Tornado Cash - The Battle for Privacy

Sept 2022

Tornado Cash – A story of privacy and censorship

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

From: A Cypherpunk's Manifesto by Eric Hughes

In our most recent month end note we wrote about the decision of the US Treasury to sanction Tornado Cash, a decentralised protocol, via the Office of Foreign Assets Control (OFAC) which is normally reserved for targeting individuals. What we are hoping to in this note is explain Tornado cash, highlight why privacy is important, outline some of the history of the crypto industry and how Tornado cash fits into this narrative. As we have advocated, Digital assets will flourish with well thought out regulation, unfortunately a great deal of the existing regulation can't be contorted to regulate the space, it will require a new approach. The good news is that process has started, the bad news is that there will likely be more missteps along the way.

The move against Tornado Cash is a highly controversial move for the crypto industry and was always going to be challenged in the courts. We didn't have to wait long. On the 8th September 2022, a lawsuit was filed by six individuals including two Coinbase employees, (Coinbase is paying legal fees) which claims Treasury overstepped its authority to block financial transactions benefiting foreign terrorists. It alleges that the department, perhaps unintentionally, ensnared law-abiding Americans conducting legitimate digital commerce through a cryptocurrency service that offers enhanced privacy and security. We say "unintentionally" but if OFAC is the only play you have then you are restricted to that tool, which in turn makes our point about suitability and the problem regulators have. Participating in the network will become prohibitive for many users.

A history lesson

Before we explain a bit more about Tornado Cash, we thought it might be interesting to a give a brief overview of some of the early work in encryption technology and its importance in preserving the privacy and freedom we enjoy in our everyday lives.

This isn't the first time the US government has been "at war" with the crypto community. While the term "cryptocurrency" or "crypto" is now in everyday use, it arose out of the field of cryptography. Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

The Crypto Wars

An unofficial name for the U.S. and allied governments' attempts to limit the public's and foreign nations' access to cryptography strong enough to resist decryption by national intelligence agencies (especially USA's NSA). It is during the 1990's that the cypherpunk community was energised by a battle with the US intelligence establishment relating to the export of cryptography (which the US Government had at the time classified as a munition). This is a battle that the cypherpunk movement and broader civilian cryptography community largely won, though some variations of government proposals still pop up to this day.

Keeping our email private using encryption - Phil Zimmermann, one of the original cypherpunks*, was a key player in this period.

(*A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change. Originally communicating through the Cypherpunks electronic mailing list, informal groups aimed to achieve privacy and security through proactive use of cryptography. Cypherpunks have been engaged in an active movement since the late 1980s.)

He developed PGP (Pretty Good Privacy) in 1991. PGP is an encryption program that provides cryptographic privacy and authentication for data communication. It is used for signing, encrypting and decrypting texts and emails to increase the security of email communication.

Shortly after its release, PGP encryption found its way outside the United States and in February 1993 Zimmermann became the formal target of a criminal investigation by the US Government for "munitions export without a license". Penalties for violation, if found guilty, were substantial. After several years, the investigation of Zimmermann was closed without filing criminal charges against him or anyone else.

Zimmermann challenged these regulations in an imaginative way. He published the entire source code of PGP in a hardback book, which was distributed and sold widely. Anybody wishing to build their own copy of PGP could scan the pages into a software reader and create a set of source code text files. One could then build the application using freely available compiler software. PGP would thus be available anywhere in the world. The claimed principle was simple: export of munitions—guns, bombs, planes, and software—was (and remains) restricted; but the export of books is protected by the First Amendment of the US Constitution. The question was never tested in court with respect to PGP.

US export regulations regarding cryptography remain in force but were liberalized substantially throughout the late 1990s. Since 2000, compliance with the regulations is also much easier. PGP encryption no longer meets the definition of a non-exportable weapon and can be exported internationally except to seven specific countries and a list of named groups and individuals (with whom substantially all US trade is prohibited under various US export controls).

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Zimmerman wrote an essay on why he wrote PGP which is linked below and is worth a read.

We've included a section below as it perfectly summarises the justification for encrypting our email communications. Something we all take for granted today. And, with the progress of technology, how much easier it's become for governments to see what we're up to if they so choose.

"The right to privacy is spread implicitly throughout the Bill of Rights. But when the United States Constitution was framed, the Founding Fathers saw no need to explicitly spell out the right to a private conversation. That would have been silly. Two hundred years ago, all conversations were private. If someone else was within earshot, you could just go out behind the barn and have your conversation there. No one could listen in without your knowledge. The right to a private conversation was a natural right, not just in a philosophical sense, but in a law-of-physics sense, given the technology of the time.

But with the coming of the information age, starting with the invention of the telephone, all that has changed. Now most of our conversations are conducted electronically. This allows our most intimate conversations to be exposed without our knowledge. Cellular phone calls may be monitored by anyone with a radio. Electronic mail, sent across the Internet, is no more secure than cellular phone calls. Email is rapidly replacing postal mail, becoming the norm for everyone, not the novelty it was in the past.

Until recently, if the government wanted to violate the privacy of ordinary citizens, they had to expend a certain amount of expense and labor to intercept and steam open and read paper mail. Or they had to listen to and possibly transcribe spoken telephone conversation, at least before automatic voice recognition technology became available. This kind of labor-intensive monitoring was not practical on a large scale. It was only done in important cases when it seemed worthwhile. This is like catching one fish at a time, with a hook and line. Today, email can be routinely and automatically scanned for interesting keywords, on a vast scale, without detection. This is like driftnet fishing. And exponential growth in computer power is making the same thing possible with voice traffic.

Perhaps you think your email is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? If you hide your mail inside envelopes, does that mean you must be a subversive or a drug dealer, or maybe a paranoid nut? Do law-abiding citizens have any need to encrypt their email?

What if everyone believed that law-abiding citizens should use postcards for their mail? If a nonconformist tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world because everyone protects most of their mail with envelopes.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

So, no one draws suspicion by asserting their privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their email, innocent or not, so that no one drew suspicion by asserting their email privacy with encryption. Think of it as a form of solidarity."

Full article.

The Bank Secrecy Act of 1970

As the timeline below illustrates, The Bank Secrecy Act of 1970 has flourished and evolved over the last fifty years as technological advances have made it easier to track and collect private citizens' financial information.

An entire industry has developed around providing software to analyse transactions to identify transactions or patterns of transactions which requires Suspicious Activity Report (SAR) filing. Financial institutions are subject to penalties for failing to properly file Currency Transaction Reports (CTRs) and SARs, such as heavy fines and regulatory restrictions, including charter revocation.

These Anti Money Laundering software applications effectively monitor customer transactions daily and, using a customer's past transactions and account profile, provide a "whole picture" of the customer to the bank management.

"The Bank Secrecy Act of 1970 (BSA) requires financial institutions to assist federal agencies in detecting and preventing money laundering and other crimes. It now forms the basis of a costly and extensive regulatory framework that forces private financial companies to act as law enforcement agents. The evidence shows that this regulatory framework has not appreciably reduced criminal activity. It has, however, placed major burdens on law-abiding Americans, including weakening their constitutional rights."

Source - Cato

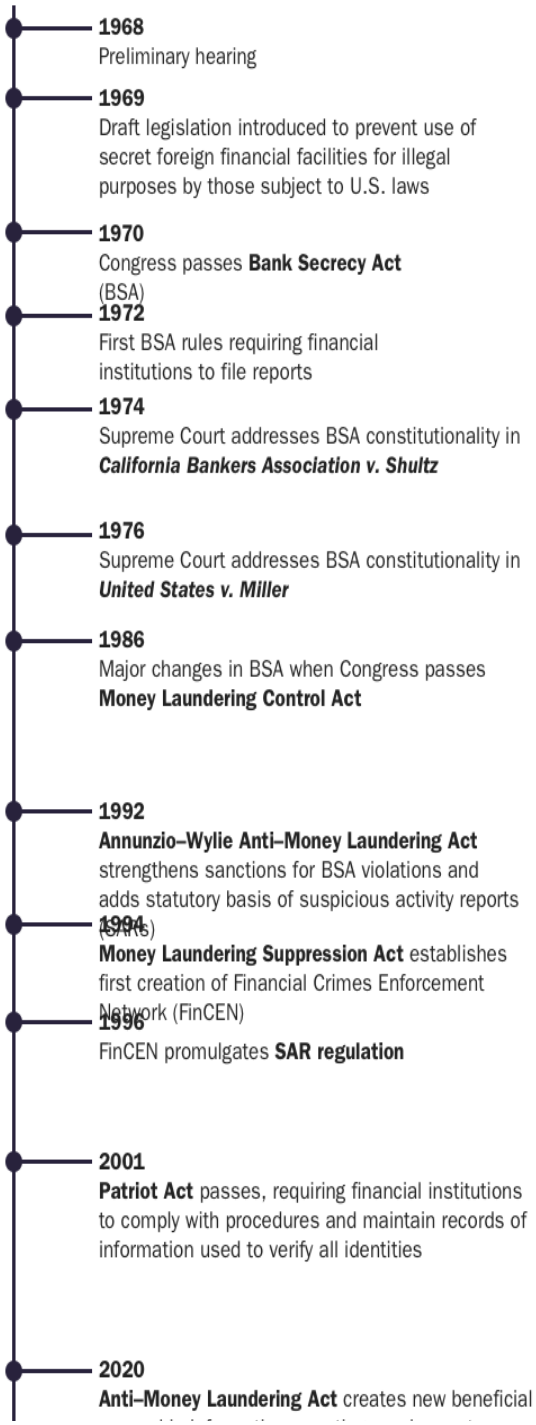
It's worth remembering that North Korea has been involved in financial crimes before Tornado Cash was developed and the challenges this has presented for federal regulators themselves. They are reportedly one of the world's major counterfeiters of US notes that are widely used and are largely impossible to trace.

"Other incidents show how difficult it can be to detect criminal activity and that federal regulators are themselves vulnerable to criminals. For example, in 2016, North Korean hackers broke into the SWIFT messaging network, stealing almost $100 million from the Bank of Bangladesh by routing it into private accounts through the Federal Reserve Bank of New York. Had it not been for a fluke occurrence, the thieves would have tricked the New York Fed into routing them nearly $1 billion from the Bank of Bangladesh. Similarly, the U.S. federal government has proven itself to be far from immune to cybercrime in recent years, and the SARs database itself contains a wealth of information that could be attractive to hackers or other criminals. On these grounds alone, it makes sense to avoid creating these data-rich targets inside federal agencies.

Source: Cato

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Figure
Timeline of Bank Secrecy Act, 1968–2020



Privacy Versus Secrecy

One of the far-reaching consequences of the technological revolution in terms of computing, the internet and smart phones is that we have almost given up our private information by accident. As companies tried to figure out how to profit from providing useful products and services to consumers on the internet, they discovered that the only business model which scaled successfully was advertising. We give away our locations (GPS) likes and dislikes (hovering a mouse pointer over an image / link / search) all for free and designed to create an emotional response. This business model has led to a concentration of surveillance capitalism in the likes of Google and Facebook which has proved to be extremely effective at generating outsized profit. Throughout this period, various governments around the world have seen the opportunities having this data can bring to be able to monitor and control their citizens. This has been enabled by centralized databases. This realization led to calls for better legislation in many countries around the world to protect our personal and financial privacy.

With this context in mind, when the bitcoin blockchain arrived on the scene in 2009, its radical transparency must have been confronting to people looking for more privacy, not less, in their financial transactions. Every transaction on the Bitcoin blockchain ever done is there for all to see. This is the same on the Ethereum blockchain. While these wallets are somewhat anonymous, we are learning that individuals can be linked to those addresses.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Here's an interesting quote from Zooko Wilcox-O'Hearn, founder of privacy coin, Zcash and a self-proclaimed cypherpunk as to why the open transparency of the Bitcoin blockchain came into being:

"And the only reason it's there is because Satoshi couldn't figure out how to include the privacy that he wanted to include in the first version of Bitcoin. From that point forward, nobody could figure out how to make Bitcoin private. And in 2010, Satoshi and some other folks had a conversation about this on the Bitcoin talk forum, where somebody suggested we could add encryption into Bitcoin, if only we had zero-knowledge proofs. And they looked into that, and Satoshi said something, and I really like the way he phrased it — I really admire Satoshi in so many ways. And one of them was he phrased it in terms of user experience for norms, that's how we talked about it. He said 'yeah, if we could figure out how to use zero-knowledge proofs, we could make a much more usable, easier version of Bitcoin'. But they couldn't, the zero-knowledge proofs in 2010 weren't scientifically mature enough. So, they looked at it, they studied it, and they said 'no, it won't work'. And then, about four months after that, Satoshi disappeared from the internet forever"

Source: The Defiant podcast 2nd Sept 2022

So, it appears that the ability to have private transactions on blockchains was always the intention. It's just that a key piece of cryptography known as zero knowledge proofs wasn't sufficiently developed at the time to incorporate it.

Hopefully by now, we have provided some background on privacy. Our legal rights to it, enshrined in the US constitution and similarly in many other democracies.

We have seen that thanks to open-source cryptography, despite governments trying to suppress its proliferation, our privacy in written electronic communications has been preserved.

We have also seen that the digital revolution has allowed for the proliferation of our private personal and private financial data to be given up to private corporations including financial institutions and subsequently to governments via legislation introduced over the past 50 years, particularly through the Bank Secrecy Act from 1970.

And finally, we covered the bitcoin blockchain which was released with an open and transparent format without a privacy feature. While this privacy feature was desired for inclusion initially, the technology at the time wasn't sufficiently developed to be included in the original bitcoin source code. Even the Ethereum blockchain , released roughly six years later, in-built privacy was not a feature of either.

This almost brings us to Tornado Cash. Well nearly. But first it is probably worthwhile having a small refresher on the Ethereum blockchain and smart contracts.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Ethereum blockchain

Ethereum is a cooperatively-run, global, transparent database. Through mutual effort, participants from all over the world maintain Ethereum's public record of addresses, which reference both user accounts and smart contract applications. These records work together much like the user accounts and software of a modern desktop computer, except that Ethereum is:

- Cooperatively-run: Ethereum's fundamental operation comes from the collective effort of its participants worldwide. No single party can make changes to how Ethereum works
- Publicly accessible: Anyone anywhere in the world can interact with Ethereum, its users, and its applications.
- Transparent: Anyone anywhere in the world can download and view all the information in Ethereum's database.

Features:

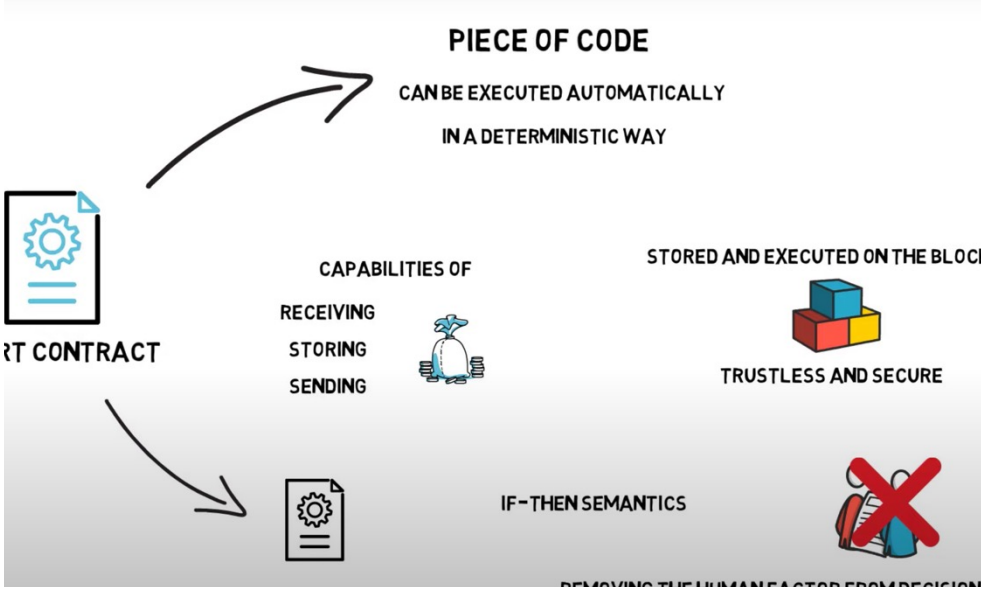
- Access to anyone with an internet connection – no need for a phone number, email, or physical address.
- You download a "wallet," - which generates a unique identifier or an "address" and a password-like number for authentication called a "private key."
- No limit to Wallets – each one is a participant in a global computing system running on open-source software, each wallet or Ethereum address is unique and unconnected.
- No-one owns this network – it functions without third-party oversight.
- Sharing your address – Users are able to receive tokens (e.g. crypto-assets like Ether) from anyone simply by sharing an address. Unlike a traditional payment service, sending and receiving tokens on Ethereum does not require an intermediary.
- The process of transfer – a series of messages - the sender broadcasts their intent to transfer tokens, signs their message mathematically using the private key, and Ethereum's network collectively updates the global records of the sender and receiver addresses with the new balances.

Unlike traditional finance, Ethereum's records are completely transparent, and no centralized party owns or keeps them: anyone can download and view the balances and transaction history of its user accounts. Although user addresses are pseudonymous, if a real-world identity is linked to a user address, it becomes possible to trace that user's complete financial history. Ethereum's transparency is important for auditability (e.g. verifying that updates to records are valid). However, this transparency also makes it difficult for users to protect their personal information. By default, a record of a casual transaction today (e.g., paying for Wi-Fi at the airport) leads directly to records of earlier transactions, which may include any intimate, revealing, or sensitive transactions made by the same user long ago.

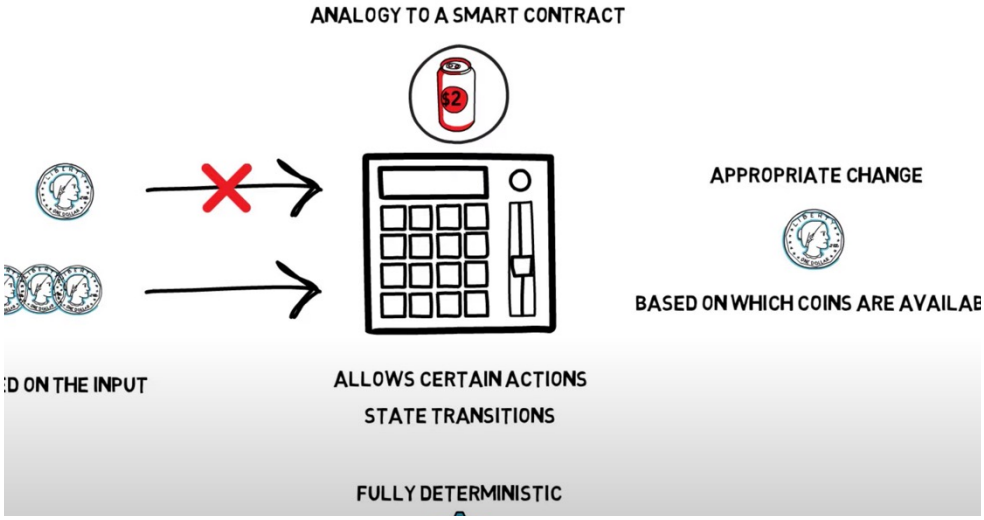
WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Smart Contracts

Tornado cash is its self a Smart Contract and as such a quick review of what they are and how they work below. Smart contarcts in Diagrams...

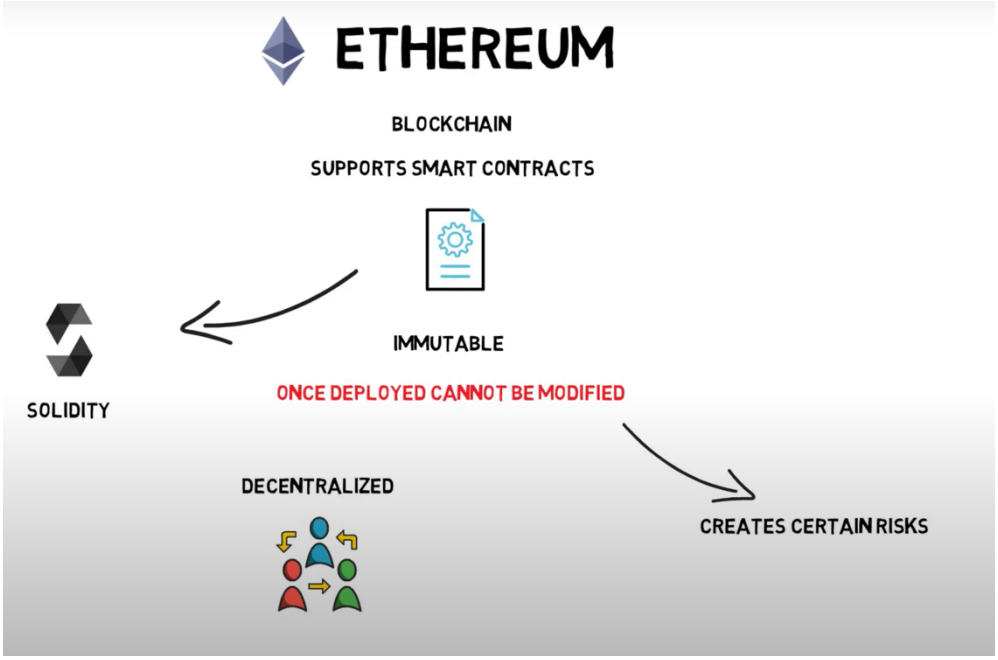


Vending Machine A real-world analogy of how a smart contract works



WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Ethereum is the most popular smart contract platform..



The Pros and Cons of Smart Contracts

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

When developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network. Once a smart contract's code is added to Ethereum's records, it receives a unique address and can be interacted with by any user to automatically carry out the rules and operations it supports.

In essence, smart contracts are open-source applications that anyone can deploy to Ethereum. Just like the rest of Ethereum, smart contracts can be viewed and used by anyone, anywhere, and without relying on an intermediary. When interacting with a protocol or Smart contract the rules and operations written in the smart contract code control the tokens.

By default, smart contracts are immutable, which means they cannot be removed or updated by anyone once deployed.

While there many different applications smart contracts may support, one of the more interesting uses is to provide an avenue for users to regain the privacy they expect when interacting with financial systems. Central to that privacy is the use of smart contracts to break the public chain of records that would otherwise link your transaction today to every transaction you've ever made in the past.

Tornado Cash: A smart contract application

Tornado Cash is an open-source software project that provides privacy protection for Ethereum's users. Like many such projects, the name does not refer to a legal entity, but to several open-source software libraries that have been developed over many years by a diverse group of contributors. These contributors have published and made Tornado Cash available for general use as a collection of smart contracts on the Ethereum blockchain.

The core of Tornado Cash's privacy tools is known as Tornado Cash Pools. Each Tornado Cash pool is a smart contract deployed to Ethereum. Like other smart contracts, the pool contracts extend the functionality of Ethereum with specific operations that can be executed by any user of Ethereum according to the rules defined in the Tornado Cash contracts' code.

This section will describe how these pools work. It will describe the key innovation that enables these pools to function autonomously: an application of privacy-preserving mathematics known as "zero-knowledge cryptography."

For some more detailed explanations of the mathematics and the computer science involved in creating and using zero knowledge proofs, we have included some links to videos and articles below.

Aa great, simplified explanation (with pictures) of how a zero knowledge proof works. Cossack Labs. Zero Knowledge Proof:

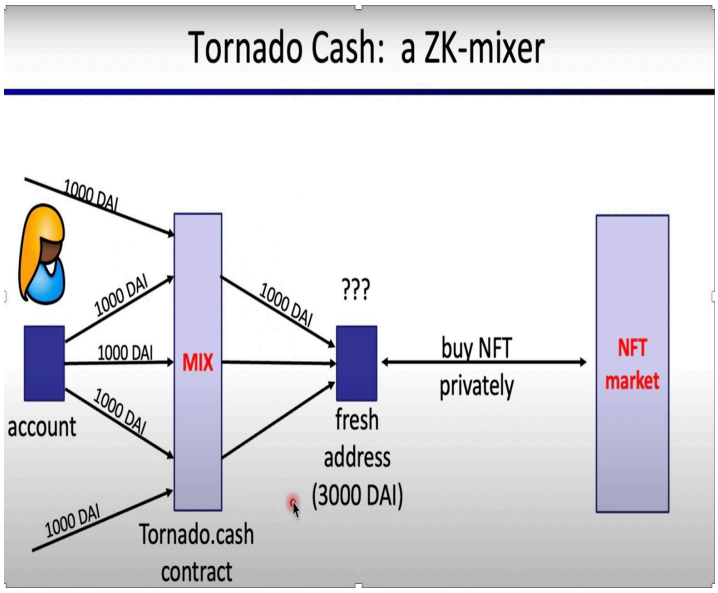
WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Tornado Cash pools are smart contracts that enable users to transact privately on Ethereum. When prompted by a user, pools will automatically carry out one of two supported operations: "deposit" or "withdraw." Together, these operations allow a user to deposit tokens from one address and later withdraw those same tokens to a different address. Crucially, even though these deposit and withdrawal events occur publicly on Ethereum's transparent ledger, any public link between the deposit and withdrawal addresses is severed. The user can withdraw and use their funds without fear of exposing their entire financial history to third parties.

In support of the deposit and withdrawal operations, these smart contracts encode strict rules that further define its functionality. These rules are automatically applied to the deposit and withdrawal operations to maintain a very important property shared by all Tornado Cash pools: users can only withdraw the specific tokens they originally deposited.

This property is enforced automatically for all the pool's operations and ensures that Tornado Cash pools are entirely non-custodial. That is, a user who deposits and later withdraws tokens maintains total ownership and control over their tokens, even as they pass through the pool. At no point is the user required to relinquish control of their tokens to anyone.

A key principle of Tornado Cash pools is that a user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it wouldn't matter that the link between the user's deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank's safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes. By guaranteeing the property that users can only withdraw tokens they originally deposited, many users can simultaneously use these pools with the assurance that no-one else will receive their tokens.



WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

We hope all the above has given you an understanding of the basic functioning of the Tornado Cash open-source software running on the Ethereum blockchain. It provides a useful function for protecting users' financial privacy. With the advance of digital technology, governments have gained greater access into our private conversations and financial transactions. We've seen recently in the situation with the Canadian Truckers and how this information can be used by a government to harass individuals for expressing their support to a certain group in society that had fallen out of favour with their government.

While we wait for the legal challenges to play out, below is an extract from Coincenter.org and their thoughts around the key issue at play – a piece of software was put on a list used for individuals.

"To understand the legal issues at stake in OFAC's addition of the Tornado Cash smart contracts to the SDN List, it helps to first understand OFAC's addition of Blender.io to the same list in May. The press release announcing those sanctions stated:

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Blender.io (Blender), which is used by the Democratic People's Republic of Korea (DPRK) to support its malicious cyber activities and money-laundering of stolen virtual currency.

This announcement drew no objection from the cryptocurrency community. That's because it makes sense that OFAC would sanction Blender since it is a company or some like entity. That is, Blender is a person or group of persons (whether legally incorporated or not) that provides Bitcoin mixing services. Executive Order 13694, under whose authority the designation was made, defines "persons" subject to listing as "an individual or entity," and it defines "entity" as "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization," and Blender certainly qualifies. When you send funds to an address provided by Blender, the persons who run Blender take control of those coins. They then mix your coins with those of other customers and send an equivalent amount back to you minus a fee.

What's important to note here is that this entity is ultimately under the control of natural persons, whether they are identified or not. That is, there are human beings with agency who control what Blender the entity does. They can decide to continue to pursue the business or not, or change how they do business. When they receive coins, they can decide to send back mixed coins or not. They can choose to serve some customers and not others, etc.

This also means that when Blender is added to the SDN list, the individuals who run the mixer—who indeed are the Blender entity—can file a petition for removal from the SDN list."

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

Blender, because it is an entity that is ultimately under the control of certain individuals, has the ability to bring to OFAC's attention any number of facts or arguments that could cause the agency to remove it from the list, such as:

- t is actually a U.S. person and therefore not properly the subject of sanctions without due process
- It has changed its behavior and no longer engages in the sanctioned activity
- The designation was made in error for some reason
- The designation exceeds Treasury's statutory or constitutional authority for some reason

And if OFAC denies or does not respond to the petition, Blender can hire lawyers to represent it and challenge the designation in court. The bottom line is that Blender is a legal person, and these are all things a person can do.

With all that in mind, we can now consider Tornado Cash. The release announcing its addition to the SDN List uses essentially identical language to that employed for Blender:

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash, which has been used to launder more than $7 billion worth of virtual currency since its creation in 2019.1

In this case, however, the statement does not make sense, is unexpected, and the crypto community has been outraged by the designation. The reason is that Tornado Cash is not equivalent to Blender the way the press release implies because, unlike Blender, it can't be said that Tornado Cash is a person subject to sanctions.

With this nuanced distinction between persons and software in mind, the uproar from the cryptocurrency community should now make eminent sense. How can it be proper to add to the sanctions list not a person, or a person's property, but instead an automated protocol not under anyone's control?"

see here: Coincenter

The OFAC designation of the Tornado Cash contracts has already had ramifications for the crypto industry. An alleged Tornado Cash software developer, Alexy Pertsev was arrested in Holland and jailed for three months without charge on the accusation of facilitating money laundering through the now sanctioned crypto mixer. The parallels to Phil Zimmerman aren't lost on people in the space. Righty, Web3 developers worry that the arrest could damage open-source software developments, as other developers could also be held responsible for how their code is being used.

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

In summarising the events of the last 6 weeks, the industry has reached a point where negotiations regarding regulation have begun in earnest. In the US we have Treasury's stance Tornado Cash, the various comments from Mr Gensler on regulation and recommendations coming out as a result of Pres. Biden's Executive Order. In Australia Sen Andrew Bragg decided to act, releasing a draft bill is called the Digital Assets (Market Regulation) Bill 2022. He has opened consultation on the draft until October 31. There is a natural tension between those that want and are empowered to regulate and those that are of the libertarian bent. Common sense that dictates that we will end up in a balanced state, however the main variable remains time to reach that point. The fact that we are seeing regulation is indeed in our mind a good thing, something that galvanises a disparate Crypto industry and that as it moves towards resolution hopefully spurs the next stage of growth and adoption.

Bibliography:

Zero Knowledge Proof: Explain it Like I'm 5 (Halloween Edition) by@cossacklabs

Tornado Cash - How it Works | DeFi + Zero Knowledge Proof

https://youtu.be/z_cRicXX1jI

"Understanding Zero-Knowledge Proofs in 15 Mins through SNARK and STARK"

https://mirror.xyz/0x803a0261275d30C7Ab5EAA37F47fD044c5c633Bb/3ase7VgQwXePn8FBZf_4Gl2hsgg-Ks2SCITcM8QKmzw

DeFi MOOC Lecture 10: Privacy on the Blockchain

Lecture 10.3: What is a zk-SNARK?

https://youtu.be/gcKCW7CNu_M

DeFi MOOC Lecture 10: Privacy on the Blockchain

Lecture 10.5: Anonymous Payments

https://youtu.be/Z0s4W3UBxM8

WE THANK YOU FOR THE OPPORTUNITY TO STEWARD YOUR CAPITAL INTO THE FUTURE OF FINANCE

DISCLAIMER

Disclaimer

Fort Canning Asset Management Pty Ltd (CAR) is a corporate authorised representative of Boutique Capital Pty Ltd (BCPL) AFSL 508011, CAR Number 1284461. CAR is an investment manager of the fund(s) described elsewhere in this document, or in other documentation (Fund).

To the extent to which this document contains advice it is general advice only and has been prepared by the CAR for individuals identified as wholesale investors for the purposes of providing a financial product or financial service, under Section 761G or Section 761GA of the Corporations Act 2001 (Cth).

The information herein is presented in summary form and is therefore subject to qualification and further explanation. The information in this document is not intended to be relied upon as advice to investors or potential investors and has been prepared without taking into account personal investment objectives, financial circumstances or particular needs. Recipients of this document are advised to consult their own professional advisers about legal, tax, financial or other matters relevant to the suitability of this information.

The investment summarised in this document is subject to known and unknown risks, some of which are beyond the control of CAR and their directors, employees, advisers or agents. CAR does not guarantee any particular rate of return or the performance of the Fund, nor does CAR and its directors personally guarantee the repayment of capital or any particular tax treatment. Past performance is not indicative of future performance.

The materials contained herein represent a general summary of CAR's current portfolio construction approach. CAR is not constrained with respect to any investment decision making methodologies and may vary from them materially at its sole discretion and without prior notice to investors. Depending on market conditions and trends , CAR may pursue other objectives or strategies considered appropriate and in the best interest of portfolio performance.

There are risks involved in investing in the CAR's strategy. All investments carry some level of risk, and there is typically a direct relationship between risk and return. We describe what steps we take to mitigate risk (where possible) in the Fund's Information Memorandum. It is important to note that despite taking such steps, the CAR cannot mitigate risk completely.

This document was prepared as a private communication to clients and is not intended for public circulation or publication or for the use of any third party, without the approval of CAR. Whilst this report is based on information from sources which CAR considers reliable, its accuracy and completeness cannot be guaranteed. Data is not necessarily audited or independently verified. Any opinions reflect CAR's judgment at this date and are subject to change. CAR has no obligation to provide revised assessments in the event of changed circumstances. To the extent permitted by law, BCPL, CAR and their directors and employees do not accept any liability for the results of any actions taken or not taken on the basis of information in this report, or for any negligent misstatements, errors or omissions.

This Document is informational purposes only and is not a solicitation for units in the Fund. Application for units in the Fund can only be made via the Fund's Information Memorandum and Application Form.