 2018, https://bitcoinist.com/dea-wants-criminals-use-bitcoin/.

[5] “AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT.” 2021.

https://int.nyt.com/data/documenttools/affidavit-in-support-of-seizure-warrant/fd1288c50cc29e1b/full.pdf

[6] Phan, Tuan. “Did the FBI Hack Bitcoin? Deconstructing the Colonial Pipeline Ransom.” *ISACA*, 2021, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/did-the-fbi-hack-bitcoin-deconstructing-the-colonial-pipeline-ransom.

[7] “Home: Ethereum.” *Ethereum.org*, https://ethereum.org/en/.

[8] Perlroth, Nicole, et al. “Pipeline Investigation Upends Idea That Bitcoin Is Untraceable.” *The New York Times*, The New York Times, 9 June 2021, https://www.nytimes.com/2021/06/09/technology/bitcoin-untraceable-pipeline-ransomware.html.

[9] Romo, Vanessa. “How a New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back.” *NPR*, NPR, 8 June 2021, https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac.

[10] “How to De-Anonymize Bitcoin - Bitcoin and Anonymity.” *Coursera*, https://www.coursera.org/lecture/cryptocurrency/how-to-de-anonymize-bitcoin-qnS76.

[11] Chen, James. “Know Your Client (KYC).” *Investopedia*, Investopedia, 19 May 2021, https://www.investopedia.com/terms/k/knowyourclient.asp.

[12] Daly , Lyle. “What Is KYC, and Why Do Crypto Exchanges Require It?” *The Motley Fool*, 29 Sept. 2021, https://www.fool.com/the-ascent/cryptocurrency/articles/what-is-kyc-and-why-do-crypto-exchanges-require-it.

[13] Matthew. “Uncover the Best Privacy Coins in 2021.” *Hacker Noon*, 25 Sept. 2021, https://hackernoon.com/meet-the-best-privacy-coins-in-2021.

[14] Smith, Timothy. “Cryptocurrency Regulations around the World.” *Investopedia*, Investopedia, 13 Oct. 2021, https://www.investopedia.com/cryptocurrency-regulations-around-the-world-5202122.

[15] Lipton, Eric, et al. “Regulators Racing toward First Major Rules on Cryptocurrency.” *The New York Times*, The New York Times, 23 Sept. 2021, https://www.nytimes.com/2021/09/23/us/politics/cryptocurrency-regulators-rules.html.

[16] Smialek, Jeanna. “Why Washington Worries about Stablecoins - the New York Times.” *NYTimes*, 2021,

https://www.nytimes.com/2021/09/17/business/economy/federal-reserve-virtual-currency-stablecoin.html.

[17] Staffer, Legal Examiner. “Privacy Coins 101.” *The Legal Examiner*, The Legal Examiner, 23 Sept. 2021, https://www.legalexaminer.com/technology/crypto/privacy-coins-101/.

[18] “Follow the Money.” *Wikipedia*, Wikimedia Foundation, 13 Aug. 2021, https://en.wikipedia.org/wiki/Follow_the_money.

[19] The White House. “Fact Sheet: The Bipartisan Infrastructure Deal.” *The White House*, The United States Government, 6 Nov. 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/06/fact-sheet-the-bipartisan-infrastructure-deal/.

[20] Tromer, Eran. “Q&A w/ Eran Tromer Re: Zcash.” 3 Dec. 2021.

[21] Financial Crimes Enforcement Network. “Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets.” *Federal Register*, 15 Jan. 2021, https://www.federalregister.gov/documents/2021/01/15/2021-01016/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.

[22] Green, Matthew D., and Eran Tromer. “Comments on FinCEN’s Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets.” Received by Policy Division: Financial Crimes Enforcement Network, USA, 3 Jan. 2020, USA.

[23] Worldometer. “GDP by Country.” *Worldometer*, 2021, https://www.worldometers.info/gdp/gdp-by-country/.

[24] Wiki. “Maxwell's Demon.” *Wikipedia*, Wikimedia Foundation, 12 Nov. 2021, https://en.wikipedia.org/wiki/Maxwell%27s_demon.

[25] Wiki. “Heat Death of the Universe.” *Wikipedia*, Wikimedia Foundation, 29 Nov. 2021, https://en.wikipedia.org/wiki/Heat_death_of_the_universe.

[26] “Crypto Wars.” *Wikipedia*, Wikimedia Foundation, 16 Oct. 2021, https://en.wikipedia.org/wiki/Crypto_Wars.

[27] Ethereal Summit. “Private Transactions with Tornado Cash | Ethereal Virtual Summit.” *YouTube*, YouTube, 12 May 2020, https://www.youtube.com/watch?v=CcqKAqGsyiQ.

[28] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfelder, S, 9 Feb. 2016, https://www.uio.no/studier/emnA%20Fistful%20of%20Bitcoins:%20Characterizing%20Payments%20Among%20Men%20with%20No%20Nameser/matnat/ifi/IN5420/v18/timeplan/resources/bitcoin-and-cryptocurrency-techniques.pdf

[29] Meiklejohn, Sarah, et al. “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names.” *Cseweb.ucsd.edu*, 2013, https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[30] Goodell, Geoff, and Tomaso Aste. “Can Cryptocurrencies Preserve Privacy and Comply with Regulations?” *Frontiers*, Frontiers, 28 May 2019, https://www.frontiersin.org/articles/10.3389/fbloc.2019.00004/full.