An argument against KYC bitcoin

by

Heady Wook

05 July 2022

Introduction

In the bitcoin white paper, Satoshi Nakamoto cited the need for a cash system over the internet without the need for a trusted third party (Nakamoto, 2008). A few months later, Nakamoto introduced the Bitcoin network to the world. In block zero (i.e., the genesis block) of the Bitcoin blockchain, the following message was included: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" (Bitcoin Wiki, 2010). On one hand, the quote references a UK news piece outlining Chancellor Alistair Darling's consideration of a *second* bailout for banks which meant pumping billions more of British pounds into the economy (Elliot and Duncan, 2009). On the other hand, the quote references Nakamoto's frustration and distrust of the traditional financial system and, more broadly, trusted third parties. This is made clear in the white paper abstract and the first paragraph's opening lines. In another section of the white paper, Nakamoto compares the traditional finance privacy model with Bitcoin's privacy model. In Bitcoin's model, trusted third parties are no longer responsible to safeguard an individual's privacy by limiting access to information. In fact, no personal information is required at all. With Bitcoin, individuals can maintain privacy simply by "keeping public keys anonymous" (Nakamoto, 2008). In an early bitcoin forum post, Nakamoto wrote:

"We have to trust them with our privacy, trust them not to let identity thieves drain our accounts… placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors… It's time we had the same thing for money… without the need to trust a third party middleman, money can be secure and transactions effortless… The result is a distributed system with no single point of failure. Users hold the

[private] keys to their money and transact directly with each other" (Nakamoto, 2009).

Nakamoto was concerned about trusting third parties with both privacy and money. Specifically, Nakamoto cites a few points of failure of the traditional finance privacy model: Bad actors or "identity thieves," lack of administrator integrity, and authoritative demands from "superiors," such as a government. One manifestation of these failures is showcased by the long history of currency debasing governments (Ammous, 2018) and includes the event cited within the genesis block. Alluding to Bitcoin, Nakamoto suggested these issues are solved with "a distributed system with no single point of failure."

Bitcoin has been a long time coming. The conversation about "private," "sovereign," or "electronic" currency has been discussed by others at least a decade before Bitcoin's inception. For instance, *A Cypherpunk's Manifesto* discusses anonymous transaction systems on the internet (Hughes, 1993), *The Sovereign Individual* predicts a private and permissionless internet currency (Davidson and Rees-Mogg, 1997), and *Cryptonomicon* describes an anonymous digital gold (Stephenson, 1999). Nakamoto designed Bitcoin with such properties: Bitcoin is pseudonymous, it can be used privately, and it is permissionless. However, KYC[1] has proven to be pervasive, persistent, and problematic for users looking to benefit from such properties.

Along with bitcoin's price action from 2020 through 2021, bitcoin companies have experienced lots of growth. Coinbase, for

1 "KYC" refers to the confirmation of identity of an account holder via the collection of documents (i.e., driver's license, social security number, employment record, selfies, etc; Federal Reserve, 1997) by financial third-party services (e.g., bitcoin exchanges) on behalf of the Internal Revenue Service (Internal Revenue Service, 2000).

example, reported reaching over 35 million users in over 100 countries by the end of 2020 (Aki, 2021). Furthermore, in 2022 Coinbase took out a 60-second Super Bowl ad featuring a floating QR code which reached over 20 million hits within just one minute (Valinsky, 2022). Surojit Chatterjee, Chief Product Officer at Coinbase, went so far as to call it "historic and unprecedented" (Surojit, 2022). However, Coinbase is only one of many successful companies. According to CoinGecko, Coinbase ranks 6th in terms of the most "trusted" exchanges with Binance (1st), OKX, FTX, KuCoin, and Huobi Global (5th) respectively taking the lead (CoinGecko, n.d.). Together, these exchanges alone have KYC'd millions upon millions of users. These massive KYC efforts are in direct contrast with the pseudonymous, permissionless, peer-2-peer, cash system with no third parties developed by Nakamoto. Furthermore, KYC creates honey pots of user information and gives rise to a permissioned social system.

KYC Creates Honey Pots of User Information

Every time an individual signs up for an exchange (or related service), they are likely asked to KYC themselves; that is, provide personally identifiable information (PII). PII typically consists of a selfie, drivers license, social security number, address, email, and phone number; and is usually stored by a third party, such as Prime Trust (n.d.). When Nakamoto (2009a) said, “We have to trust them with our privacy [and] trust them not to let identity thieves drain our accounts,” the reference to “them” can be thought of as third party bitcoin services. Third parties come with inherent risks, such as bad actors (e.g., insider job; BitThumb, 2019), lack of administrator integrity (e.g., BitConnect exit scam; Mangan, 2021), and susceptibility to government demands (e.g., IRS forces compliance; Coinbase, 2018). When Nakamoto references “identity thieves,” he refers to data breaches in which

"hackers" gain access to and profit from PII, either by directly stealing funds, selling the PII to interested parties, or extortion. Given all the PII provided, KYC creates a honey pot of user information that is ripe for exploitation.

Data breaches have become more and more prevalent over the years (Khosrowshahi, 2017; Lawler, 2021; McLean, 2019; Muncaster, 2018; Ng and Musil, 2017; Reuters, 2017; Silver-Greenberg and Goldstein, 2014; Tabuchi, 2015; Warren, 2011; Winder, 2020). According to Statista (2021), data breaches have increased over 500% from 2005 through 2020. Furthermore, according to the Cost of Data Breach Report, 80% of all data breaches in 2019 included customer PII (i.e., name, credit card information, health records, and payment information; IBM Corporation, 2020). Data breaches may also affect more sensitive types of PII, such as social security number, driver's license number, or biometrics (Department of Homeland Security, 2021).

All trusted third parties are susceptible to a data breach, including bitcoin companies. For instance, consider the Ledger hack of July 2020. In an official statement by Ledger CEO, "1 million email addresses had been stolen as well as 9,532 more detailed personal information (postal addresses, name, surname and phone number)" (Gauthier, 2020). That same year, the Ledger customer database was dumped on to Raidforum, a database sharing and marketplace forum (Ledger, 2022). Thereafter, several Ledger users reported phishing attempts, extortion, and threatening emails, including threats of kidnapping and violence, such as murder.

Reddit user Cuongnq received a phishing email prompting him to "download the latest version of Ledger Live" and to follow the instructions to set up a "new PIN" for his wallet (Cuongnq, 2020). Another Reddit user, Silkblueberry (2021), received an email stating that hackers had videos of him "masturbating to

porn" and that they would post the videos publicly unless he sent them bitcoin as payment. Silkblueberry saw through the ploy. However, the hackers resorted to more extreme measures, threatening to associate his email with "child porn sites" and frame him as a "child predator" if he did not send them $500 in bitcoin. Yet another user received a phone call from an unknown man demanding payment. The man threatened he would "show up to [his] house, kidnap [him], and 'stab to death' any relatives living at [his] address" if he did not send a payment by midnight that night (Osemka8, 2020).

The Ledger hack is one example that illustrates how damaging an exploited KYC honey pot can be. Still some might suggest that KYC services are needed because they offer an easy on-ramp for newcomers and that exposure is worth the risk. To this one can point to the many non-KYC alternatives known to preserve individual privacy and security. Furthermore, these non-KYC alternatives have become easier over time with the help of several guides and resources. These non-KYC alternatives include: (1) Using decentralized peer-to-peer exchanges like Bisq Network or Hodl-Hodl to buy bitcoin (Wook, 2020a and Bitcoin QnA, 2021); (2) buying privately from a bitcoin ATM (Wook, 2020b); (3) buying or selling face-2-face or selling goods and services at a bitcoin meet-up (Bitcoin Only, n.d.); and (4) mining for bitcoin at home (Diverter_NoKYC, 2020 and Econoalchemist, 2021).

Others might cite the use of bitcoin in criminal activity and suggest KYC provides individuals with the peace of mind that one is not inadvertently supporting illicit activity. However, bitcoin's use in criminal activity is small compared to that of the US dollar. In 2017, during a judiciary committee hearing, Deputy Assistant Secretary of the Office of Terrorist Financing and Financial Crimes, Jennifer Fowler, testified that "although virtual currencies are used for illicit transactions, the volume is small

compared to the volume of illicit activity through traditional financial services" (Fowler, 2017). Given the differences in volume, it is unlikely one may inadvertently support criminal activity by buying non-KYC bitcoin. This becomes even more unlikely when one buys or sells peer-to-peer at a local bitcoin meetup, mines bitcoin, or buys from a bitcoin ATM.

Bitcoin was designed in part as pseudonymous, yet there is an alarming level of KYC taking place which completely undermines this property. Millions of users all over the world are tying their identity to their bitcoin and everyone of them is contributing to the creation of honey pots of user information. This remains true even in the face of overwhelming evidence that data breaches have become almost an everyday occurrence. Rather than sacrificing pseudonymity, taking on additional risk, or contributing to the problem, users should instead be part of the solution and take back their pseudonymity, reduce risks, and protect PII by using non-KYC alternatives.

KYC Gives Rise to a Permissioned Social System

The Bitcoin network is a permissionless cash system outside the control of any third party. However, the majority of individuals are not using bitcoin this way. Instead, individuals have become reliant on third-party KYC services, such as bitcoin exchanges, yield platforms, and hosted mining, among others. Not only does KYC undermine one's pseudonymity (established in the previous section), it also undermines one's transactional privacy. This is true even after taking custody of one's bitcoin. Unlike physical cash, where a bank cannot track what one does with it after withdrawal, a third party, such as an exchange, *is* able to track what one does with their bitcoin after it has been withdrawn (Samourai Wallet, 2022). That is, until the proper privacy

measures are taken, such as participating in a coinjoin[2]. However, even if an identity can be obfuscated from an individual's bitcoin transactions, the KYCing third party still retains all the user's personally identifiable information (PII), including name, address, selfies, and total purchase amount. Armed with PII and the ability to "spy" on transactional behavior, KYC gives rise to a permissioned social system. While there are many examples one can cite as to how KYC gives rise to a permissioned social system (e.g., limits and restrictions, Zhao, 2021 and Pratz, 2021; intrusive verification measures, Bitonic, n.d.-a and Bitonic, n.d.-b; address whitelisting, Celsius, n.d., Kraken, n.d., and OMGfin, 2018; and state interventions, Brennan, 2022 and Gaceta Oficial de la Rebública Bolivariana de Venezuela, 2020), this section focuses on coinjoin as an example of a forbidden behavior within a permissioned social system. Coinjoin was selected given the important role it plays in everyday privacy.

Since Bitcoin is a public ledger, it is good practice to "make every spend a coinjoin" (SamouraiDev, 2019). This is true for two reasons: First, coinjoining limits any inferences a spying third-party might be able to draw up from one's transaction history and, second, coinjoining protects others from peering into one's personal finances. Reason one is important because, as discussed above, a KYCing third party can track what one does with their bitcoin and coinjoining can help users gain forward-looking privacy. Reason two is important because, unlike cash or

2 Coinjoin "is a trustless method for combining multiple bitcoin payments from multiple spenders into a single transaction to make it more difficult for outside parties to determine which spender paid which recipient or recipients" (Bitcoin Wiki, 2015). In other words, coinjoin is a privacy tool that obfuscates transaction history by undermining the common input heuristic. This effectively and reliably provides users with forward-looking transactional privacy at the application layer with no changes to the main bitcoin protocol.

debit/credit cards, where a merchant (i.e., a payee) cannot peer into a payer's finances (i.e., bank account totals), with bitcoin, payee's *can* peer into a payer's finances. This is akin to handing out one's bank statement with every transaction.

If one takes a moment to ponder some of the situations that may arise from such a situation, one will quickly realize the implications this has on privacy. One caricatured example is put forth by Samourai Wallet (2022), "Imagine if your church pastor was able to see your OnlyFans subscription when you place a dollar bill into the offering plate." The dollar bill here represents a typical bitcoin transaction. A coinjoin would have provided the user in this example the privacy needed to avoid this awkward situation by obfuscating the payments transaction history. In another more extreme example, imagine paying someone a small amount but using a large UTXO. The person receiving the payment would be able to see the payer holds a significant amount of bitcoin. This might place the payer at a higher risk for a five-dollar wrench attack. A coinjoin would have broken up a large UTXO into smaller UTXOs, reducing the payee's ability to determine a payer's holdings. Given these examples, it becomes clear that Bitcoin lacks essential qualities found in physical cash that coinjoin can make up for. Despite the benefits that coinjoin provides users, KYC third-party services operate on the false premise that coinjoining is malicious or risky and prohibit its use. With coinjoin prohibition as a common practice among some of the most popular exchanges, a permissioned social system has effectively designated coinjoins as "bad."

Take BlockFi for example. They have a "prohibited uses" page stating to maintain "a policy of strict regulatory compliance" and therefore prohibit deposits and withdrawals to or from: Mixing services, peer-to-peer and other exchanges which do not have KYC, gambling sites, and dark net marketplaces.

Furthermore, BlockFi "retains the right to return funds and freeze/close accounts as necessary" (BlockFi, n.d.). BlockFi is only one of many exchanges known to prohibit or flag coinjoins. For instance, in one of the more extreme examples, Reddit user Bujuu (2020) reported his exchange account was closed due to the "amount and frequency" of his coinjoin transactions. The exchange, Bitvavo, claimed Bujuu posed an "unacceptable risk" and closed his account as a measure of mitigation. Later Bujuu said, "It kinda bugs me that I'm not allowed to do what I want with my BTC, that it's all being monitored." Coinjoin prohibition is perhaps one of the clearest examples of how KYC gives rise to a permissioned social system.

Several other users have reported milder experiences. One user claimed, "@bottlepay [has] rejected my incoming btc transaction due to the coins having been in samourai wallet and/or mixed with @SamouraiWallet #Whirlpool / If you have sent mixed coins you will get stung" (Marty_P_B, 2021). Marty reported this issue upon the deposit of funds which demonstrates a backward-looking analysis on his coin's history. A similar level of intrusion has been reported by others. For instance, another user received an email from Paxos stating, "We noticed that a BTC withdrawal from your account has potentially been sent to a known bitcoin mixing service. This type of transaction is not permitted on the platform. Please confirm whether the funds have been sent to a mixing service" (McHodled, 2020). This time the issue arose upon the withdrawal of funds which demonstrates a forward-looking analysis on the coin's history. Furthermore, RiccardoMasutti (2021) claimed "@bitwala sent [him] an email 3 days ago about a couple of post-CoinJoin transactions that happened almost 6 MONTHS AGO" and Kristapsk (2021) claimed he received "an e-mail from @BitMEX about [an] old #Bitcoin deposit transaction (last summer) that 'may be connected with

activity that is against 1.1(a) of the HDR Terms of Service.', it was @joinmarket coinjoin." These last two examples demonstrate the depth of chain analysis conducted by KYCing third parties.

Taken together, one can see how pervasive a permissioned social system can be. Users want to reap the benefits a coinjoin yet coinjoining is considered prohibited behavior by many major third-party KYC exchanges (or related services; 6102bitcoin, n.d.). This general distaste for coinjoin, along with blatant chain analysis, places individuals who KYC in a vulnerable position. First, individuals who KYC are prohibited from exercising basic privacy rights. Furthermore, they face punitive measure if they do; and, second, KYC'd individuals are being spied on. Any reasonable individual would agree this is not a good position to be in, especially when participating in an independent and alternative cash system with no third parties. Despite the clear benefits that coinjoin has to offer, the current view is that coinjoins are too "risky." On a coinjoin panel at Bitcoin Conference 2022, Craig Raw, founder of Sparrow Wallet, said:

> "If we use the tools [i.e., coinjoin] that we have today, it changes the mindset of people and it changes how society views it. If coinjoin becomes a widely used thing today, then that will change the way that society views it and I think that it is important not to wait too long and to actually use the tools because… it changes the way that the rules and regulations of the world will form." (Bitcoin Magazine, 2022).

According to Raw, coinjoin normalization is a function of its use. Therefore, individuals must take it upon themselves to exercise their rights to privacy. This cannot be accomplished from within a permissioned system; nor will it be granted. Rather, coinjoin normalization must be accomplished outside of a

permissioned system, such as within the Bitcoin network as it was designed to be used–without permission.

Conclusion

In the present article, the claim was made that KYC creates honey pots of user information and gives rise to a permissioned social system. In summary, when one KYCs, they must provide a lot of sensitive personal information which contributes to the honey pot. This action alone is enough to negate pseudonymity given an identity has been associated with one's bitcoin holdings. Furthermore, individuals must trust that third parties will keep sensitive information safe. Further, when one KYCs, they voluntarily enter into a permissioned relationship with a third party. That is, a user must abide by the rules set in place by a third party or potentially face punitive measures, such as asset seizure, account closure, or frozen assets. Given the important role it plays in everyday privacy, coinjoin was cited as an example of a forbidden behavior within a permissioned social system. Upon examination of the evidence it becomes clear that KYC indeed creates honey pots of user information and gives rise to a permissioned social system. Several implications on privacy were also made.

References

6102bitcoin. (n.d.). *Coinjoin flagging*. Retrieved July 2, 2022, from https://6102bitcoin.com/coinjoin-flagging/

Aki, J. (2021, August 25). Coinbase users top 35 million as exchange continues on growth pattern. *Inside Bitcoins*. https://insidebitcoins.com/news/coinbase-users-top-35-million-as-exchange-continues-on-growth-pattern

Ammous, S. (2018). Monetary metals. In *The Bitcoin standard: The decentralized alternative to central banking* (1st ed., pp. 17–40). John Wiley & Sons, Inc.

Bitcoin Magazine. (2022, April 10). *Coinjoins & coinswaps with Ben Carman, Craig Raw, Fontaine, and Nicholas Gregory* [Video]. YouTube. https://www.youtube.com/watch?v=OwJLoJ_nPDE&t=2272s

Bitcoin Only. (n.d.). *Meetups*. https://bitcoin-only.com/meetups

Bitcoin QnA. (2021). *10 steps to your first non-KYC bitcoin*. Bitcoiner Guide. https://bitcoiner.guide/hodlhodl/

Bitcoin Wiki. (2010, December 16). *Genesis block*. Retrieved July 2, 2022, from https://en.bitcoin.it/wiki/Genesis_block

Bitcoin Wiki. (2015, March 2). *Coinjoin*. Retrieved July 3, 2022, from https://en.bitcoin.it/wiki/CoinJoin

Bitonic. (n.d.-a). *Why do we ask you to sign a message?* Retrieved July 2, 2022, from https://bitonic.nl/en/faq/43/why-do-we-ask-you-to-sign-a-message

Bitonic. (n.d.-b). *Why do we ask you to verify your bitcoin address?* Retrieved July 2, 2022, from https://bitonic.nl/en/faq/42/why-do-we-ask-you-to-verify-your-bitcoin-address

BitThumb. (2019, March 30). *Apology for internal embezzlement accident*. BitThumb Cafe. https://cafe.bithumb.com/view/board-contents/1640037

BlockFi. (n.d.). *Prohibited uses*. Retrieved July 2, 2022, from https://blockfi.com/prohibited-uses/

Brennan, M. (2022, February 9). Russia to publish bill that will legalize and regulate cryptocurrencies on february 18, 2022. *The Crypto Basic*. https://thecryptobasic.com/2022/02/09/russia-to-publish-bill-that-will-legalize-and-regulate-cryptocurrencies-on-february-18-2022/

Bujuu. (2020, August 13). *Exchange account closed because of "risk profile" (btc sent to mixing services)* [Online forum post]. Reddit. https://www.reddit.com/r/Bitcoin/comments/i8ye6x/exchange_account_closed_because_of_risk_profile/

Celsius. (n.d.). *Whitelist withdrawal addresses*. All about Celsius. Retrieved July 2, 2022, from https://allaboutcelsius.com/whitelist-withdrawal-addresses/

Coinbase. (2018, February 23). *IRS notification*. Coinbase Support. https://archive.ph/4IfUM

CoinGecko. (n.d.). *Top crypto exchanges ranking*. Retrieved July 2, 2022, from https://www.coingecko.com/en/exchanges

Cuongnq. (2020, October 25). *[Phishing Alert] To all Ledger customer* [Online forum post]. Reddit. https://www.reddit.com/r/ethfinance/comments/jhqhc0/phishing_alert_to_all_ledger_customer/

Davidson, J. D., & Rees-Mogg, W. (1997). *The sovereign individual* [E-book]. Simon & Schuster. https://archive.org/details/sovereignindivid00davi

Department of Homeland Security. (2021, December 8). *What is personally identifiable information?* Homeland Security. http://dhs.gov/privacy-training/what-personally-identifiable-information

Diverter_NoKYC. (2020). *Mining for the streets*. On a Path, Diverted. https://diverter.hostyourown.tools/mining-for-the-streets/

Econoalchemist. (2021, January 29). *Home mining for non-KYC bitcoin*. Burn the Bridge Blog. https://www.econoalchemist.com/post/home-mining-for-non-kyc-bitcoin

Elliott, F., & Duncan, G. (2009, January 3). Chancellor Alistair Darling on brink of second bailout for banks. *The Times*. https://archive.ph/ICMLC

Federal Reserve. (1997, September). *Know Your Customer*. https://www.federalreserve.gov/boarddocs/SupManual/bsa/bsa_p5.pdf

Fowler, J. (2017, November 28). *Testimony of Jennifer Fowler*. Judiciary Committee. https://www.judiciary.senate.gov/imo/media/doc/Fowler%20Testimony.pdf

Franklin, B. (1756). *Pennsylvania assembly: Reply to the governor, 11 November 1755*. National Archives. Retrieved July 2, 2022, from https://founders.archives.gov/documents/Franklin/01-06-02-0107

Gaceta Oficial de la Rebública Bolivariana de Venezuela. (2020, September 21). *Gaceta Oficial de la Rebública Bolivariana de Venezuela*. Internet Archive. https://web.archive.org/web/20200926222909/https://www.morocotacoin.com/wp-content/uploads/2020/09/Gaceta-Oficial-41969.pdf

Gauthier, P. (2020, December 21). *Message by Ledger's CEO - update on the July data breach. Despite the leak, your crypto assets are safe*. Ledger. https://www.ledger.com/message-ledgers-ceo-data-leak

Hughes, E. (1993, March 9). *A cypherpunk's manifesto*. Nakamoto Institute. https://nakamotoinstitute.org/cypherpunk-manifesto/

IBM Corporation. (2020, July). *Cost of a data breach report*. IBM. https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

Internal Revenue Service. (2000). *Application procedures for qualified intermediary status*. IRS. https://www.irs.gov/pub/irs-drop/rp-00-12.pdf

Khosrowshahi, D. (2017, November 22). *2016 data security incident*. Uber Newsroom. https://www.uber.com/newsroom/2016-data-incident

Kraken. (n.d.). *Adding and confirming a new cryptocurrency withdrawal address*. Kraken Support. Retrieved July 2, 2022, from https://support.kraken.com/hc/en-us/articles/360000672863-Adding-and-confirming-a-new-cryptocurrency-withdrawal-address

Kristapsk. (2021, March 23). *Got an e-mail from @BitMEX about old #Bitcoin deposit transaction (last summer) that "may be connected with activity* [Tweet]. Twitter. https://twitter.com/kristapsk/status/1374336620158140419

Lawler, R. (2021, August 18). T-Mobile data breach exposed the personal info of more than 47 million people. *The Verge*. https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii

Ledger. (2022, April 6). *E-commerce and marketing data breach*. Ledger Support. https://support.ledger.com/hc/en-us/articles/360015559320-E-commerce-and-Marketing-data-breach-FAQ?support=true

Mangan, D. (2021, November 16). U.S. to sell cryptocurrency worth $56 million after record seizure in BitConnect fraud case. *CNBC*. https://www.cnbc.com/2021/11/16/us-selling-seized-cryptocurrency-in-bitconnect-fraud-case.html

Marty_P_B. (2021, March 2). *1. @bottlepay have rejected my incoming btc transactions due to the coins having been in samourai wallet and/or mixed with* [Tweet]. Twitter. https://archive.ph/8cMR9

McHodled. (2020, January 28). *Wtf?? Apparently you are not allowed to do what you want with your bitcoin once you own the keys. Fortunately* [Tweet]. Twitter. https://twitter.com/McHodled/status/1222172084610027523

McLean, R. (2019, July 30). Capital One data breach: A hacker gained access to 100 million credit card applications and accounts. *CNN*. https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

Muncaster, P. (2018, November 22). US Postal Service exposes 60 million users in API snafu. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/us-postal-service-exposes-60m

Nakamoto, S. (2008, October). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Nakamoto, S. (2009, February 11). *Bitcoin open source implementation of P2P currency* [Online forum post]. P2P Foundation. https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source

Ng, A., & Musil, S. (2017, September 8). Equifax data breach may affect nearly half the US population. *CNET*.

https://www.cnet.com/news/privacy/equifax-data-leak-hits-nearly-half-of-the-us-population/

OMGfin. (2018). *Rules of procedure and internal audit rules compiled pursuant to money laundering and terrorist financing prevention act*. OMGfin Exchange. https://omgfin.com/assets/pdf/Rules_of_procedure_and_internal_control_rules.pdf

Osemka8. (2020, December 22). *A user on r/ledgerwalletleak sharing his shocking story* [Online forum post]. Reddit. https://www.reddit.com/r/CryptoCurrency/comments/ki3x7z/a_user_on_rledgerwalletleak_sharing_his_shocking/

Partz, H. (2021, July 28). Binance cuts withdrawal limits, rolls out tax reporting tool. *Cointelegraph*. https://cointelegraph.com/news/binance-cuts-withdrawal-limits-rolls-out-tax-reporting-tool

Prime Trust. (n.d.). *Qualified custody*. Retrieved July 2, 2022, from https://www.primetrust.com/products/qualified-custody

Reuters. (2017, May 24). Target settles 2013 hacked customer data breach for $18.5 million. *NBC News*. https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031

RiccardoMasutti. (2021, March 26). *#CoinJoin flagging @bitwala sent me an email 3 days ago about a couple of post-CoinJoin transactions that happened* [Tweet]. Twitter. https://twitter.com/RiccardoMasutti/status/1375507165151076353

Samourai Wallet [@SamouraiWallet]. (2022, February 3). *When you withdraw from your exchange it isn't like withdrawing physical cash from an ATM. The exchange is able to* [Why we coinjoin, a thread]. Twitter.

https://threadreaderapp.com/thread/1489220847336308739.html

SamouraiDev. (2019, January 3). *Bob paid Alice but how much and with which utxo(s)? https://bitcoinmagazine.com/articles/blockchain-analysis-about-get-harder-p2ep-enters-testing-phase/ https://blockstream.info/testnet/tx/6e568c4f8ab7cda73879d45a245bd127e825b8f9bc8183576b5be22d6dc1a4c4 #Stowaway #Cahoots #P2EP Make every spend a* [Tweet]. Twitter. https://twitter.com/samouraidev/status/1080879231234727936

Silkblueberry. (2021, April 2). *Criminally threatening email* [Online forum post]. Reddit. https://www.reddit.com/r/ledgerwalletleak/comments/mj0teu/criminally_threatening_email/

Silver-Greenberg, J., & Goldstein, M. (2014, October 2). JPMorgan Chase says more than 76 million accounts compromised in cyberattack. *Deal Book*. https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

Statista. (2021, March 3). *Cyber crime: Number of breaches and records exposed 2005–2020*. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Stephenson, N. (1997). *Cryptonomicon* [E-book]. Harper Perennial. https://archive.org/details/cryptonomicon0000step_b9v1

Surojit. (2022, February 13). *Some more details. We had over 20M hits on our landing page in one minute. That was*

historic and unprecedented. [Tweet]. Twitter. https://twitter.com/surojit/status/1493113238275297280

Tabuchi, H. (2015, July 17). CVS and Walmart Canada are investigating a data breach. *The New York Times*. https://www.nytimes.com/2015/07/18/business/cvs-and-walmart-canada-are-investigating-a-data-breach.html

Valinsky, J. (2022, February 15). Coinbase's strange QR-code Super Bowl ad briefly crashes app. *CNN*. https://edition.cnn.com/2022/02/14/investing/coinbase-qr-code-app/index.html

Warren, C. (2011, June 11). Sony pictures website hacked, 1 million accounts exposed. *Mashable*. https://mashable.com/archive/sony-pictures-hacked

Winder, D. (2020, August 19). 235 million Instagram, TikTok and YouTube user profiles exposed in massive data leak. *Forbes*. https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=5169fb781111

Wook, H. (2020a, July 7). *How to buy non-KYC bitcoin with a US Postal Money Order on Bisq*. Internet Archive. https://archive.org/details/how-to-buy-non-kyc-bitcoin-with-a-us-postal-money-order

Wook, H. (2020b, November 27). *How to use Text Verified to buy non-KYC bitcoin at a bitcoin ATM*. Internet Archive. https://archive.org/details/how-to-use-text-verified-to-buy-non-kyc-bitcoin-at-a-bitcoin-atm

Zhao, C. (2021, July 27). *Thread by @cz_binance on Thread Reader App*. Thread Reader. https://threadreaderapp.com/thread/1420056975094665226.html

Donate

Please consider a donation by visiting**:**

https://btcpayjungle.com/apps/2NqQwXoB5ejGPqtHTefrsoE2oeyH/pos

Or connect via PayNym and donate:

+whitefirefly714

PM8TJeDuf5J3Xs16WxcHyMKDGas7fUjjJw49Vx1Vj9kFKURXwDBmDx78dUB9aQpvYQ8qrazSnPA4EkWNB8QLfN3X1s1qdUyuudSgKK1j2YR5ezxHPpPb

Or donate Monero (XMR):

8BCn19ApVcdMWYyNs3Xb1F8aWTcq79KSmhFSGEqcJQW85cT12pJYbr6bCrMmhqvTxNWWy7CLgKvegAKNVPd1AWXD2yH6TwJ