CRYPTOMASTER

WORKBOOK 3

2023

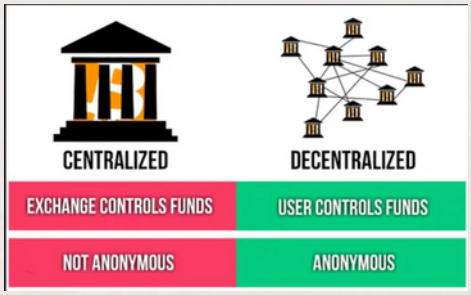
VOLITION LABS

SESSION 3

01 CUSTODIAL VS NON-CUSTODIAL WALLETS

Many crypto users have suffered losses as a result of not being in custody of their coins. This happens when a third party controls the keys to your crypto addresses, mostly through usage of custodial exchanges. These operate much as fiat banks where they are the central controller of your funds.

Custodial exchanges (CEX) such as Coinbase and Etoro are useful for on-ramping fiat to crypto (purchasing crypto with card, bank transfer or Paypal) or for performing live market trades between crypto currencies (Binance, Bitfinex) due to their high liquidity.



Criteria	CEX	DEX
Privacy	Not Anonymous: Personal Data	Anonymity
Liquidity	High Liquidity	Low Liquidity
Security	Exchange Hacks: 30 Hacks in the Last 9 Years	Secure
Sensorship	Government Bans, Regulations, and Shutdowns	No Shutdowns
Funds	Exchange Controls Funds	User Controls Funds

It is important to be able to clearly identify when you are in custody of your coins and when not.

Examples of centralized exchanges that have lost users' funds include Mt. Gox, one of the largest Bitcoin exchanges in the world until it suffered a massive security breach in 2014, loosing around over $450 million in Bitcoin at the time. More recently the FTX exchange that lost over $8bn of its customers' money.

To ensure you are in custody of your crypto it is important to use non-custodial wallets to hold your digital assets. Examples of these are Edge and Exodus wallets.

SESSION 3

A downside to custodial wallets is that they do not always provide a way to purchase crypto with fiat or to offboard your crypto back to fiat. Decentralized exchanges (DEXes) allow for trading between cryptocurrencies only.

02 HOT VS COLD WALLETS

Hot wallets refer to wallets that connect to the internet, in particular desktop or mobile phone wallets. While private keys are encrypted within the wallet, if large amounts of crypto funds are being stored, it is wise to move them into a cold wallet such as Tresor or Ledger to ensure the highest level of security.

Cold storage wallets are physical devices that keep the private keys to your crypto addresses offline and safe from malware and hackers. Transactions are made in the desktop application but signed offline by connecting your hardware wallet to your device. As with hot wallets, cold wallets are backed up by a seed phrase.

03 PRIVACY TOOLS

Although Bitcoin and other cryptocurrencies are recorded on transparent ledgers, a number of methods are available to ensure greater transaction privacy.

Using new crypto address every time a payment of crypto is received ensures no previous transaction history can be obtained. In wallets such as Exodus, this feature has to be manually activated. It is also important not to disclose your crypto holdings to any third party to avoid being a target for theft.

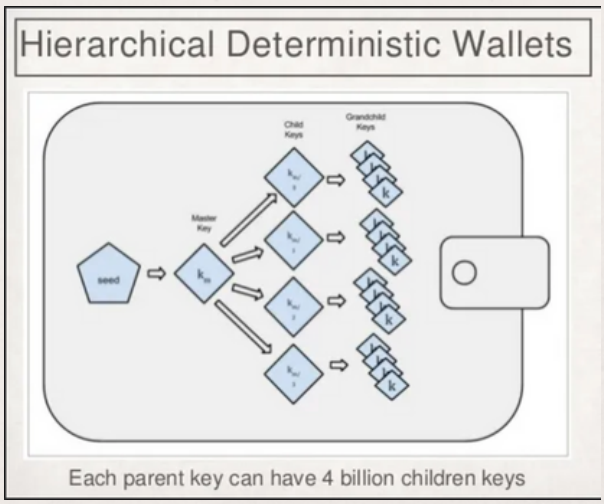
It is important also to ensure that your personal identity is not connected with any crypto wallet.

For greater privacy, privacy crypto such as Monero and Dero are solutions. When using Bitcoin, mixers or tumblers can be used.

SESSION 3

04 SECURING YOUR CRYPTO ASSETS

When using a custodial wallet such as Exodus or Ledger, it is essential to securely record your seed phrase off-line. Seed phrases are the result of the BIP32 Bitcoin Development Proposal that enables all subsequent private keys across all crypto- currencies held in that wallet to be repopulated should the wallet be corrupted, lost or access blocked.



The seed phrase is a random sequence of 12 or 24 words that is used to derive a master private key, which can then be used to generate a tree-like structure of sub-keys, each of which can be associated with a different bitcoin address.

While it is good operational practice to use a new address with each receipt of crypto, it is therefore not necessary to record each private key. These are managed for you by your wallet which is backed up by the seed phrase.

It is important to note that digital assets are held on the blockchain and not in the wallet. The wallet manages your private keys and constructs and sends your transactions to the network

SESSION 3

05 SECURE SEEDPHRASE BACK UP METHODS

The safest way to back up a seedphrase is to etch it into non-corrosive, fireproof metal and keep in a safe. A number of products exist on the market that make this efficient. Be sure to read reviews before purchasing.

Tresor cold storage wallet and Crypto Steel seedphrase storer

While there are many different methods for backing up your seedphrase, the method you choose needs to suit your lifestyle. Perpetual travellers might consider online encryption methods for storing seed phrases to give them access on the move. Splitting seedphrases is not considered a good practice.

A crypto user must also consider worst case scenarios, such as loss of memory, death and incapacity. In such a case it is important to make arrangements for next of kin or trusted parties to have access to the crypto holdings, such as via a lawyer, trustee or a will.

SESSION 3

06 PRIVACY COINS AND TUMBLERS

Privacy coins are a method of disguising the history of crypto usage. For instance Monero is designed to provide strong privacy protections for its users by using advanced cryptography to obscure transaction details such as the sender's address, recipient's address, and transaction amount.

Crypto usage can be obscured for instance by receiving Bitcoin to a wallet, exchanging it to Monero, then exchanging it back to Bitcoin to a new address.

Wallets such as Samourai and Sparrow utilise coin mixers or tumblers which aim to enhance the privacy and anonymity of cryptocurrency transactions by obfuscating the transaction history of the coins.

07 OPERATIONAL SECURITY (OPSEC)

Starting out in crypto is an appropriate time to conduct an audit of your current your OpSec (operational security) and assess where unnecessary data leakages might be occurring, such as through social media, unencrypted email, messaging platforms or non-private browsers.

While it may not be possible to achieve complete privacy and security, it is good practice to make surveillance difficult.

Suggested steps for improving your operations security include:
s

- Use a VPN such as Proton VPN (free) to obscure your IP when using the internet
- Have both public and private aliases to ensure your private crypto use stays private

SESSION 3

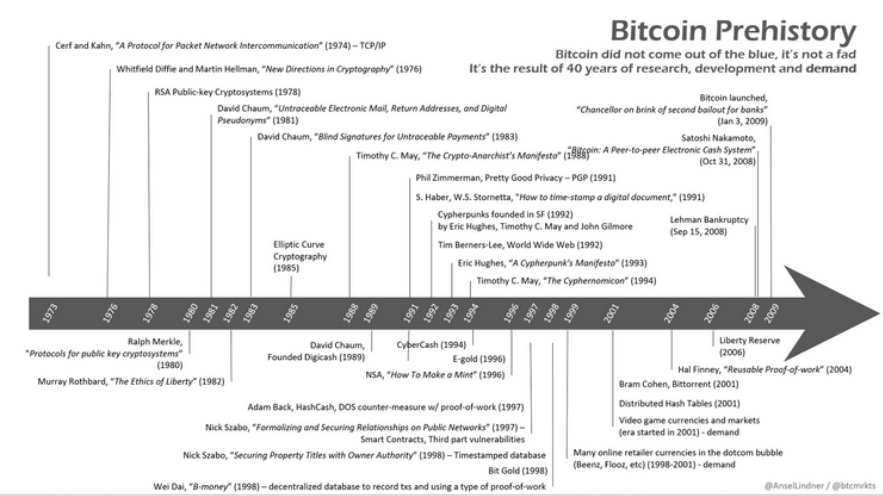
s

- Use encrypted email providers only (protonmail, tutanota)
- Use privacy-focussed browsers such as Brave or Tor browsers
- Use privacy-focussed communications platforms such as Signal (requires cell number) or Session (no cell number required).
- Keep sensitive information off your devices or securely encrypted.

To learn more about operational security watch Braxman on Tech and Privacy X for technical security tips. For examples of OpSec fails, listen to the Darknet Diaries.

08 THE CYPHERPUNKS & BITCOIN'S PREHISTORY

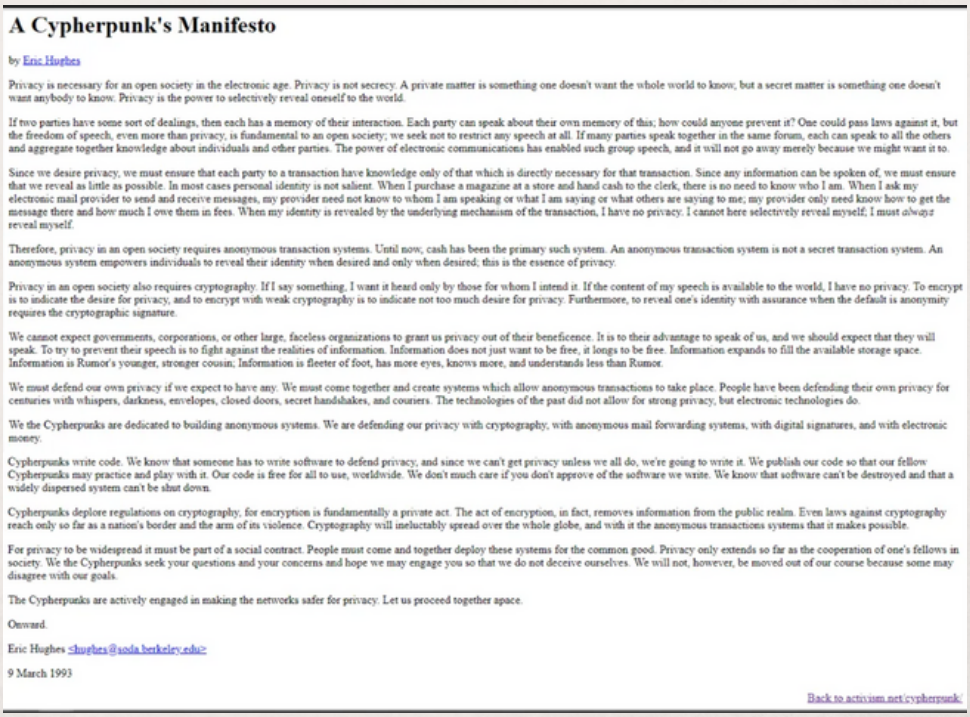
Bitcoin emerged off the back of a number of previous innovations made by a group of activists, academics and computer experts operating mainly in the 1980s and 1990s who advocated for strong cryptography and privacy-enhancing technologies as a means of achieving individual freedom and privacy in the digital age.



SESSION 3

The term "cypherpunk" was coined by Eric Hughes in his 1992 "Cypherpunk Manifesto," which outlined the group's core beliefs and values.

The manifesto called for the widespread use of cryptography to protect individual privacy, and for the development of tools and technologies that could enable anonymous communication and financial transactions.



A Cypherpunk's Manifesto

by Eric Hughes

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.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must *always* reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes <hughes@soda.berkeley.edu>

9 March 1993

Back to activism.net/cypherpunk/

The Cypherpunks have been influential in the development of various privacy-enhancing technologies, including PGP encryption, Tor, and Bitcoin.

Leading figures include:

1. Eric Hughes: Hughes is considered one of the founding members of the Cypherpunk movement. He authored "A Cypherpunk's Manifesto," which outlined the principles and goals of the movement.

SESSION 3

2. Timothy C. May: May was a significant figure in the Cypherpunk movement and co-founded the Cypherpunks mailing list in 1992. He contributed to discussions on various topics related to cryptography, privacy, and digital rights.

3. Whitfield Diffie: Diffie is a prominent cryptographer who, along with Martin Hellman, invented public-key cryptography, which is crucial for secure online communication. His work laid the foundation for the use of encryption technologies.

4. Phil Zimmermann: Zimmermann is best known as the creator of Pretty Good Privacy (PGP), a widely used email encryption software. PGP revolutionized secure communication for individuals and played a significant role in the advancement of the Cypherpunk movement.

5. David Chaum: An influential figure in the field of cryptography and privacy. Chaum is known for his work on cryptographic protocols, including the creation of the first digital currency called "eCash." His ideas and research have significantly influenced the development of privacy-enhancing technologies.

For more information on the cypherpunks visit the Volition Labs cypher punk resources page.