6 myths about privacy on blockchains

David Sverdlov and Aiden Slavin (a16z crypto)

New technologies — from the telegraph and telephone to the internet — have always sparked fresh anxieties about privacy's impending demise. Blockchains have proven no different, and privacy on blockchains is often misunderstood as either creating a dangerous level of transparency or a haven for crime.

But the real challenge is not about choosing between privacy and security, but about building tools — technical and legal — that support both. From zero-knowledge proof systems to advanced cryptography, privacy-preserving solutions are already scaling. Far from being just about finance, blockchain privacy opens doors for identity verification, gaming, AI, and more applications that benefit users.

And with U.S. stablecoin legislation recently signed into law, the need for blockchain privacy is now more urgent than ever. Stablecoins represent an opportunity to onboard a billion people into crypto. But for users to be comfortable using crypto to pay for everything from their coffee to their medical bills, they will need to be certain that the activities they undertake onchain are private. Now is not the time to mythmake, but to build.

The debate over privacy is not new, and neither is the answer: Innovation, not myths and misconceptions, will shape its future.

Myth #1: The internet is responsible for modernity's "privacy problems"

The truth: Nearly a century before the advent of the internet, the communications revolutions of the late 19th century spurred the development of privacy rights in the United States. Entrepreneurs developed technologies that allowed for the unprecedented transmission of information — news, words, pictures, and other media — including the first commercial telegraph, the telephone, the commercial typewriter, the microphone, and many others.[1] Historian and professor Sarah Igo observed that in America at the time "conflicts over privacy grew up alongside new modes of communication," eliciting new privacy questions: Could news media use the names, portraits, or pictures of others for the purpose of trade? Could law enforcement wiretap telephone lines to listen in on conversations, or use photography and fingerprinting to establish permanent records or a registry for identifying criminals?[2]

Soon after the introduction of these technologies, legal scholars began to grapple with the privacy challenges that they raised. In 1890, future Supreme Court Justice Louis D. Brandeis and fellow lawyer Samuel D. Warren published "The Right to Privacy" in the *Harvard Law Review*.[3] Privacy laws were then steadily developed in legislation, tort, and constitutional law throughout the 20th century. It was more than a century after Brandeis and Warren published their law review article, in 1993, when the first widely

[1] Sarah E. Igo, The Known Citizen: A History of Privacy in Modern America, at 26 (2018).
[2] *Id.*, at 27-34, 47-52.
[3] Warren & Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

available commercial internet browser, Mosaic, was released, and the privacy issues associated with the internet increased.

Myth #2: The internet works fine without privacy

The truth: A lack of privacy in the early internet was a significant impediment to its more widespread adoption. In general, people had higher degrees of privacy prior to the internet. As Simon Singh recounts in *The Code Book*, Whitfield Diffie, an early pioneer in cryptography research, noted that when the Bill of Rights was ratified, "any two people could have a private conversation — with certainty no one in the world enjoys today — by walking a few meters down the road and looking to see no one was hiding in the bushes."[4] Similarly, people could engage in financial transactions based on commodities or cash with a level of privacy and anonymity that is absent from most digital transactions today.

Advancements in the study of cryptography reduced concerns about privacy and resulted in new technologies that could facilitate the exchange of confidential digital information and ensure robust data protection. Predicting that many users would demand basic privacy protections for their digital activities, cryptographers like Diffie sought out new solutions that could provide such protection — namely, asymmetric public key cryptography.[5] Diffie and others developed new encryption tools that now underpin e-commerce and data protection. These tools also paved the way for other confidential exchanges of digital information, which apply to blockchains today.

The development of HyperText Transfer Protocol Secure (HTTPS) is just one example of a privacy tool that allowed the internet to flourish. In the early days of the internet, a user (i.e., a client) would communicate with a web server using the Hypertext Transfer Protocol (HTTP). This web protocol allowed data to be transferred to web servers, but it had a significant drawback: It transferred that data without encryption. Malicious actors could therefore read any sensitive information users submitted to a website. Developed a few years later by Netscape for its browser, HTTPS added a layer of encryption that could protect sensitive information. As a result, users could send credit card information over the internet and engage in private communications more broadly.

With encryption tools like HTTPS, internet users are more comfortable providing personal identifying information — names, dates of birth, addresses, and social security numbers — through online portals. This has helped make digital payments the most common payment method used in the US today. Corporations also accept the risks that arise from receiving and safeguarding such information.

These changes in behavior and process unlocked many new applications, from messaging to online banking to e-commerce. Internet activities are now a significant aspect of today's economy and generate unprecedented communications, entertainment, social networking, and other experiences.

---

[4] Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, at 307 (2000).

[5] For centuries, a "virtual dogma" in the rules of cryptography was keeping secret the "key" to deciphering a message. Steven Levy, Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age, at 69-88 (2002). That is because the same key was necessary for both scrambling and unscrambling messages, hence the term "symmetrical" cryptography. Nonetheless, this dogma created a practical problem for encrypting secret communications: persons involved in the communication had to pass the secret key between one another, which increases the chance of compromise. Although he may not have been the first to discover it, *id.*, at 312-30, Diffie's cryptography research led to the commercial development of public-key cryptography or "asymmetric" cryptography, where a public key would be used to encrypt a message and a separate private key would be used to decrypt it.

Myth #3: Public blockchain transactions are anonymous

The truth: Public blockchain transactions are transparently recorded on an open, shared digital recordbook, making them pseudonymous, not anonymous — an important distinction. A centuries-old practice, pseudonymity even played an important role in the early United States: Benjamin Franklin famously adopted the pen name "Silence Dogood" to publish his early writings in the *New-England Courant*, while Alexander Hamilton, John Jay, and James Madison used "Publius" to identify their contributions to The Federalist Papers (Hamilton used several pseudonyms in his writings).[6]

Blockchain users transact with one another via wallet addresses that are associated with a unique series of algorithmically generated alphanumeric characters (i.e., keys), rather than their real names or identities. The distinction between pseudonymity and anonymity is critical for understanding the transparent nature of blockchains: Although the alphanumeric characters of a wallet address cannot be immediately linked to the identifying information of a particular user, the holder of the keys has far less privacy protection — let alone anonymity — than one might think. A cryptographic address can function like a username, email address, phone number, or bank account number. Once a user interacts with another person or entity, the counterparty can link the pseudonymous wallet address with a particular user, exposing the user's entire onchain transaction history and potentially revealing their personal identity. For example, if a shop accepts payment in cryptocurrencies from its customers, the store's cashiers could see where else those customers had shopped before and the customer's crypto holdings (at least for the wallet on the blockchain network used for that particular transaction, given that sophisticated crypto users have multiple wallets and tools). Think of this as the equivalent of having the history of your credit card use made public.

The original Bitcoin White Paper discussed this risk, stating that "if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner."[7] Ethereum co-founder Vitalik Buterin has also written about the challenges involved in "making a significant portion of your life public for anyone to see and analyze,"[8] and he has proposed solutions such as "privacy pools" — where zero-knowledge proofs allow users to prove legitimate funds and sources without having to reveal full transaction history.[9] For this reason, several companies are working on solutions in this space as well, not just to protect privacy but also to allow new applications that combine privacy with other unique properties of blockchains.

Myth #4: Due to blockchain privacy, criminality abounds

The truth: Data from the U.S. government and blockchain analytics companies shows that the use of crypto for illicit finance is still below that of fiat currencies and other traditional sources, and illicit activities are a small portion of the total activity that occurs on blockchains (see here and here; we also discuss this in greater detail below). This data has been consistent for years. In fact, as blockchain technology has continued to develop, rates of illicit activities on chain have declined.

---

[6] *See* Massachusetts Historical Society, *The Birth of Silence Dogood*, https://www.masshist.org/online/silence_dogood/essay.php?entry_id=203. James Madison, John Jay, and Alexander Hamilton published the *Federalist Papers* under the pen name "Publius." *See* Library of Congress: Research Guides, *Federalist Papers: Primary Documents in American History*, https://guides.loc.gov/federalist-papers.
[7] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 10 (2008), https://bitcoin.org/bitcoin.pdf.
[8] Vitalik Buterin, *An incomplete guide to stealth addresses* (Jan. 20, 2023), https://vitalik.eth.limo/general/2023/01/20/stealth.html.
[9] Vitalik Buterin et al., Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium (Sept. 6, 2023), https://ssrn.com/abstract=4563364 or http://dx.doi.org/10.2139/ssrn.4563364.

It is no secret that illicit activities made up a large portion of the Bitcoin network's total activity in its earliest days. As David Carlisle observes, citing researcher Sarah Meickeljohn, "At one point, the main Bitcoin address that the Silk Road used contained 5% of all bitcoins in existence, and the site accounted for as much as one-third of Bitcoin transactions that took place during 2012."[10]

But the crypto ecosystem has since successfully integrated effective mechanisms to mitigate illicit finance, and the total amount of lawful activities has grown. Recent reports from TRM Labs estimate that illicit volume accounted for less than 1% of total crypto volume in 2024 and 2023 (based on the USD value of funds stolen in crypto hacks, as well as the USD value of transfers to blockchain addresses that have been linked to entities in illicit categories).[11] Chainalysis and other blockchain analytics companies have published similar estimates (including for earlier years as well).[12]

Likewise, government reports, particularly those from the Biden Administration's Treasury Department, have shed light on the lower illicit finance risks of cryptocurrencies when compared to offchain activities. Indeed, Treasury's recent reports that discussed crypto — including its 2024 National Risk Assessments,[13] Illicit Finance Risk Assessment on Decentralized Finance,[14] and Illicit Finance Risk Assessment of Non-Fungible Tokens[15] — recognized that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or via more traditional methods.

Furthermore, the transparency features of many blockchains (such as those discussed in Myth #3) have made it easier for law enforcement to catch criminals. Because the movement of illicit funds is visible on public blockchain networks, law enforcement can track the funds to "off-ramps" (i.e., cash-out points for cryptocurrencies) and blockchain wallet addresses associated with bad actors. Blockchain tracing techniques played an important role in the takedowns of illicit marketplaces, including the Silk Road, Alpha Bay, and BTC-e.

It is precisely for these reasons that many criminal actors have realized the potential pitfalls of using blockchains for transferring illicit funds and have therefore stuck to more traditional methods. While increased blockchain privacy could, in certain instances, make law enforcement efforts to police onchain

---

[10] David Carlisle, The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond, at 10 (2024), citing Sarah Meiklejohn et al., "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" (2023), https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.

[11] TRM Labs, *2025 Crypto Crime Report: Key trends that shaped the illicit crypto market in 2024* (2025), http://www.trmlabs.com/files/report-2025-crypto-crime-report.

[12] Chainalysis Team, *2025 Crypto Crime Trends: Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized* (2025), https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/; Elliptic, *Financial Crime Typologies in Cryptoassets: The Concise Guide for Compliance Leaders* (2020), https://www.elliptic.co/resources/typologies-concise-guide-crypto-leaders.

[13] U.S. Department of the Treasury, Treasury Publishes 2024 National Risk Assessments for Money Laundering, Terrorist Financing, and Proliferation Financing (Feb. 2024), https://home.treasury.gov/news/press-releases/jy2080.

[14] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf ("[T]his risk assessment recognizes that most money laundering, terrorist financing, and proliferation financing by volume and value of transactions occurs in fiat currency or otherwise outside the virtual asset ecosystem via more traditional methods.").

[15] U.S. Department of the Treasury, Illicit Finance Risk Assessment of Non-Fungible Tokens (May 2024), https://home.treasury.gov/system/files/136/Illicit-Finance-Risk-Assessment-of-Non-Fungible-Tokens.pdf ("The assessment identifies that NFTs and NFT platforms are, to date, rarely being used for proliferation financing or terrorist financing.").

criminal activities more challenging, new cryptographic techniques are being developed that can both protect privacy and address the needs of law enforcement.

Myth #5: You can choose between combating illicit finance or protecting user privacy — but not both

The truth: Modern cryptographic techniques can reconcile the privacy needs of users and the informational and national security needs of regulators and law enforcement. These techniques include zero-knowledge proofs, homomorphic encryption, multi-party computation, and differential privacy. Zero-knowledge proof systems may have the greatest potential to help strike the right balance. These methods may be applied in many ways to deter crime and enforce economic sanctions while also preventing the surveillance of American citizens or the use of the blockchain ecosystem to steal or launder funds.

Zero-knowledge proofs are a cryptographic process that allow one party (the prover) to convince another party (the verifier) that a statement is true without revealing information other than the fact that the specific statement is true. Take the example of proving whether someone is a citizen of the United States. Using a zero-knowledge proof, a person could prove that proposition to someone else without having to disclose a driver's license, passport, birth certificate, or other information. A zero-knowledge proof allows that fact to be confirmed without exposing the specific or additional information — whether address, birthdate, or indirect password hints — that could compromise privacy.

Given these features, zero-knowledge-proof solutions are among the best tools that can help detect and deter illicit activities while also preserving user privacy. Current research suggests that there are a number of possible methods for privacy-enhancing products and services to mitigate risk, including:

1. **deposit screening** to prevent deposits of assets coming from sanctioned persons or wallets;
2. **withdrawal screening** to prevent withdrawals from sanctioned addresses or addresses associated with illegal activity;
3. **voluntary selective de-anonymization**, which provides persons who believe that they have been erroneously added to a sanctions list with the option to de-anonymize the details of their transaction to selected or designated parties; and
4. **involuntary selective de-anonymization**, which involves a private-key-sharing arrangement between a gatekeeper entity (like a non-profit or other trusted organization) and the government, where the gatekeeper entity evaluates requests from the government to use the private keys to de-anonymize wallet addresses.[16]

With the concept of "privacy pools," Buterin and others also argue in favor of using zero-knowledge proofs so users can demonstrate that their funds do not originate from known unlawful sources — but without having to publicly reveal their entire transaction graph to do so. If users are able to furnish such proofs upon exchanging crypto for fiat currency, the cash-out points (i.e., exchanges or other centralized intermediaries) will have reasonable assurances that the crypto did not derive from proceeds of crime, while the users are able to retain privacy over their onchain transactions.

Although critics have historically raised scalability concerns about cryptographic privacy techniques like

---

[16] Joseph Burleson, Michele Korver & Dan Boneh, *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, a16z crypto (2022), https://a16zcrypto.com/posts/article/privacy-protecting-regulatory-solutions-using-zeroknowledge-proofs-full-paper/.

zero-knowledge proofs, recent advancements are making them more practical for larger-scale implementation. By reducing computational overhead, scaling solutions are making zero-knowledge proofs more efficient. Cryptographers, engineers, and entrepreneurs continue to improve the scalability and usability of zero-knowledge proofs, making them an effective tool for fulfilling the needs of law enforcement, while preserving individual privacy.

Myth #6: Blockchain privacy is only useful for financial transactions

The truth: Privacy-preserving blockchains could unlock a wide variety of both financial and non-financial use-cases. These capabilities underscore how privacy-preserving blockchain technologies fundamentally expand the scope of secure and innovative digital interactions across use cases. Examples include:

Digital ID: Private transactions enhance digital identity verification, enabling individuals to selectively — and verifiably — disclose attributes like age or citizenship without exposing unnecessary personal data. Likewise, digital ID can help patients improve the confidentiality of their sensitive information while also granularly transmitting appropriate test results and the like to their physicians.

Gaming: Encryption allows developers to create more exciting gameplay by concealing parts of a digital universe — like a special item or hidden level — from a player until their actions unlock them. Without privacy tools, blockchain-based virtual worlds would be transparent to their users, diminishing their immersiveness; a player who knows everything about a digital universe will be less motivated to explore it.

AI: Privacy-preserving blockchain tools also open new possibilities in AI, allowing for encrypted data sharing and model verification methods, without compromising sensitive information.

Finance: In finance, encryption allows decentralized finance applications to offer a wider array of services while maintaining privacy and security. Novel decentralized exchange designs could leverage encryption to improve market efficiency and fairness.

Voting: In decentralized autonomous organizations, there is a strong desire for private onchain voting to avoid the repercussions that could arise from voting for an unpopular measure, or the group-think that could result from mirroring the voting behavior of a particular individual.

These are just some of the obvious applications; as with the internet, once privacy-preserving features are added, we expect to see many novel applications.

***

The debate over privacy — who controls it, how it is protected, and when it is forfeited — precedes the digital era by at least a century. Each new technology has been met with comparable panic in its time: the telegraph and the telephone, the camera and the typewriter, all prompted debates that would shape society for generations.

To assume that blockchains uniquely imperil privacy — or that they are singularly capable of being weaponized to nefarious ends — misunderstands both history and technology. Just as encryption and cryptographic protocols enabled secure communication and commerce online, emerging

privacy-preserving technologies such as zero-knowledge proofs and advanced encryption techniques could offer practical ways to preserve privacy while also achieving compliance objectives and combatting illicit finance.

The real question is not whether new innovations reshape privacy but whether technologists and societies will rise to the challenge by implementing new solutions and practices. Privacy is not lost or compromised; it adapts to fit the broader, pragmatic needs of society. The question, for this technological revolution like for those that preceded it, is how.

***

David Sverdlov is Regulatory Counsel Partner a16z crypto. Prior to joining a16z, David worked as an associate at Baker McKenzie and Jones Day. David received his JD from Cornell Law School, and his BA from the University of California, Berkeley.

Aiden Slavin is Policy Partner for a16z crypto, supporting the advancement of the firm's global web3 policy goals. Prior to joining a16z crypto, he led crypto policy initiatives across government and industry at the World Economic Forum focused on DAOs, decentralized ID, and the metaverse. Before that, he managed the development of decentralized ID governance and standards.

***