BINANCE RESEARCH

Wallets: A Deep Dive into Crypto Custody

January 2023

Mac Naggar

Table of Contents

Key Takeaways

- The mainstream adoption of blockchain technology is dependent on how user-friendly and safe crypto wallets are to use.
- Crypto custody is a rapidly evolving space and a topic of increased focus given industry events and an influx of new market participants into crypto over the past couple years.
- Understanding how an underlying wallet account works is critical to securing one's funds.
- Wallets rely on complex record-keeping, connective, and cryptographic processes to interact with the blockchain.
- Wallet options are differentiated by the unique ways in which they store private keys, connect to the internet, and sign transactions.
- Current wallet options face a tradeoff between convenience and security.
- There must be a range of different wallet options to meet the needs of a heterogeneous set of users in a decentralized system.
- Trends point to developers mitigating the convenience vs. security tradeoff and enhancing the functionality of current wallet options.

Introduction

2022 has been a watershed year in the crypto custody space.

Custodial carnage, security concerns about hacks, and widespread compromisation of private keys have led to an increased focus on crypto custody. Now more than ever, discussions around how to safely store, save, and hold your crypto are taking place.

Furthermore, the growing popularity of crypto and the greater prospects of widespread adoption have led many to question whether current custody solutions are really conducive to capturing a new, non-crypto native user base. Singapore-based blockchain firm TripleA, estimated that as of 2022, the global crypto ownership rate is only around 4.2%.[1] Increased investments and rapid developments are being made into creating more user-friendly ways of holding crypto and accessing the blockchain, all in hopes of ultimately capturing the next wave of users.

Meanwhile, within the current crypto industry, wallets already generate some revenue, with US$1.398B generated by wallets in 2022 alone.[2] In the custodial space, this revenue mainly arises from transaction, deposit and withdrawal fees. On the non-custodial side, this mainly arises from in-wallet swapping fees or shared revenue with dApps (payment made by dApp applications for wallet users interacting with their app). As innovations continue to accelerate in the custody space and wallet users expand, wallet earnings are expected to cross US$3 billion within the next decade.[2]

In this report, we provide a deep dive into the rapidly evolving crypto custody space. More specifically, we prime readers with an understanding of how wallets fundamentally work, then, we move into a comparison of the current crypto custody options, and ultimately end by highlighting future trends in the custody space. Given the complexity of some of the topics discussed, this report assumes a surface-level understanding of what crypto wallets are. A beginner's introduction to wallets can be found on Binance Academy here.

How Wallets Work

Contrary to popular belief, crypto wallets do not actually store or hold digital assets. Instead, digital assets are stored and recorded on the blockchain. Wallets, on the other hand, simply provide the tools required to interact with that blockchain, allowing the wallet user to do things like send funds or check account balances. Unfortunately, this is a widespread misconception and illustrates that many wallet users lack awareness of how their wallet actually works.

In this section, we provide a breakdown of how crypto wallets work and the infrastructure that wallets rely on to interact with blockchains. By understanding how wallets work, one will be able to understand the differences between available wallet options, and furthermore, identify potential elements to consider when using a wallet.

Record Keeping of Funds on Blockchains

Crypto wallets are unlike real-life wallets. With real-life wallets, you can check how much someone owns, by physically opening the wallet and counting the bills and coins that the wallet holds. **Crypto wallets, on the other hand, do not hold money, but rather are simply a reflection of how much money the user *should own* based on a blockchain's records.** Since blockchains maintain a continuous record of transactions between network participants, crypto wallets are able to utilize this information to reflect the balance of any respective user.

Interestingly, different blockchains have different means of record-keeping. Your crypto wallet relies on a blockchain's respective means of record-keeping to in turn, determine the digital assets you hold. Today, there exist **two main models that blockchains use to record the flow of digital assets:** (1) the **UTXO Model** and (2) the **Account-Based Model.**

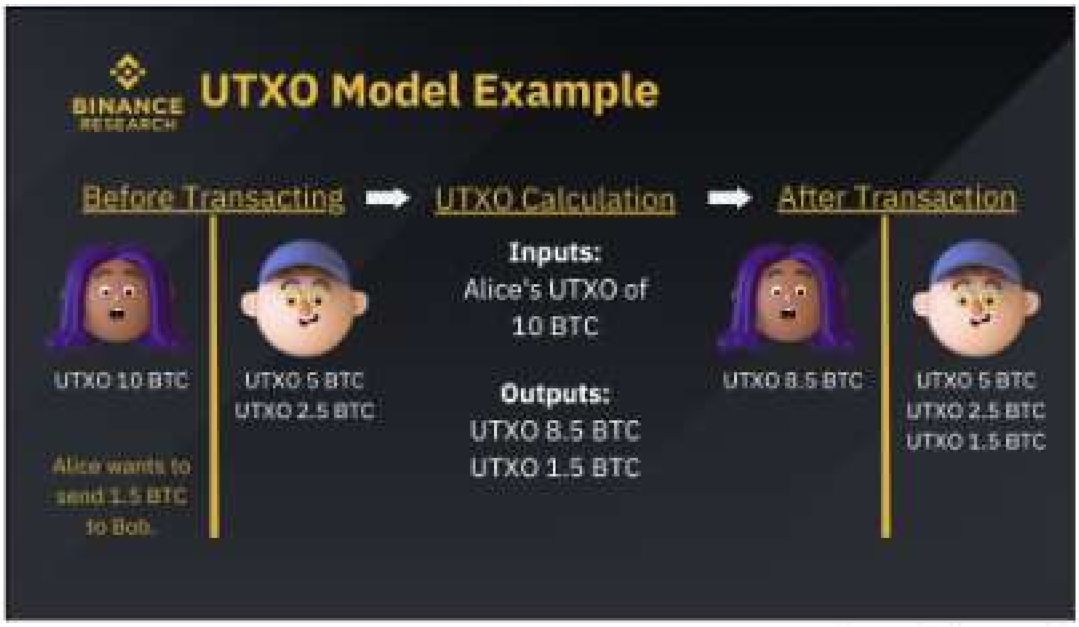
UTXO Model

The UTXO model is the original form of blockchain record-keeping and is used by Bitcoin and Bitcoin derivatives such as Zcash and Litecoin. UTXO is an acronym for "Unspent Transaction Output," a technical term used to refer to the amount of digital currency that remains unspent after committing a transaction. When someone transacts on a UTXO modeled blockchain, they are not actually sending/receiving any particular amount of digital currency, but rather are transacting in the denomination of UTXOs.

The way UTXOs work is best explained by an example. To set the stage, let's assume that Alice and Bob have both transacted on the Bitcoin blockchain before and have been left with UTXOs worth 10 BTC and 5 BTC + 2.5 BTC respectively. Now, suppose that Alice wants to send Bob

1.5 BTC. When Alice uses her wallet to interact with the blockchain, she will effectively be using her existing UTXOs (worth 10 BTC) as the sole input. The transaction will yield an output of UTXOs worth 1.5 BTC (the amount she is sending to Bob) and 8.5 BTC (the amount left over from her current UTXOs). Ultimately, after the transaction takes place, blockchain records will show that the cumulative amount of UTXOs Alice has over the life of her transactions on the blockchain is worth 8.5 BTC. Similarly, blockchain records will show that the cumulative amount of UTXOs Bob has over the life of his transactions is worth 5 BTC, 2.5 BTC, and 1.5 BTC.

Figure 1: An example of how UTXO record-keeping works



BINANCE RESEARCH UTXO Model Example

Before Transacting ➡ UTXO Calculation ➡ After Transaction

UTXO 10 BTC

Alice wants to send 1.5 BTC to Bob.

UTXO 5 BTC
UTXO 2.5 BTC

Inputs:
Alice's UTXO of 10 BTC

Outputs:
UTXO 8.5 BTC
UTXO 1.5 BTC

UTXO 8.5 BTC

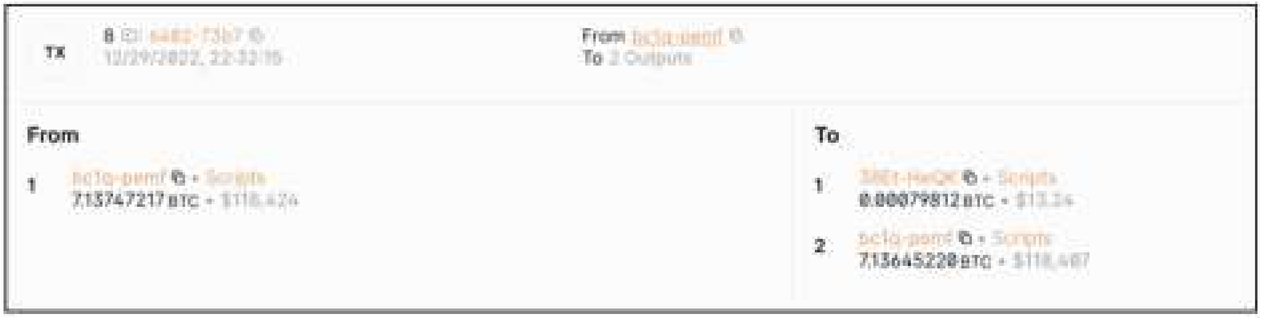
UTXO 5 BTC
UTXO 2.5 BTC
UTXO 1.5 BTC

Source: Binance Research

In our example, after transacting with Alice, Bob would see 9 BTC in his *Trust Wallet* which is the aggregation of his UTXOs worth 5 BTC, 2.5 BTC, and 1.5 BTC. **When you check your Bitcoin balance on *Trust Wallet* or another wallet, what you are looking at is the aggregation of the UTXOs.**

Post-transaction, each of Bob's UTXOs are recorded and sent to a new address on the blockchain. Often, users, after they have spent some BTC, will notice on block explorers that their remaining balance of BTC was sent to a wallet address they do not recognize. In turn, they may fear that they have lost their remaining change. However, it is important to note that UTXOs, even though they are sent to a new address, are often tagged by your wallet to your main address. Thus, as long as your digital wallet has taken care of handling the new addressing and aggregating the UTXOs (most do), there is nothing to worry about, your change will return to the main address from which you transacted from.

Figure 2: Example of UTXO which is sent to a new address



TX

8 ID: 6482-73b7
12/29/2022, 22:32:15

From bc1q-pemf
To 2 Outputs

From

1 bc1q-pemf • Scripts
7.13747217 BTC • $118,424

To

1 3BEt-HeQK • Scripts
0.00079812 BTC • $13.24

2 bc1q-pemf • Scripts
7.13645228 BTC • $118,487

Source: Binance Research, Blockchain.com Bitcoin Explorer

To remember how the UTXO model works, it is helpful to think of the model as being similar to receiving change after paying in cash. If someone has a $10 bill and that person needs to pay $4 to another person, they will receive back a single $5 bill and a single $1 bill. The $5 bill and the $1 bill in this example are UTXOs. The $5 and $1 UTXOs can then be used to pay for subsequent transactions. The only difference between cash change and UTXOs, is that cash has specific denominations, whereas UTXOs can have fractional values (eg. UTXO worth 2.5 BTC). Furthermore, each time you receive and transact from your cash change, it is not recorded. In contrast, the record of UTXOs are cemented in the history of the blockchain ledger. An account balance can be derived at any moment in time by following the recorded UTXOs of a particular address.

The UTXO model has positive and negative implications for Bitcoin based wallets. On one hand, the UTXO model encourages privacy preserving behavior, as it is near impossible to definitely link digital assets to a particular wallet (as new addresses are created each time there is UTXO). On the other hand, UI/UX considerations are tricky. We tend to associate the concept of money with accounts. However, since there is no concept of an account in the UTXO model, a user must rely on their wallet provider to manage a diverse set of addresses and sum up the corresponding UTXO balances.

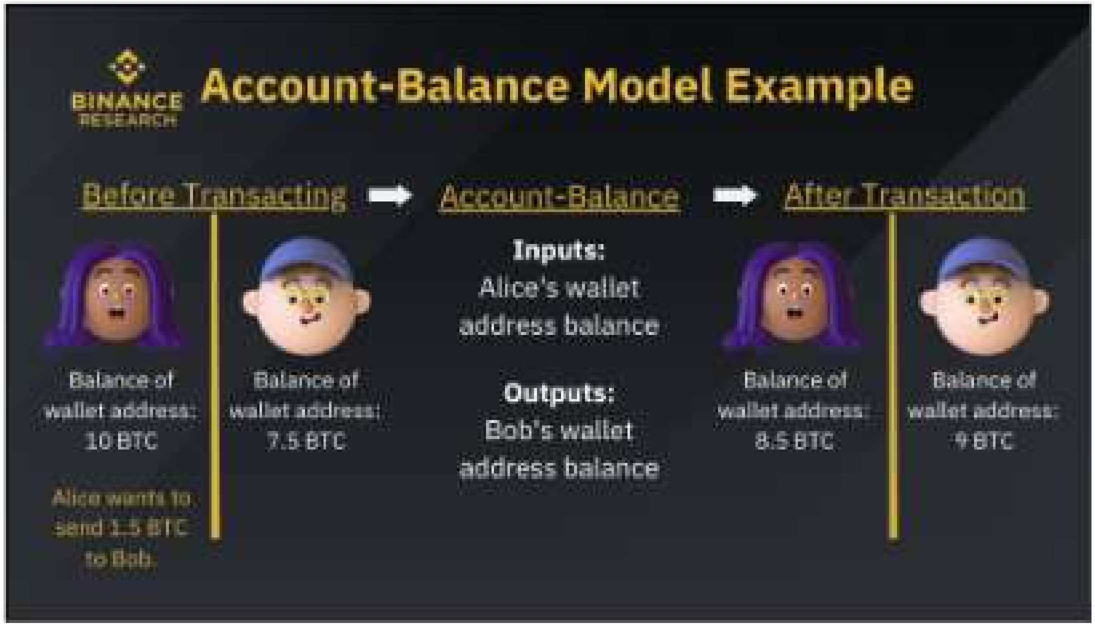
Account-Balance Model

The Account-Balance model is another form of blockchain record-keeping that is primarily used by smart contract platforms, such as Ethereum and BNB Chain. This model arose out of frustration, after Ethereum developers struggled to conform the accounts of dApps to the privacy-preserving, disconnected logic of the UTXO model.

While the UTXO model's means of accounting resembles that of cash, the Account-Balance model's means of accounting resembles that of a bank. On smart contract platforms, each wallet address has a singular balance, which is added to or subtracted from depending on if the user receives funds or sends funds from their wallet.

In the Alice and Bob example, the record-keeping of funds is much simpler as compared to that of the UTXO model. Prior to transacting, Alice and Bob's BTC are recorded in the state of the blockchain as a balance. When Alice sends 1.5 BTC, the transaction implies that 1.5 BTC is simply removed from Alice's balance and added to Bob's balance. Post transaction, there is no dispersed UTXOs, but rather one coherent account balance (8.5 BTC for Alice, and 9 BTC for Bob).

Figure 3: An example of how Account-Balance record-keeping works



Account-Balance Model Example

Before Transacting

Balance of wallet address: 10 BTC

Alice wants to send 1.5 BTC to Bob.

Balance of wallet address: 7.5 BTC

Account-Balance

Inputs:
Alice's wallet address balance

Outputs:
Bob's wallet address balance

After Transaction

Balance of wallet address: 8.5 BTC

Balance of wallet address: 9 BTC

Source: Binance Research

While the Account-Balance model allows wallets to derive account balances in a much more simplistic and efficient manner as compared to the UTXO model, it should be noted that outside of wallet implications, Account-Balance models are more susceptible to double spending attacks as compared to the UTXO model.

Overall, the record-keeping model that a blockchain employs is important because it directly influences how a crypto wallet derives digital asset holdings. If a wallet is unable to correctly conform to the blockchain's mode of record-keeping, then the wallet is not viable. For example, if a Bitcoin-based wallet provider is unable to meet the complexity of the UTXO model and track all the new addresses associated with UTXOs, then it will result in perceived loss of funds for the wallet user.

Infrastructure to Interact with Blockchain Records

Now that we understand how blockchains record-keep how much digital currency each particular user has, we now need to understand how wallets actually source this data from the blockchain to do things like check an account balance or send funds.

Source of Blockchain Data

As described above in the record-keeping section, wallets utilize blockchain records to determine how much digital currency a user holds. **To source data from a blockchain, current wallets rely on a "remote client". Remote clients (which run alongside a blockchain API) allow wallets access to the data of a blockchain, without having to store the entirety of the blockchain data itself.** Remote clients can be contrasted with "full nodes", which store the entirety of the blockchain data.

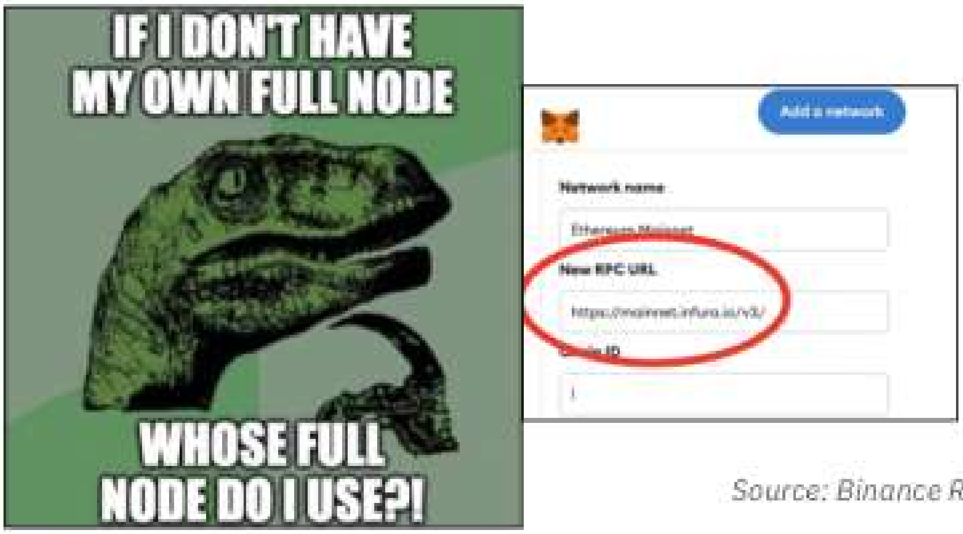
The first ever wallet, created by Satoshi Nakamoto, was a full node. The so-called "Bitcoin-qt" wallet required users to download the entire Blockchian history for the wallet to sync. In the early days of blockchains, this was not a huge issue, since the entirety of the blockchain did not have much of a history and thus, did not require much data to download.

Figure 4: The first crypto wallet, Bitcoin-qt's user interface

Source: Bitcoin.com

Reviewing the "Bitcoin-qt" in 2012, Vitalik Buterin wrote in a Bitcoin Magazine post "*Because it is a full node, the client must download the entire (currently 6 GB) blockchain to operate, which can take up to a few days the first time you start the client and several minutes to an hour every time you start the client afterward if you do not keep it running constantly.*" Since 2012, the Bitcoin blockchain has inevitably gotten larger. At the time of writing, the Bitcoin blockchain exceeds 442 GB. As a result, to run a full node today is not only expensive but also technically difficult, as it requires personalized hardware to meet the data needs of the blockchain's large size. This makes it infeasible for an average wallet user to run a full node, just to check an account or a past transaction. Instead, the average wallet user relies on a remote client to source blockchain data.

Figure 5: If remote clients do not store blockchain data like full nodes, where do they source blockchain data from?



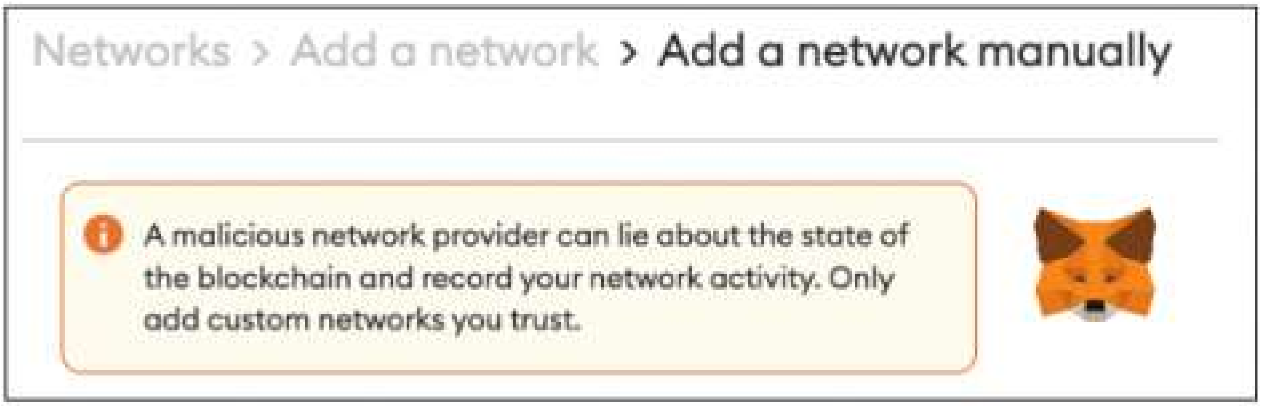
Network name
Ethereum Mainnet
New RPC URL
https://mainnet.infura.io/v3/
Chain ID
1

Source: Binance Research

If wallets rely on remote clients to source data but remote clients do not store blockchain data themselves, then where do remote clients gather data from? Remote clients gather data through a remote procedure call ("RPC"), which is a connection to a node that is synced with the blockchain. The RPC call can be made to a full node you run yourself, but is more likely to a full node outsourced from a node-provider such as Alchemy or Infura, who handle data-intensive, technically-complex and costly nature of running a full node for you. **In this way, node providers allow remote clients and the average wallet user, who does not run a full node, to connect to one of their full nodes and access the entirety of blockchain data.**

Over the past couple months, specific node providers have faced criticism for being centralized and collecting the IP addresses of the wallets that made RPC calls. Critics have deemed node providers as being antithetical to the decentralized ethos of blockchain technology. As a result, many wallet users have sought out ways to avoid node providers, with some even going as far to set up their own full nodes. While it may not be economically or technically feasible for everyone to set up their own full node, it is important to understand how your wallet connects to the blockchain, because otherwise, if you are connected to a malicious network provider, your wallet/network activity can be monitored and exploited.

Figure 6: Metamask advises users to understand how they are connecting to the blockchain as network providers could be malicious



Networks > Add a network > Add a network manually

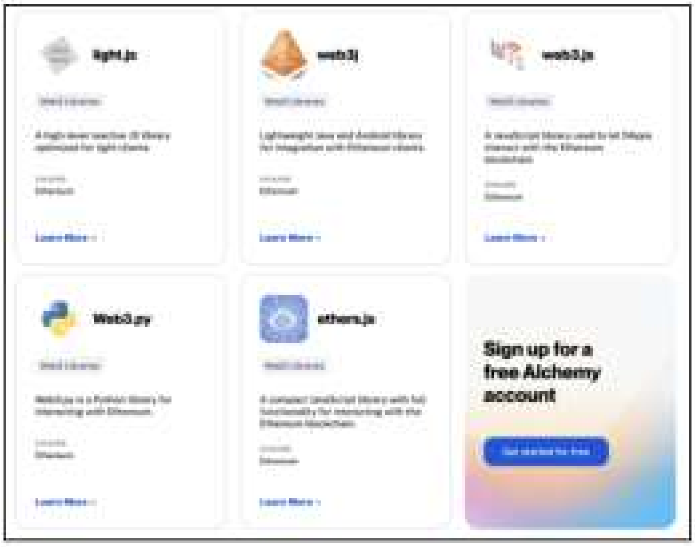
A malicious network provider can lie about the state of the blockchain and record your network activity. Only add custom networks you trust.

Source: Binance Research

- **Interacting with blockchain Data**

If your wallet is a full node or has a node provider that it can connect to, then it can begin to interact with the blockchain. By clicking a button on your wallet front-end, you can send requests to your blockchain node to do things like query the blockchain for gas estimates, send transactions, sign transactions, and call smart contracts. **The backends of most wallets utilize language-specific APIs to make these method requests to interact with the blockchain node they are connected to. For example, on the EVM, popular language specific API libraries include Ethers.js (JavaScript based), Web3.js (JavaScript based), and Web3.py (Python based).**

Figure 7: Wallet backends use language-specific API libraries to make calls to the blockchain



light.js

Web3 Libraries

A high-level reactive JS library optimized for light clients.

Ecosystem

Ethereum

Learn More →

web3j

Web3 Libraries

Lightweight Java and Android library for integration with Ethereum clients.

Ecosystem

Ethereum

Learn More →

web3.js

Web3 Libraries

A JavaScript library used to let DApps interact with the Ethereum blockchain.

Ecosystem

Ethereum

Learn More →

Web3.py

Web3 Libraries

Web3.py is a Python library for interacting with Ethereum.

Ecosystem

Ethereum

Learn More →

ethers.js

Web3 Libraries

A compact JavaScript library with full functionality for interacting with the Ethereum blockchain.

Ecosystem

Ethereum

Learn More →

Sign up for a free Alchemy account

Get started for free

Source: Binance Research, Alchemy

To summarize, the way your wallet sources data and interacts with the blockchain is something we do not commonly think about when we make an NFT purchase or token swap. However, understanding operational infrastructure is incredibly important. **The operational infrastructure of wallets dictates the user experience - it determines if you are contributing to a centralized or a decentralized system, and it is the direct determinant of proper order routing or alternatively, a cyberattack.** Thus, wallet users should have some understanding of the operational infrastructure behind their wallets, even if it is ultimately abstracted away.

Cryptographic Protections

The "crypto" component of the term "cryptocurrency" stands for "cryptography." Cryptography is the study of protecting information and communications through the use of codes. The secure, decentralized, and fraud-proof nature of blockchain technology is a direct result of its implementation of cryptographic practices. In fact, blockchains use cryptography for various security purposes. Perhaps, the most notable use case of cryptography in the blockchain space is within crypto wallets. **Cryptographic methods and principles are employed to both (1) creating crypto wallet key pairs and (2) authentically signing transactions on the blockchain.**

Creating Crypto Wallet Key Pairs

As iterated previously, wallets do not actually hold cryptocurrency. What wallets do store however, is a user's access to interact with the blockchain, enabling them to do things like send and manage their digital currency holdings. More specifically, wallets store 'private keys,' which unlocks the use of funds on a blockchain account and furthermore, allows the private-key holder to transact.

The concept of 'private keys' arises from the field of Cryptography. More specifically, "Asymmetric Encryption Cryptography" (otherwise known as "Public-Key Cryptography") concerns the use of two different "keys" (a public key and a private key) to secure a wallet's data and access. The public and private key work together to provide a public-facing means for transacting, while still, maintaining a private means of verifying transactions. You can think about the public key of your wallet as being analogous to a bank account number. Alternatively, you can think about the private key of your wallet as being analogous to your bank account's PIN number. The bank account number (public-key) is how you reference your prospective transactions, your bank pin (private-key) is how you access your account's data and sign off on transactions.

It is clear then, that the security and privacy of your private key is of the utmost importance. If your private key falls into the wrong hands, is forgotten, or is lost, then access to your wallet account is compromised. There are many resources online that provide advice on how to protect your private key *once you already have it*, such as CZ's Keep your Crypto #SAFU tips.

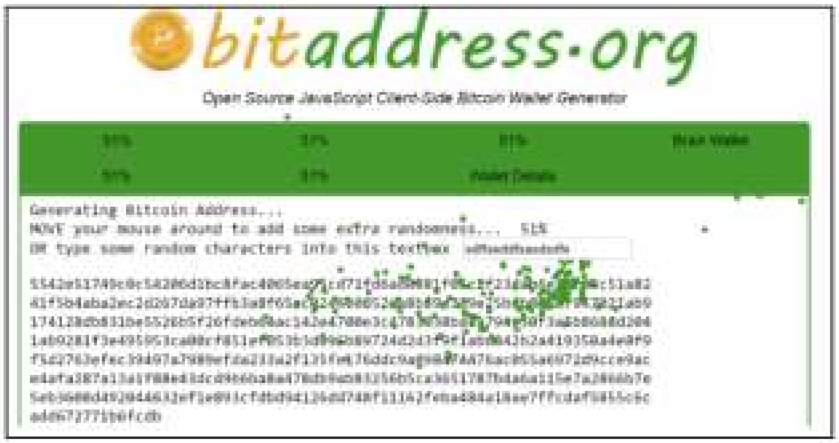
But what if your private key is compromised *before you already have it?* This begs the following questions: How is the key-pair of your wallet generated? What are the security implications around the generation of keys and the security of your wallet?

To answer these questions, we need to understand the process of how private and public keys are generated.

1. First, your private key is generated through some sort of random number generator

Many modern wallets, such as Metamask, automatically create a random number for a private key. This involves Metamask using an internet browser function called "Crypto.getRandomValues" to derive a random number. However, other wallets allow for more control over the random number generation process. For example, some wallets allow you to manually derive a random number, based on some act of randomness, such as the wiggle of your mouse or based on the soundwaves of you talking into your computer's microphone. This random number is allowed to be any number within 256-bits (or between 1 and 2^{256}), an incredibly large range. Ultimately, this random number serves as your private key.

Figure 8: Private key random number generated by random mouse movements



```
Generating Bitcoin Address...
MOVE your mouse around to add some extra randomness...   51%
OR type some random characters into this textbox
[illegible]
```

Source: Binance Research, bitaddress.org

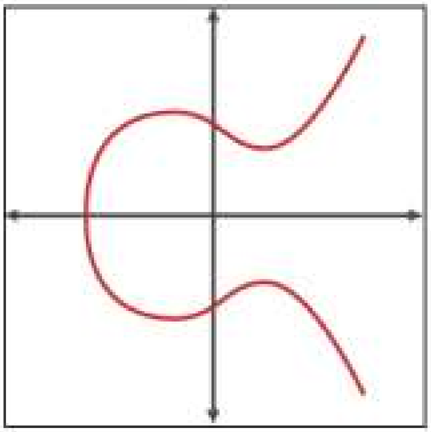
If you have used a wallet before, you may not be familiar with any particular number representing your private key, but instead, you are probably familiar with a "seed phrase." A seed phrase is a sequence of random words that is actually your private key's random number mapped to a set of words. In this way, the seed phrase is a reflection of your private key, and serves as an abstraction away from the random number.

2. The random number representing your private key is then injected into a cryptographic algorithm to derive your public key

After a private key has been generated either automatically manually, the private key is then used to generate the public key. More specifically, the private key is injected into a blockchain's cryptographic algorithm called an "Elliptic Curve Algorithm," which involves taking a starting point on an elliptic curve (known as a generator point) and multiplying it by the random private key number to produce a new point on the curve. The specific x and y coordinates of the resulting point becomes representative of the public key.

The reason for using this complex cryptographic method to create a wallet account is so that your public key cannot be reverse engineered to your private key. In fact, finding the private key while knowing the public key is almost impossible because of how difficult it would be to retrace to the private key number. Theoretically speaking, it would take a quantum computer more than 13 million physical cubits to reverse engineer your private key from your public key. To date, one of the world's most advanced quantum computers, the IBM Eagle processor, possesses only 127 qubits.[3] This means that your private key is almost certainly safe, despite your public-facing key being exposed to the world.

Figure 9: The elliptic curve of the elliptic curve cryptographic algorithm



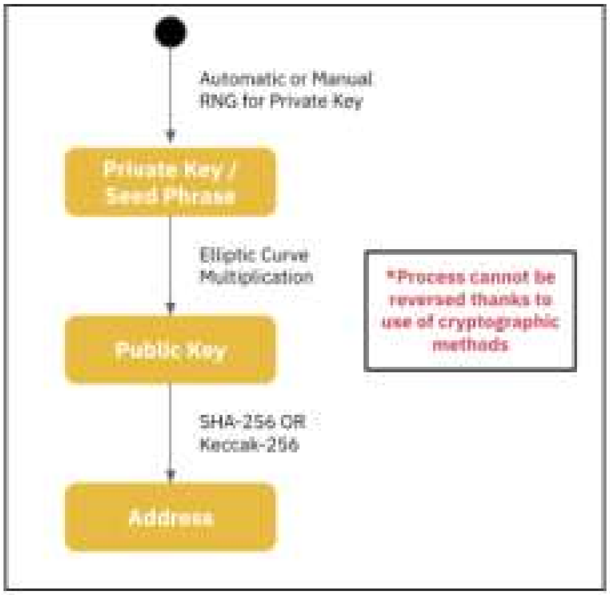
Source: Binance Research, Munish Kohli

3. Finally, to create your wallet address, your public key is put through another cryptographic algorithm

The last step of the process is to take the public key generated through the elliptic curve algorithm, and put it into another cryptographic algorithm to receive an address. Different blockchains use different algorithms to turn a public key into an address. Bitcoin utilizes an algorithm called SHA-256, BNB Chain and Ethereum uses an algorithm Keccak-256. Similar to how a public key is just a cryptographic reflection of a private key, a wallet's address is simply a cryptographic reflection of the public key.

Interestingly, the public key and address have the same functionality (to serve as a public-facing reference to receive or reference funds). However, addresses became standard to use in blockchains because they contain a smaller amount of digits than a public key. This is an example of abstraction to make the UX of wallets and transacting easier for the user.

Figure 10: Process to cryptographically generate a key-pair and address



Source: Binance Research

Overall, private keys cryptographically produce public keys. Public keys produce addresses. It is almost impossible for public keys to be reverse engineered to become private keys and it is almost impossible for addresses to be reverse engineered to become public keys. The key-pair generation process is cryptographically proven to be safe. Wallet holders can feel comfortable knowing there is very little potential to reverse engineer your key-pair and gain access to your private keys.

The only clear susceptibilities that wallets can face are if: (1) The random generated number for the private key in Step #1 is kept by the wallet provider, or is not actually randomly generated (2) Some exhaustive brute-force program, such as those made possible by quantum computers, is able to guess the inputs of Step #2 and Step #3 and effectively reverse engineer the key-pair. This is a real possibility and has given rise to account abstractions and the niche of wallet infrastructure research on how to make wallets that are insusceptible to quantum computers.

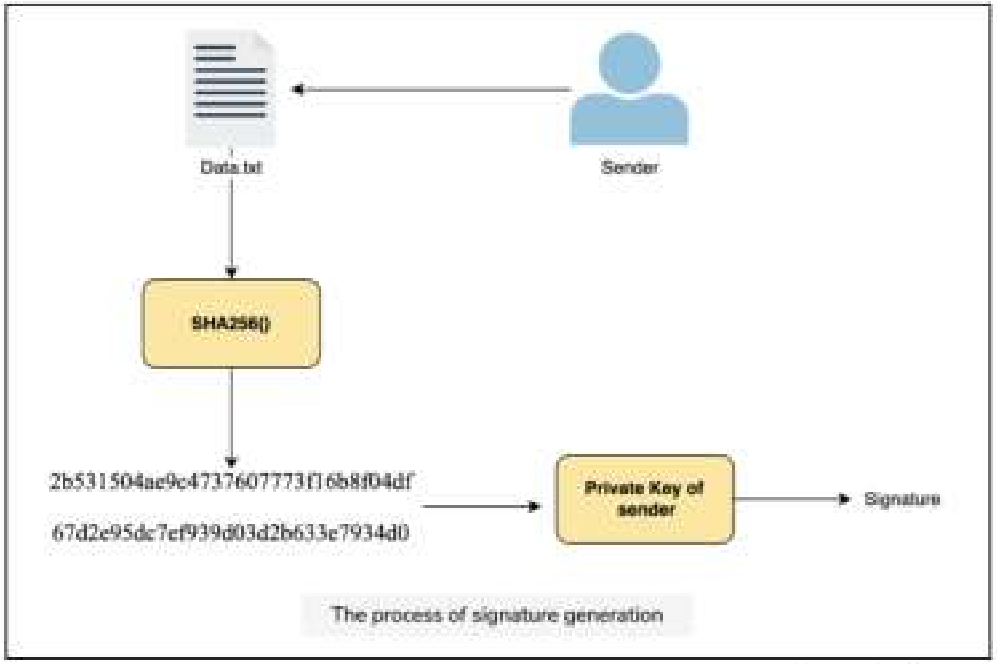
Authentically Signing Transactions

Off the blockchain, when you are ratifying an official transaction or document, there is almost always a need for a trusted intermediary, such as a notary or an apostille to verify that the transaction/document is authentic. On the blockchain, there is no need for such a trusted, centralized intermediary. Instead, wallet accounts use cryptographic methods to authentically sign and verify transactions by themselves.

In order to send a transaction from your wallet, you first need to have access to the private key. As the wallet user, you will then fill out the transaction's standard fields, including the recipient of the transaction, the amount of digital assets that are to be sent, and any transaction fee /gas parameters. Once you have inputted this information, the transaction can be authentically signed in preparation of being sent to the blockchain.

The process of signing a transaction employs the same cryptographic methods that are used when creating a wallet. SHA-256 (in the Bitcoin blockchain) or Keccak-256 (in the BNB Chain or Ethereum blockchain) will take the transaction data and "encrypt" the data (or cryptographically render the transaction data to be hidden). Next, this encrypted transaction data is digitally "signed," or more literally, combined with the wallet holder's private key. Lastly, the nodes of the blockchain will receive this sent transaction, compare the modified transaction data with the sender's public key, and then ultimately will confirm that transaction must have been signed by the sender's private key. This process verifies that the transaction is authentic and hasn't been modified by anyone except the wallet holder of the private keys.

Figure 11: Process of authentically signing transactions on the blockchain


Data.txt
Sender
SHA256()
2b531504ae9c4737607773f16b8f04df
67d2e95dc7ef939d03d2b633e7934d0
Private Key of sender
Signature
The process of signature generation

Source: Binance Research

Overall, from the creation of your wallet to the ability to sign transactions, it is clear that your wallet's security is dependent on cryptography. Once again, even if your wallet abstracts from these backend operational processes, it is important to understand, because it reiterates how important careful handling of your private keys are. Being your "own-bank" is refreshing, invigorating, and perhaps, freeing. However, to be your own bank, means you should be aware of all the operations of how that bank works. Without any knowledge of how key-pairs work, how your private keys are generated, or how signing transactions works, you are susceptible to potential compromizations to your wallet and funds.

Comparing Wallet Options

By understanding how wallets work, it becomes clear that wallets truly shape the user experience of a blockchain. They are the user's primary, and often only, touch-point to gain access to a blockchain's decentralized network. They are responsible for holding one's private keys, which provide exclusive access to the use of funds and the ability to transact. Wallets are truly the portal to the blockchain.

As such, a lot of time and development has been devoted towards optimizing the user experience of wallets. Also, spurred by momentous cycles such as DeFi Summer in 2020, L1 Chains in 2021, and the centralized contagion of 2022, wallet infra is of an increasing focus in a modern crypto world. If the goal is to create a truly decentralized system, in which people with different motivations, technical capacities, ages, and locations can use the blockchain, then a lot of work must be done to create wallets that cater to such a heterogenous group of users.

In this following section, we highlight the multiplicity of available wallet options today, and the ways in which current wallet options differentiate from each other. More specifically, we highlight how each wallet option is distinctively oriented and designed towards suiting a particular user profile of a broad-scoping decentralized network. Additionally, by using empirical and qualitative data, we illustrate how these different wallet options currently compare in terms of usage and user opinion.

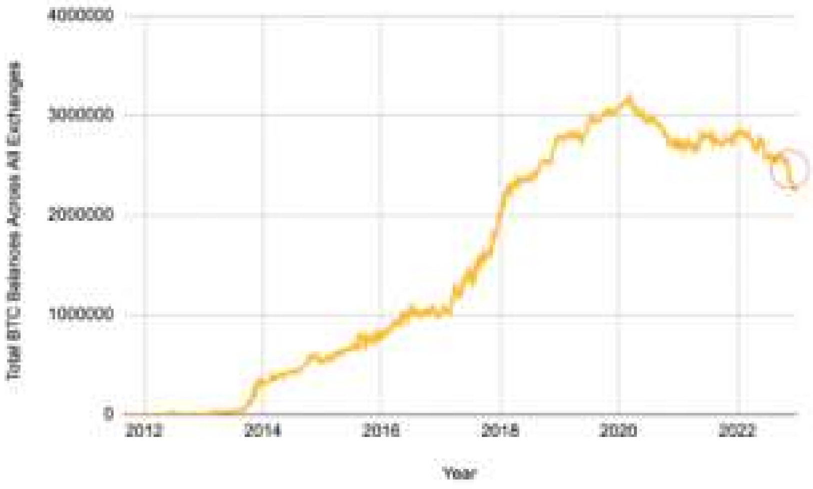
Key-Pair Storage: Custodial vs. Self-Custodial Wallets

A primary differentiating factor between wallet options is whether they are custodial or non-custodial. **A custodial wallet is one in which a third party manages the private key of the wallet**. An example of a custodial wallet is one that a centralized exchange would maintain for their users. On the other hand, **a self-custodial wallet implies the wallet user maintains their own private keys without the infringement of any third party.** Examples of non-custodial wallets are Trust Wallet or Metamask.

As discussed previously in the **How Wallets Work** section, control over private keys is synonymous with control over the wallet itself, the funds within the wallet, and any transaction activity that happens on the wallet. In this way, custodial services that manage a user's private keys, have complete control over the user's wallet. Ultimately, this implies that if the third party who is managing your private keys is a bad actor, they can take control over your wallet and spend your funds.

In 2022, unfortunately, the crypto space witnessed a number of occurrences in which custodial services have wrongly taken control over their users' funds. Perhaps, most notable of which, was in November 2022, in which certain centralized custodial services and exchanges were using customer funds without their permission. Ultimately, fear of using custodial services spread across the crypto industry and resulted in large withdrawals from custodial wallets to non-custodial wallets. In fact, shortly after the November 2022 revelation, Bitcoins swiftly fled exchanges to be moved into self custody. This has been reported to be the fastest rate of BTC moving off exchanges over the past 5 years.

Figure 12: BTC was swiftly moved off exchanges to self-custody options in response to custodial misuse of funds



Source: Binance Research, Glassnode

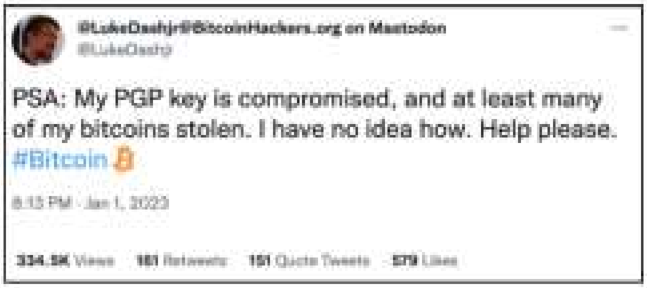
Furthermore, Kosala Hemachandra, creator of non-custodial solution MyEtherWallet reported usership to be up 75% post the November centralized custodian fallout.[4]

The potential dangers of malicious custodians, and the sanctity of self-custodial has been well highlighted by CZ. For years, CZ has been a supporter of self-custody, referring to it as a "fundamental human right" as self-custody implies true ownership and protection from bad-actors. Furthermore, self-custody is inline with the decentralized ethos of blockchain and the freedom from reliance of centralized counterparts.[5]

However, CZ also pointed out that self-custody wallets are not free of risk. On a December 2022 Twitter Spaces, CZ remarked that *"if we can have a way to allow 99% of the general population to hold their own assets in their custody securely and easily,"* then custodial services "*probably don't need to exist, which is great.*"[5] But unfortunately, in reality, this is not the case.

There are many different risk factors that come with self-custodial wallets, which make it infeasible for every crypto user to move away from custodial services. Best practices of managing one's own private keys requires strong technical and op-sec practices (see CZ's Keep your Crypto #SAFU tips). Unfortunately, without this strong technical and op-sec knowledge, *"most normal people will not be able to"* properly *"back up their security keys,"* or have proper *"encryption for that backup."*[5] Perhaps, they write the backup on a piece of paper, someone else *"sees the paper, and their funds can be stolen."*[5] Even Luke Dashjr, an OG Bitcoin core developer, on January 1st, 2023, had his private keys compromised and his wallet hacked, to ultimately lose $3.5M in BTC.[6]

Figure 13: Luke Dashjr's tweet about his compromised self-custodial wallet and lost Bitcoins



@LukeDashjr@BitcoinHackers.org on Mastodon
@LukeDashjr

PSA: My PGP key is compromised, and at least many of my bitcoins stolen. I have no idea how. Help please. #Bitcoin ₿

8:13 PM · Jan 1, 2023

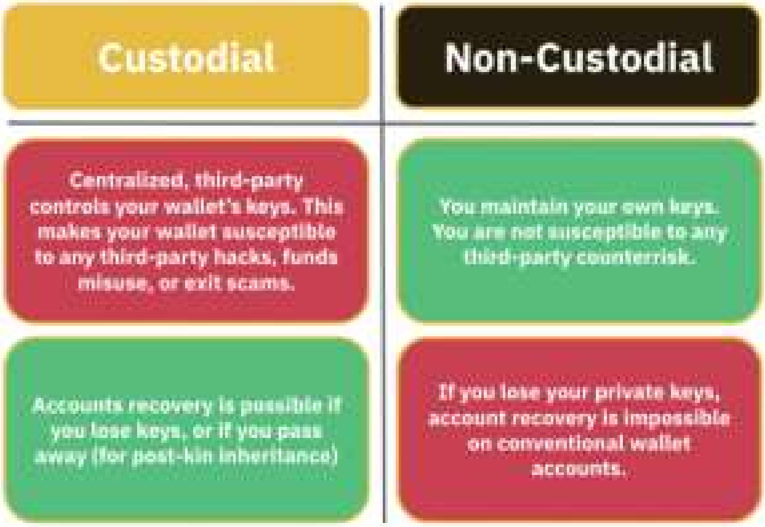
334.5K Views 181 Retweets 151 Quote Tweets 579 Likes

Source: Twitter (@LukeDashjr)

Furthermore with self-custodial wallets, *"if a person passes away, they don't have a way to give [the private keys] to their next of kin."* [5]

The reality is while *"different [custody] solutions have different risk profiles,"* there will always be some form of risk factors present.[5] The choice between custodial and non-custodial options truly depends on the user, and which risks they deem less likely to come to fruition.

Figure 14: Comparison of risk factors between custodial and non-custodial wallets

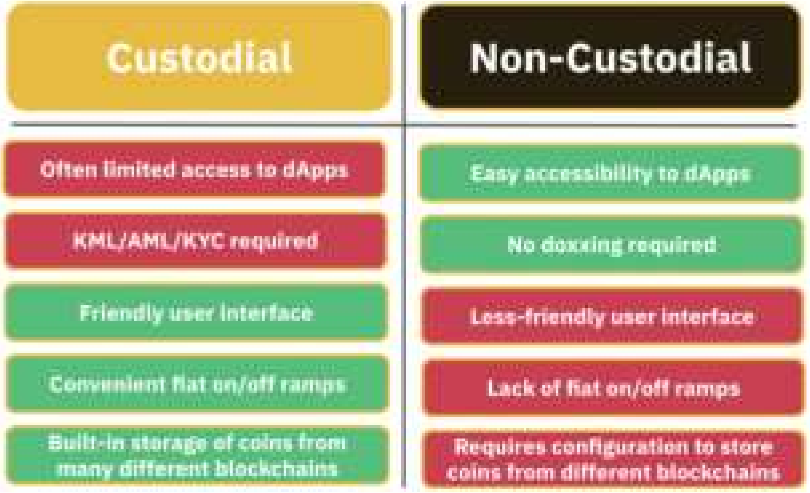


Custodial	Non-Custodial
Centralized, third-party controls your wallet's keys. This makes your wallet susceptible to any third-party hacks, funds misuse, or exit scams.	You maintain your own keys. You are not susceptible to any third-party counterrisk.
Accounts recovery is possible if you lose keys, or if you pass away (for post-kin inheritance)	If you lose your private keys, account recovery is impossible on conventional wallet accounts.

Source: Binance Research

Choosing a custodial or non-custodial wallet however, is often not judged solely on risk factors alone. UX factors such as usability, functionality, and convenience are also considered. Custodial wallet options often have friendly user-interfaces, convenient fiat onramps/offramps, and capabilities of storing coins from many different blockchains. However, custodial options often limit the functionality of the wallet to using their centralized service offerings (such as their own exchange) and in most jurisdictions will require users to provide KML/AML/KYC. Conversely, non-custodial options provide decentralized access to any dApp on the corresponding network, and do not require any doxxing of identity. However, non-custodial options, have comparatively less friendly UX designs, often do not have clear fiat on-ramps/off-ramps, and either require manual configuration to store multi-chain coins or only can store coins of a specific blockchain.

Figure 15: Comparison of risk factors between custodial and non-custodial wallets



Custodial	Non-Custodial
Often limited access to dApps	Easy accessibility to dApps
KML/AML/KYC required	No doxxing required
Friendly user interface	Less-friendly user interface
Convenient fiat on/off ramps	Lack of fiat on/off ramps
Built-in storage of coins from many different blockchains	Requires configuration to store coins from different blockchains

Source: Binance Research

Connectivity: Hot vs. Cold Wallets

A further delineation between wallet options is whether they are considered “hot” or “cold.”

A “hot wallet” is a wallet that is connected to the internet. An example of a hot wallet could be a non-custodial wallet such as Trust Wallet / Metamask or a custodial, centralized exchange wallet. Hot wallets are able to directly sign transactions and send transactions to the blockchain as they are connected to the internet.

A “cold wallet” is not connected to the internet. Cold wallets require the user to use a “crypto-bridge” to receive transaction data offline, sign the transaction data, then ultimately, send the transaction back through the “crypto-bridge” to broadcast the transaction online. This process requires more time to send a transaction than a hot wallet and perhaps, is also less convenient as compared to the internet-readiness of the hot wallet. What cold wallets lack in convenience, they make up for in security. Hot wallets are vulnerable to online hacks, whereas cold wallets are offline and do not have the same susceptibilities.

Many exchanges, such as Binance, store some of their customer’s funds in cold wallets, and then the rest of theirunds needed for withdrawals in hot wallets. Given the trade-offs, using a combination of both cold and hot wallets is usually ideal. Your cold wallet can store crypto you don’t plan on moving often. A hot wallet can be for everyday transactions, emergency transactions, trading, and whatever other kind of transaction requires a convenient and timely response.

Format: Browser Extension vs. Mobile vs. Desktop vs. Hardware vs. Paper

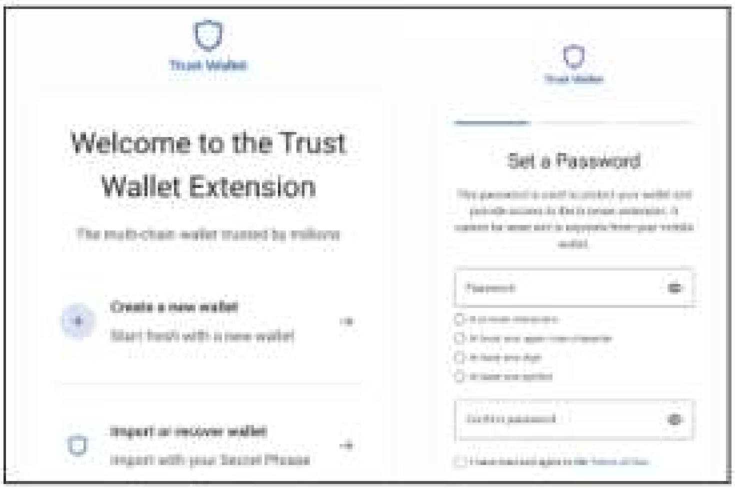
A third differentiation between wallet options is the format. Wallets come in a diverse set of formats, including browser extension wallets, desktop wallets, mobile wallets, hardware wallets, and paper wallets.

- **Browser Extension Wallets**

Browser Extension wallets are a type of wallet installed into one’s web browser, allowing the user to access their wallet with ultra-convenience. Whenever the user clicks on the extension, or interacts with a transaction prompting element on a web-page (such as a button to swap on a dApp like PancakeSwap), the wallet pops up in the browser and allows the user to transact, check their account balance, or check their transaction activity.

Creating a browser extension wallet follows the process discussed in the **How Wallets Work** section. Alternatively, many browser extension wallets today also allow for a private key or seed phrase to be imported into the wallet. Effectively, by importing the private key/seed phrase, you are logging into an existing wallet, instead of creating a new wallet. To improve the convenience of using their products, many browser extensions have abstracted away from repeated creation of wallets or importation of private keys. The wallet in one's browser only requires creation/importation of private keys once. After which, most browser extensions protect the use of the wallet with a password rather than one's private keys.

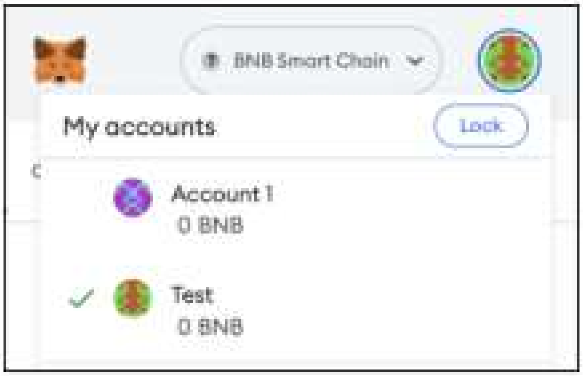
Figure 16: Create a wallet or import your private keys, then set a password to login


Trust Wallet
Welcome to the Trust Wallet Extension
The multi-chain wallet trusted by millions
Create a new wallet
Start fresh with a new wallet
Import or recover wallet
Import with your Secret Phrase
Trust Wallet
Set a Password
Password
Confirm password

Source: Trust Wallet

Additionally, many wallets today allow users to seamlessly create multiple accounts, with private key access and balances all aggregated in the wallet user's balance. This feature allows wallet users to create two individual accounts, transact privately through each account, but have an aggregated balance between the two accounts. Without an account's private keys or the doxxing of the wallets, there is no way to prove that the accounts came from the same wallet.

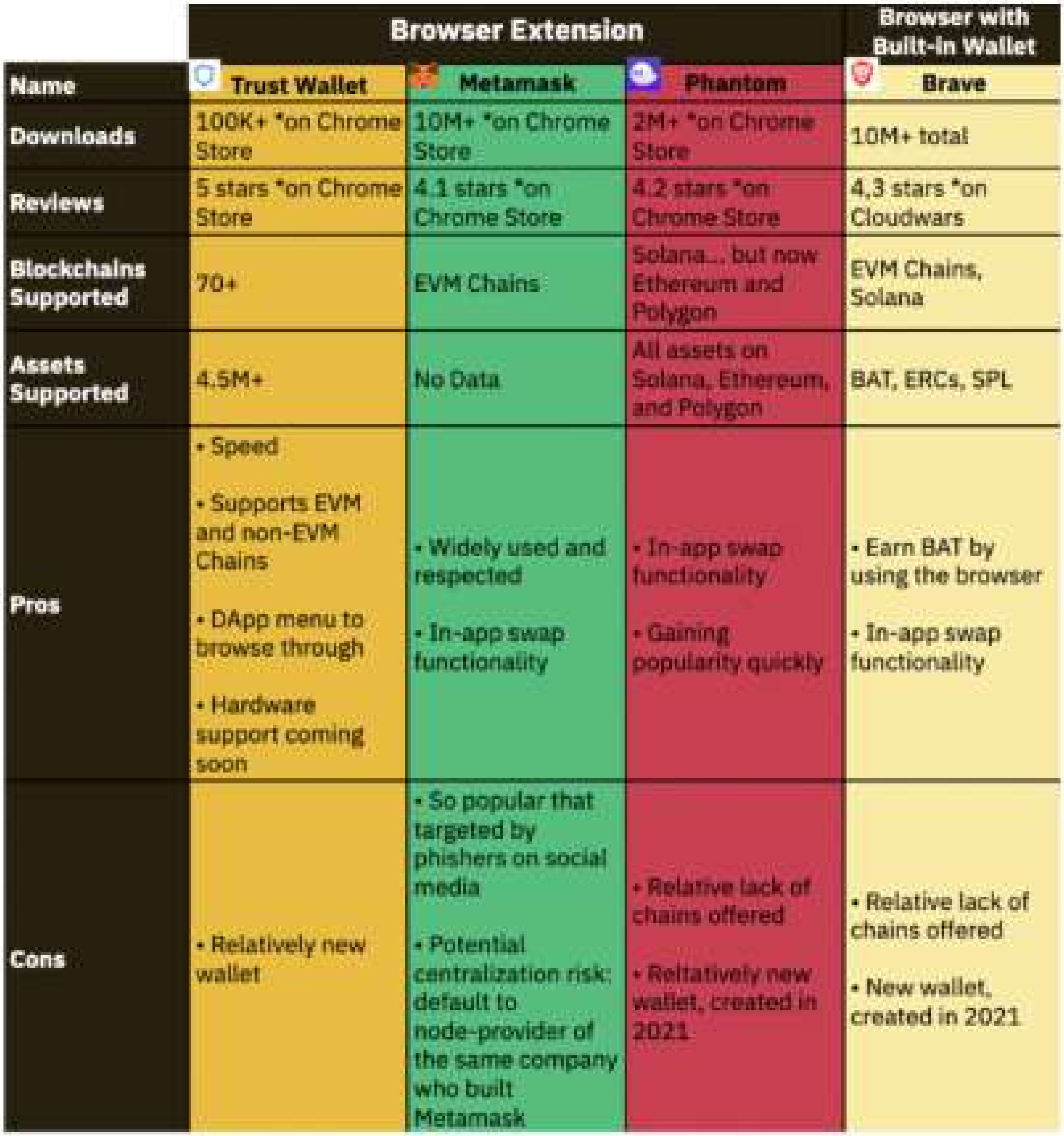
Figure 17: Most browser extension wallets allow users to create multiple accounts under the same wallet



Source: Metamask

Below depicts a review of a few browser extension wallet options. All browser extensions represented in the chart wallets are hot, and non-custodial (as most are). Trust Wallet and Metamask are the most popular browser extension wallets. Phantom is a browser extension wallet that has significant market share in the Solana ecosystem, and just recently announced compatibility with Ethereum and Polygon. One interesting browser extension wallet option is the Brave Wallet. The Brave Wallet is a part of the Brave Browser. BAT or Basic Attention Tokens accumulate to one's Brave wallet for using the Brave Browser to surf the web.

Figure 18: Comparison table of different browser extension wallets



	Browser Extension			Browser with Built-in Wallet
Name	**Trust Wallet**	**Metamask**	**Phantom**	**Brave**
Downloads	100K+ *on Chrome Store	10M+ *on Chrome Store	2M+ *on Chrome Store	10M+ total
Reviews	5 stars *on Chrome Store	4.1 stars *on Chrome Store	4.2 stars *on Chrome Store	4,3 stars *on Cloudwars
Blockchains Supported	70+	EVM Chains	Solana... but now Ethereum and Polygon	EVM Chains, Solana
Assets Supported	4.5M+	No Data	All assets on Solana, Ethereum, and Polygon	BAT, ERCs, SPL
Pros	• Speed • Supports EVM and non-EVM Chains • DApp menu to browse through • Hardware support coming soon	• Widely used and respected • In-app swap functionality	• In-app swap functionality • Gaining popularity quickly	• Earn BAT by using the browser • In-app swap functionality
Cons	• Relatively new wallet	• So popular that targeted by phishers on social media • Potential centralization risk: default to node-provider of the same company who built Metamask	• Relative lack of chains offered • Reltatively new wallet, created in 2021	• Relative lack of chains offered • New wallet, created in 2021

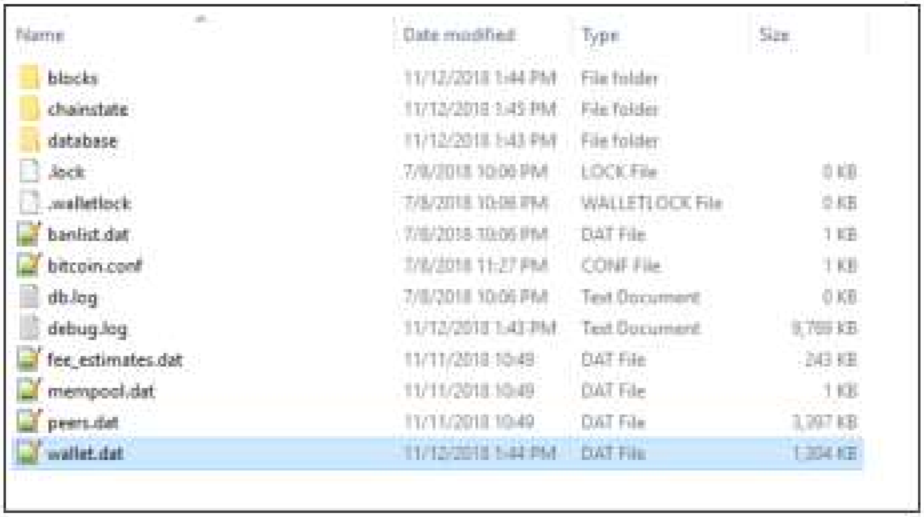
Source: Binance Research, Wallets' websites

Desktop Wallets

Desktop wallets are software programs that allow users from different operating systems to access their crypto directly from their desktop. Desktop apps are typically defined as hot wallets, but only connect to the internet when the device is on. This renders desktop wallets to be more secure than their browser extension counterparts, and exposes vulnerability to online hacks only when the computer is connected to the internet.

Desktop wallets are almost always non-custodial, and upon creation of a wallet, require the user to download their private key as an encrypted file, often called "wallet.dat," to their computer. Like browser extension wallets, most desktop wallets are also able to import private keys/seed phrases so that if a computer is damaged, stolen, or lost, they will not lose access to their wallet. Also, desktop wallets often require 2-factor authentication (2FA), which requires a user to login to their desktop by first providing a password (like browser extensions), but also a code from a connected email, phone number, or authenticator app.

Figure 19: Screenshot of encrypted private key file of desktop wallet



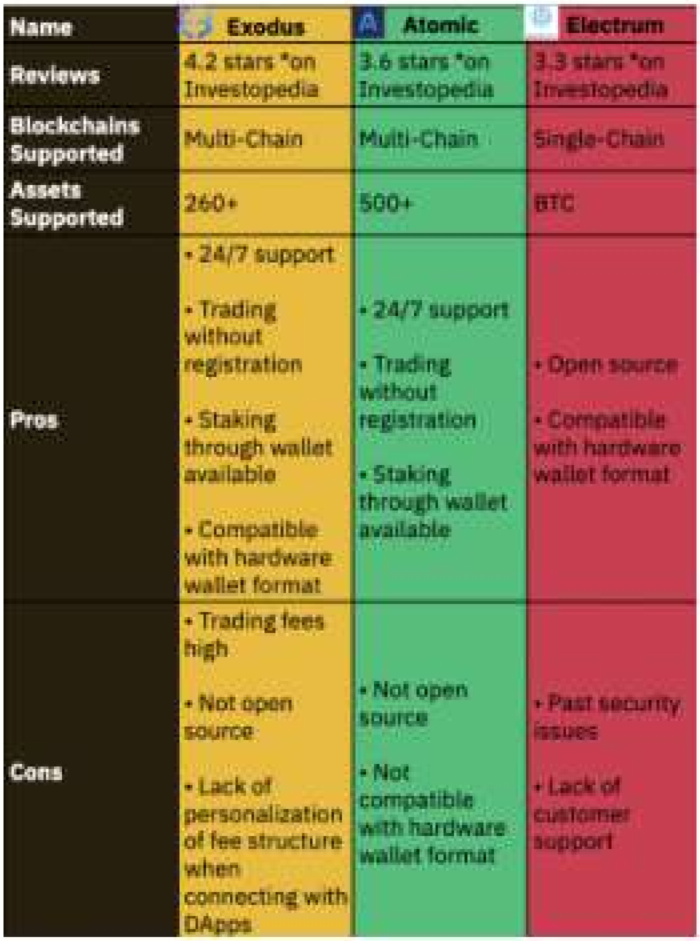
Name	Date modified	Type	Size
blocks	11/12/2018 1:44 PM	File folder	
chainstate	11/12/2018 1:45 PM	File folder	
database	11/12/2018 1:43 PM	File folder	
.lock	7/8/2018 10:06 PM	LOCK File	0 KB
.walletlock	7/8/2018 10:08 PM	WALLETLOCK File	0 KB
banlist.dat	7/8/2018 10:06 PM	DAT File	1 KB
bitcoin.conf	7/8/2018 11:27 PM	CONF File	1 KB
db.log	7/8/2018 10:06 PM	Text Document	0 KB
debug.log	11/12/2018 1:43 PM	Text Document	9,769 KB
fee_estimates.dat	11/11/2018 10:49	DAT File	243 KB
mempool.dat	11/11/2018 10:49	DAT File	1 KB
peers.dat	11/11/2018 10:49	DAT File	3,297 KB
wallet.dat	11/12/2018 1:44 PM	DAT File	1,204 KB

Source: Binance Research

However, unlike browser extension wallets, because desktop wallets are not ingrained into the browser, there are relatively less dApps that support desktop wallets. In response, some desktop wallets have created in-app trading functionalities. It should be noted that trading fees tend to be higher on desktop wallets as opposed to transacting on chain or through a centralized exchange.

Below depicts a review of a few browser extension wallet options. All desktop wallets listed are hot wallets. Exodus and Atomic are multi-chain wallets whereas Electrum is a single-chain wallet. Exodus and Atomic are regarded as the most popular desktop wallets. There are in-app trading features on Exodus and Atomic, but fees are relatively higher on average than trading on a centralized exchange or directly through a dApp. Additionally, on Exodus there is no ability to personalize gas/transaction fees parameters prior to sending a transaction. Other than the wallets listed, there are a swath of other desktop wallets. However, they aren't listed here because their desktop-wallet product is not their default format of their wallet offerings.

Figure 20: Comparison table of different desktop wallets



Name	Exodus	Atomic	Electrum
Reviews	4.2 stars *on Investopedia	3.6 stars *on Investopedia	3.3 stars *on Investopedia
Blockchains Supported	Multi-Chain	Multi-Chain	Single-Chain
Assets Supported	260+	500+	BTC
Pros	• 24/7 support • Trading without registration • Staking through wallet available • Compatible with hardware wallet format	• 24/7 support • Trading without registration • Staking through wallet available	• Open source • Compatible with hardware wallet format
Cons	• Trading fees high • Not open source • Lack of personalization of fee structure when connecting with DApps	• Not open source • Not compatible with hardware wallet format	• Past security issues • Lack of customer support

Source: Binance Research, Wallets' websites,

Mobile Wallets

There are many similarities between mobile and desktop wallets. Mobile wallets, like desktop wallets, are downloaded software, and are often hot and self-custodial. However, it should be recognized that mobile wallets have begun to differentiate themselves from desktop wallets in terms of convenience.

First, because phones are portable and have ready-to-use cameras, mobile wallets may be considered more convenient than desktop wallets. A mobile wallet can be carried around everywhere. The wallet holder can then use their camera to scan QR codes, prompt transactions, and make everyday transactions in an extremely convenient manner.

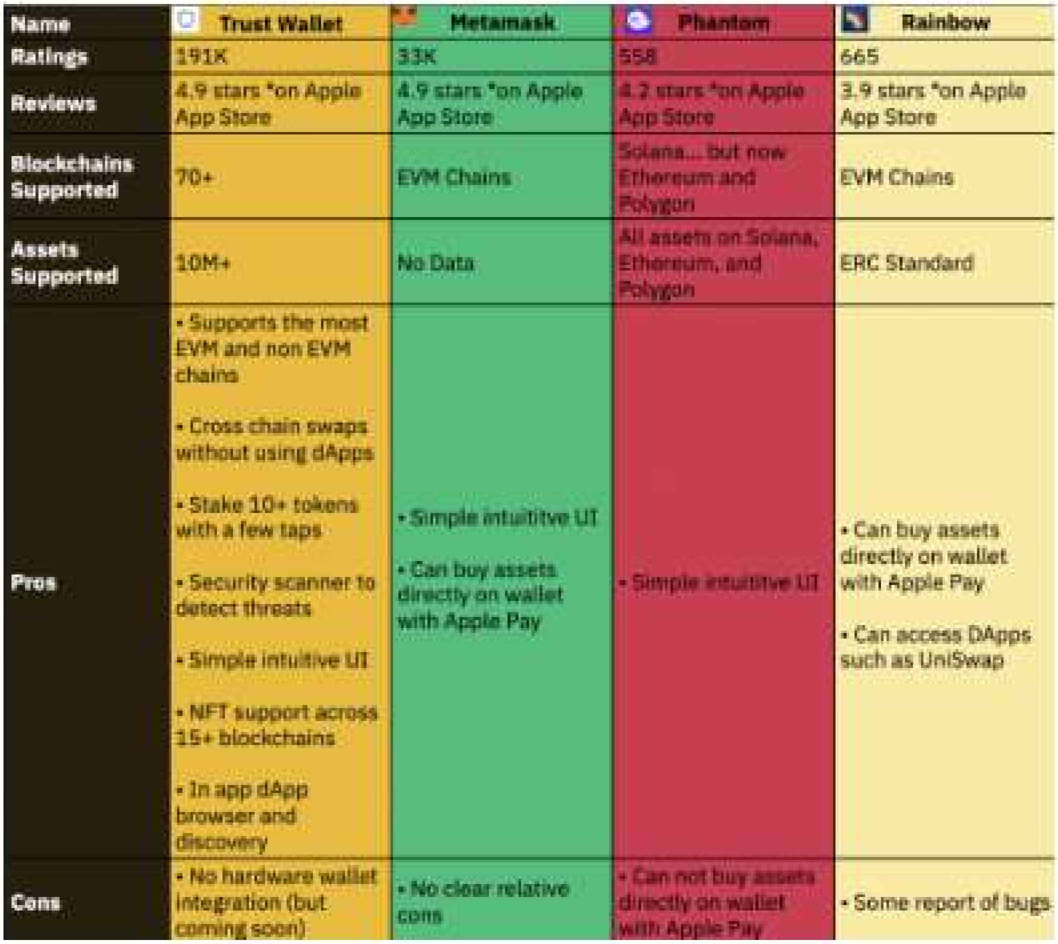
Second, mobile wallets are relatively more compatible with dApps, and thus provide convenience of using the blockchain that desktop wallets do not. Historically, software wallets, including both desktop and mobile formats, were incompatible with dApps because they were software-based, and not ingrained into the browser. However, recent innovations in the mobile wallet space are bridging the gap, and allowing users to have similar levels of compatibility with dApps as compared to browser extensions. For example, Trust Wallet has a feature called "Trust dApp Browser," which is a fully functioning Web3 browser that can be used to interact with any dApp. Your wallet will still maintain its private keys within the mobile wallet software, but you will be able to sign transactions and transact on dApps through the dApp Browser interface. In this way, the Trust dApp browser allows Trust Wallet users to conveniently browse, find the best dApps to use, and then interact with those dApps.

Another example of this trend towards mobile wallet compatibility is the Solana phone, which is set to be the first blockchain compatible mobile phone. The phone, expected to be released in early 2023, will use a "Mobile Wallet Adapter," as a protocol for connecting dApps to the wallets on the mobile device. The Mobile Wallet Adapter is designed to support all mobile platforms, is open source, and can work with wallet apps by providing signing services to dApps.

Lastly, mobile wallets may serve as a more convenient way to maintain cold storage than desktop wallets. A growing trend is the "use of a second phone that serves solely" as a cold, mobile crypto wallet.[7] Many people are taking old smart-phones, downloading a mobile crypto wallet, transferring their crypto to that mobile wallet, and then turning off the internet/putting the phone on airplane mode. This is effectively taking the old smart-phone and turning it into a cold wallet. When one wants to use the mobile wallet, they can simply turn on the internet through the phone's configurations and proceed to make transactions. A mobile wallet in this way, may serve as a more convenient cold storage than desktop wallets, because on average people have more old phones than old laptops, and because it is simpler and easier to turn the internet on and off on these devices.

Below depicts a review of a few mobile wallet options. Trust Wallet in the mobile wallet category clearly dominates in terms of downloads. As shown by user reviews, Metamask and Trust Wallet are well regarded. All wallets except for Phantom provide the ability to use Apple pay to buy digital assets in the mobile wallet.

Figure 21: Comparison table of different mobile wallets



Name	Trust Wallet	Metamask	Phantom	Rainbow
Ratings	191K	33K	558	665
Reviews	4.9 stars *on Apple App Store	4.9 stars *on Apple App Store	4.2 stars *on Apple App Store	3.9 stars *on Apple App Store
Blockchains Supported	70+	EVM Chains	Solana... but now Ethereum and Polygon	EVM Chains
Assets Supported	10M+	No Data	All assets on Solana, Ethereum, and Polygon	ERC Standard
Pros	• Supports the most EVM and non EVM chains • Cross chain swaps without using dApps • Stake 10+ tokens with a few taps • Security scanner to detect threats • Simple intuitive UI • NFT support across 15+ blockchains • In app dApp browser and discovery	• Simple intuititve UI • Can buy assets directly on wallet with Apple Pay	• Simple intuititve UI	• Can buy assets directly on wallet with Apple Pay • Can access DApps such as UniSwap
Cons	• No hardware wallet integration (but coming soon)	• No clear relative cons	• Can not buy assets directly on wallet with Apple Pay	• Some report of bugs

Source: Binance Research, Wallets' Websites

So far, we have discussed browser extension, desktop, and mobile wallets, which are most often used as hot wallets. These wallets were used quite conveniently, given their ability to connect to the internet. Now we will introduce two forms of wallets that are configured to be cold wallets: hardware wallets, and paper wallets. These wallets are marketed and configured to prioritize security, not convenience.

Hardware Wallets

Hardware wallets are one type of cold wallet. Hardware wallets are physical devices that typically resemble a USB stick, but actually function as a "stripped-down, single-purpose computer that can only perform a few basic but essential functions."[8]

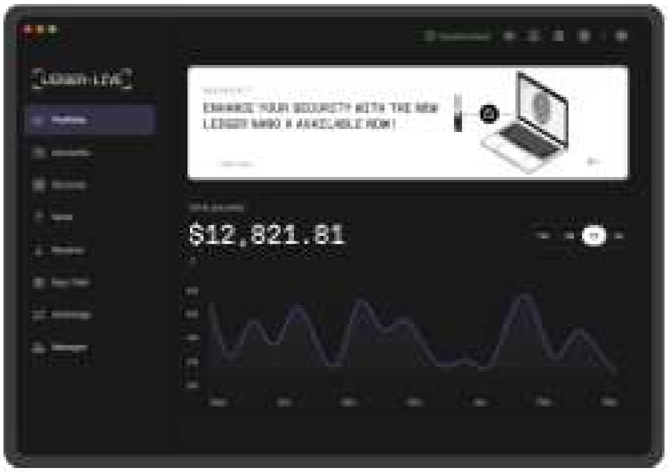
The design of the hardware wallets gives them unmatched security as compared to other wallet options. As compared to the hot wallets previously discussed, hardware wallets are not connected to the internet, making it virtually impossible for external hackers to access their contents. Even the most powerful malware can't sign a hardware wallet transaction to steal funds if the wallet is offline. In fact, the hardware wallet's intentional lack of internet connection even makes it difficult for the owner of the wallet to send transactions, let alone use the wallet to access dApps. To send a transaction, a hard wallet holder must connect their hard wallet to a PC, then utilize something called a "crypto-bridge" to transfer unsigned transaction data to the device, so that the hardware wallet can sign that transaction data with the offline private keys. Only to ultimately, return the signed transaction data back through the crypto-bridge to be broadcasted online to the rest of the blockchain network.

To bolster the security profile of hardware wallets further, most have additional security measures like lock PIN, 2-Factor authentication, and biometric security (buttons that let the device know it's physically you authenticating transaction). If the device ever gets lost, the wallet can be recovered by importing the seed phrase of the hardwallet into at creation can any other wallet provider (hot or cold).

The aforementioned security aspects of hardware wallets makes it appealing for users looking to engage in long-term storage of crypto, or who are more risk-averse to custodial solutions and hot wallets. In fact, during November 2022, when there were reports of centralized exchanges using customer funds, users fled to safety and sales of hardware wallets surged. Trezor and Ledger, two hardware wallet companies, as a result, reported a tripling of sales revenues.[9]

Historically, hardware wallets have been used for long-term storage of crypto. This meant that they didn't have to be as user-friendly as any of the previously discussed hot wallet types. However, overtime, hardware wallets have made innovations to become more convenient and compatible with dApps. For example, Ledger has come out with a platform of apps and services called Ledger Live, which serves as a secure gateway to NFT and DeFi based services. In practice, if a Ledger hardware wallet is connected to one's computer, then it can easily approve transactions through a crypto bridge. Even if the Ledger hardware wallet is not connected to one's computer, Ledger Live can show the wallet's account balance based on the wallet's last sync. This allows users to monitor their portfolio, even when the hardware wallet is stored securely.

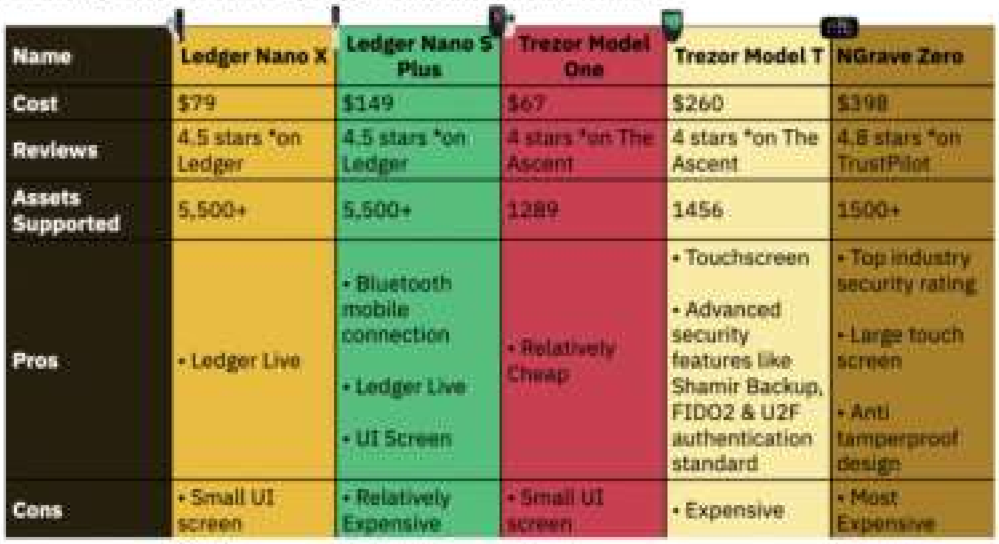
Figure 22: User interface of Ledger Live


LEDGER LIVE
ENHANCE YOUR SECURITY WITH THE NEW LEDGER NANO X AVAILABLE NOW!
$12,821.81

Source: Ledger

Below depicts a review of a few mobile wallet options. In the crypto space, Ledger and Trezor are by far the most recognizable hardware wallets. However, also included in the table is Ngrave's Zero wallet, which has recently been gaining traction. Ngrave differentiates itself amongst Ledger and Trezor for its "fully air-gapped" hardware wallet, which doesn't require any USB, network connection, or 4G. The Zero wallet has been called the "coldest" hardware wallet for this reason. Ledger and Trezor have an expensive wallet type and a less expensive wallet option, whereas Ngrave just has one wallet option. The discrepancies between the expensive and less expensive type is usually the screen size. However, the Trezor Model T as compared to the Trezor Model One also can support more coins. Ngrave's wallet has the largest screen size and supports a relatively similar amount of coins.

Figure 23: Comparison table of different hardware wallets



Name	Ledger Nano X	Ledger Nano S Plus	Trezor Model One	Trezor Model T	NGrave Zero
Cost	$79	$149	$67	$260	$398
Reviews	4.5 stars *on Ledger	4.5 stars *on Ledger	4 stars *on The Ascent	4 stars *on The Ascent	4.8 stars *on TrustPilot
Assets Supported	5,500+	5,500+	1289	1456	1500+
Pros	• Ledger Live	• Bluetooth mobile connection • Ledger Live • UI Screen	• Relatively Cheap	• Touchscreen • Advanced security features like Shamir Backup, FIDO2 & U2F authentication standard	• Top industry security rating • Large touch screen • Anti tamperproof design
Cons	• Small UI screen	• Relatively Expensive	• Small UI screen	• Expensive	• Most Expensive

Source: Binance Research, Wallets' websites

Paper Wallets

A paper wallet is a type of cold wallet that is simply a piece of paper (or any object) that has a private key printed on it. Often, in the form of a QR code, so that the private key can be scanned through a mobile phone application and used to sign transactions.

Early on in crypto, paper wallets were seen as a high security wallet option. They reached their peak popularity in the late 2010s for their lack of internet susceptibility. However, by 2016 it became apparent that paper wallets were prone to many other dangers that could compromise the private keys. Now paper wallets are largely a thing of the past.

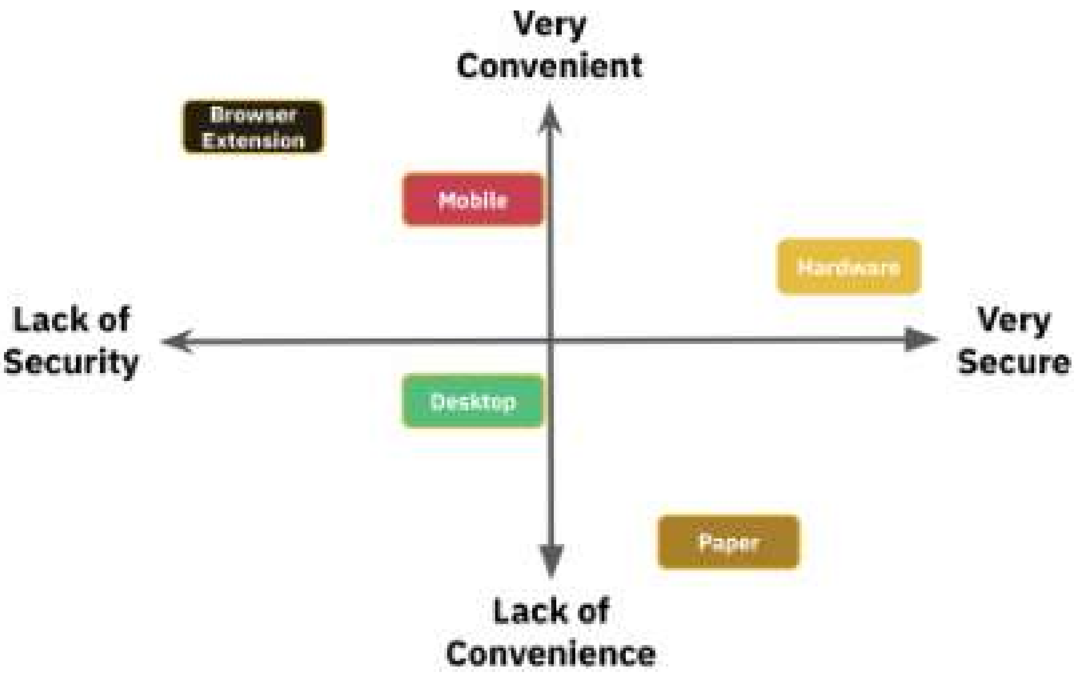
Susceptibilities of paper wallets include the following:

1. Prone to environmental damage: water, fire, moisture
2. Easily stolen, misplaced, or lost
3. Is incapable of tracking UTXO change, as the wallet has no way to tag new addresses to the main wallet

Overview of Formats

Overall, it is clear that the format of the wallet has large implications for the convenience and risk factors associated with the wallet. Browser extensions are very convenient, have optimal connectivity to the blockchain and dApps, but are the most prone to hacks. Mobile and desktop wallets are a bit more secure as they are not ingrained into the browser and can be turned into cold wallets. Mobile wallets have made strides in convenience, whereas desktop wallets haven't shown clear signs of convenience yet. Hardware wallets prioritize security. Hardware wallets are also becoming more convenient as more dApps build on their secure signing bridges. Paper wallets are cold wallets and thus are inherently more secure. However, they are completely inconvenient as they cannot aggregate UTXOs or bridge to dApps in any simple manner.

Figure 24: Comparing wallet options based on the Convenience vs. Security tradeoff



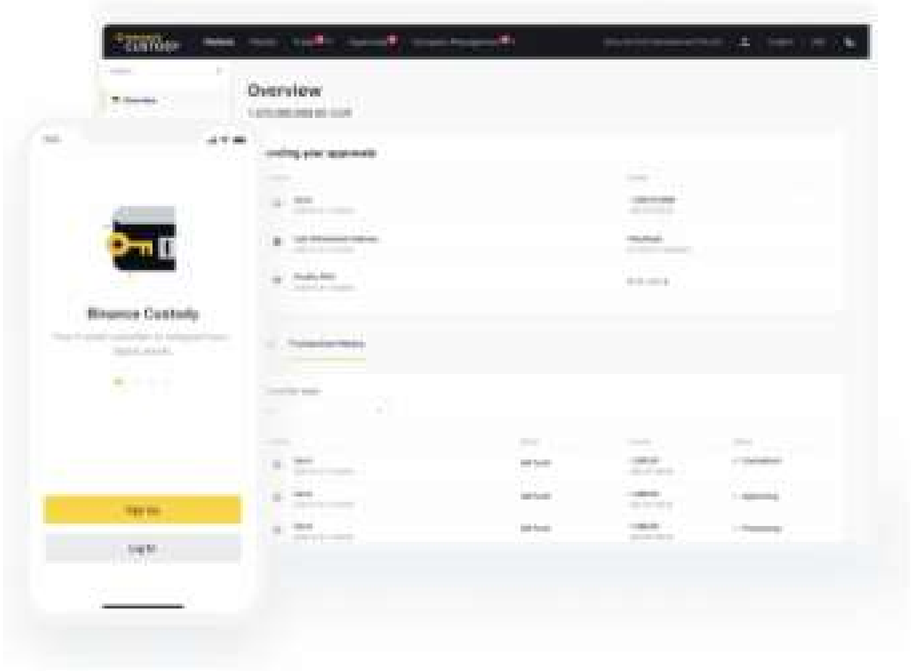
Source: Binance Research

It becomes clear by overviewing the various wallet options that using a combination of different wallet formats for different purposes is ideal. When you need convenience for everyday transactions or timely trades, perhaps you utilize a mobile or browser extension. When you need to optimize security for longterm crypto holdings, perhaps, you utilize a hardware wallet.

Binance Custody recognizes the value in optimizing for wallets' differing comparative advantages. As such, they offer a wide range of wallet options to their clients including a "Qualified Wallet" product (hard wallet cold storage), a "Prime Wallet" product (combination of cold storage and hot wallet designed for instantaneous withdrawals), and other personalized solutions. Alongside these wallet options,

Binance Custody also solves for some of the drawbacks of different wallet formats. For example, they offer a "Cold Convert" service for their clients hardware wallets, in which client's can trade directly with Binance at competitive OTC rates without compromising any keys. They also just recently began offering "Binance Mirror," which enables institutions to access trading and investment products within the Binance Exchange ecosystem without having to post collateral directly on the exchange. Through Binance Mirror, institutions lock a specified amount of their asset balance available in their Qualified Wallet, Binance Custody's cold storage solution, and mirror it onto their Binance Exchange account with a 1:1 balance. Their assets remain secure in their segregated cold wallet for as long as their Mirror position remains open on the Binance Exchange, which can be settled at any time. As an added benefit, Binance Custody is insured and SAFU protected, to insure their clients funds, which is coverage that no wallet format alone provides. It is ISO 27001/27701 certified and SOC 2 Type 1/Type 2 attested.[9]

Figure 25: User interface of Binance Custody



Source: Binance Custody

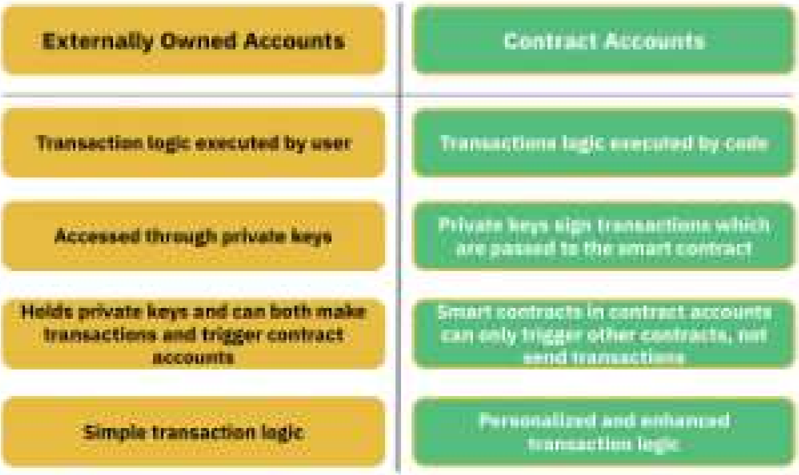
Code Logic: External vs. Contract

A further differentiator between wallet types is whether the code logic of the wallet is external, or smart contract based. Smart contract platforms have enabled the blockchain to become programmable, and moreover, have added layers of personalization and functionality that did not exist prior to smart contract platforms. Wallet functionality has and will continue to benefit directly from the introduction of programmability.

Most wallet accounts today have no code logic. The wallet accounts we have discussed thus far are called "externally owned accounts" (EOAs), which signifies that the wallets have no additional embedded code logic. These wallets can only do basic, standard operations like check account balances and send transactions. Furthermore, these wallets abide by conventional standards laid out by the blockchain, and allow for limited flexibility in how private keys are stored.

However, over the past few years, so-called "contract account" wallets have been gaining traction. **Contract accounts as opposed to externally owned accounts are programmable and as a result, have enhanced functionality as compared to external accounts.** In their most basic form, contract accounts are simply a combination of an external account, which is responsible for initiating transactions and maintaining private keys, and a smart contract, which is responsible for executing the transactions. To execute a transaction on a contract account, the externally owned account signs a transaction to be sent to the smart contract, which is then verified to carry out complex, arbitrary logic.

Figure 25: Comparison of EOAs and contract accounts



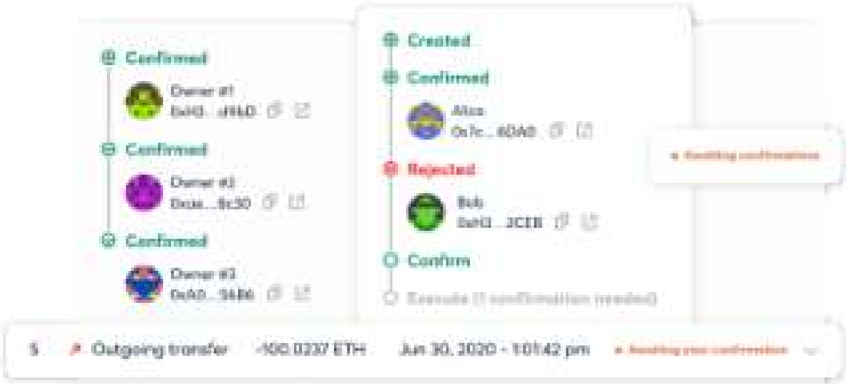
Externally Owned Accounts	Contract Accounts
Transaction logic executed by user	Transactions logic executed by code
Accessed through private keys	Private keys sign transactions which are passed to the smart contract
Holds private keys and can both make transactions and trigger contract accounts	Smart contracts in contract accounts can only trigger other contracts, not send transactions
Simple transaction logic	Personalized and enhanced transaction logic

Source: Binance Research

Contract accounts serve many different use cases and have been designed to be highly customizable.

For example, Gnosis Safe has used contract accounts to create a wallet which requires multiple signatures instead of just one. These wallets are commonly referred to as "multi-signature" or "multi-sig" wallets. How does this work? When a user wants to create a multi-sig wallet, they prompt Gnosis Safe to create a "Safe" by sending a transaction containing the public addresses of users they wish to have access to the safe. This safe is really just a smart contract that represents a collaborative escrow account. Each white listed public address can then propose transactions that alter the balance of the safe. If the other whitelisted users agree to this proposal, they can sign off on the transaction proposal by interacting with the safe. Ultimately, once a certain threshold of whitelisted users has signed off on the proposal, the safe will autonomously execute the transaction. The Gnosis Safe contract account wallet is particularly useful for groups of individuals that need to maintain some kind of collaborative set of funds. This could be a treasury for a Decentralized Autonomous Organization (DAO), or more simply, a collection of funds for a blockchain-based club.

Figure 26: User interface of Gnosis Safe



Source: Gnosis Safe

Another example of a contract account wallet is Argent. Argent is a mobile wallet that allows users to recover lost or forgotten private keys. According to Chainalysis, about 20% of the bitcoins in circulation as of 2021 were lost because the owner did not remember their private key.[10] This is a pervasive problem with EOAs models across all blockchains. Argent attempts to solve this problem by using a process called "social recovery." Social recovery requires that users of the Argent wallet, upon creation of an account, list a "guardian" or the public address of someone you trust to help you recover lost private keys. You can list an infinite amount of public addresses to be guardians. If you lose your private key to your Argent wallet, you can request these guardians to help you recover access to your wallet by sending a notification to the guardians letting them know you lost your private keys. The guardians will then be prompted to accept to reject this recovery attempt. If at least half of one's guardians approve a recovery, then the wallet will then be unlocked in the mobile app, and the user will be sent a code to their phone/email address to unlock it thereafter. It should be noted that social recovery on Argent requires a mobile phone number and email address. This may be seen as less decentralized/anonymous than the standard external account model and a trade-off for the enhanced functionality of the contract account.

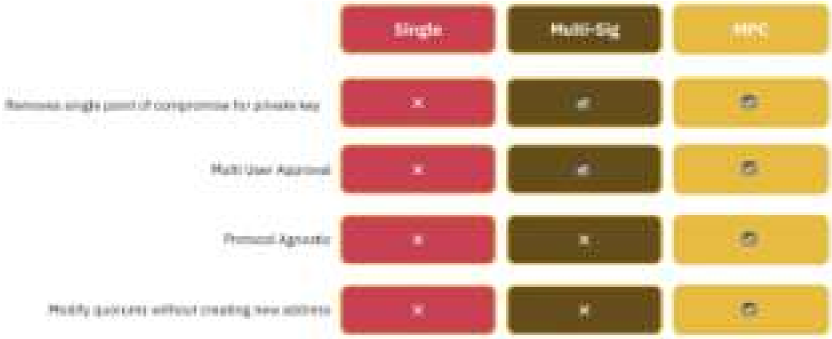
Contract accounts wallets like Gnosis and Argent are clearly an abstraction from the basic standard of the externally owned account model. At the current moment, these contract accounts are highly customized and lack a unified industry standard. Furthermore, most contract account wallets are relatively new. As such, contract account wallets are less time-tested as compared to externally owned accounts. Additionally, the first time using a contract account wallet, the wallet holder must deploy the smart contract that will execute the customized functionality. As a result, the first transaction on a contract account wallet is usually expensive. Perhaps due to the aforementioned reasons, at the current moment, contract account wallets remain less widely used than externally owned accounts.

Control: Single vs. Multi-sig vs. MPC

A final variable in wallet options that we will discuss is whether they are controlled by a single user or multiple users. **A single user wallet is one that requires the private key of only one user to sign and approve transactions. Alternatively, multi-sig and MPC wallets are controlled by more than one user, requiring multiple users to approve transactions.** As discussed in the last section, multisig wallets, like Gnosis Safe, do this by requiring multiple users to sign an authenticating smart contract. **MPC wallets on the other hand, use an off-chain, cryptographic process called multi-party computation to break a wallet's private key into multiple pieces, and hand over the private key fragments to a set of users.** The pieces can be spliced together to form a complete private key and ultimately, allow a decentralized set of users to collaboratively approve transactions.

MPC wallets were invented to address the downsides of multisig wallets. Multisig wallets today often lack the ability to support new chains, given that the smart contract implementations of the wallets on each respective chain are distinct from one another. Furthermore, multisig wallets are operationally inflexible. Once a safe contract is created, it is difficult to change the threshold of signatures needed to execute transactions. For a growing and ever changing DAO or team that utilizes a multisig wallet, this can be a problem. MPC design on the other hand, is protocol agnostic (given the lack of dependency on a particular safe contract), and allows for continually fractioning of the private key and therefore modification of the operational threshold to sign transactions.

Figure 27: Comparison of single, multi-sig, and MPC wallets



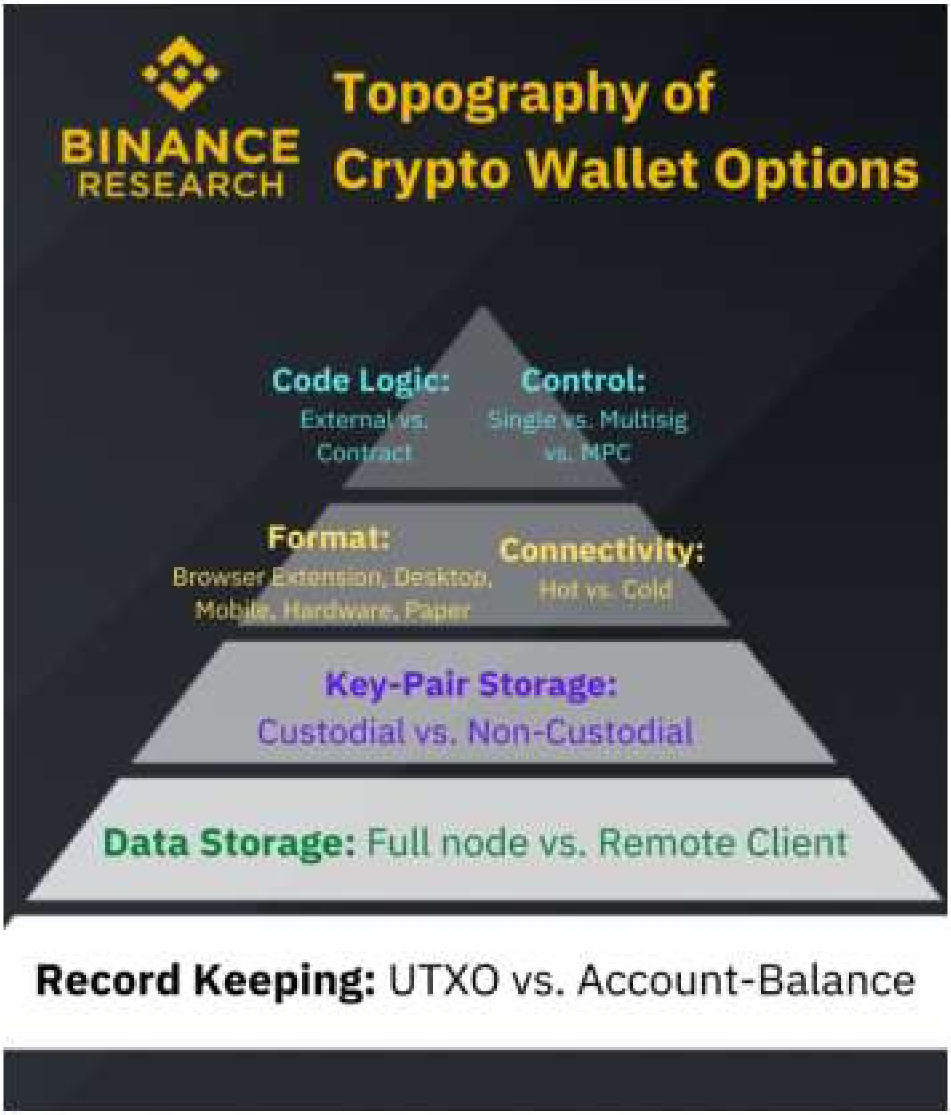
	Single	Multi-Sig	MPC
Removes single point of compromise for private key	✗	✓	✓
Multi User Approval	✗	✓	✓
Protocol Agnostic	✗	✗	✓
Modify quorums without creating new address	✗	✗	✓

Source: Binance Research

Topography of Crypto Wallet Options

The graphic below depicts a topography of crypto wallet options. Each step in the pyramid moves away from the most fundamental differences of wallet accounts to more abstract differences between wallet accounts. The bottom of the pyramid concerns base-layer differentiations in how different wallet options access blockchain data. The middle of the pyramid concerns what environment the private keys are in. The very top of the pyramid concerns progressions away from conventional wallet standards.

Figure 28: Topography of crypto wallet options


BINANCE RESEARCH
Topography of Crypto Wallet Options
Code Logic: External vs. Contract
Control: Single vs. Multisig vs. MPC
Format: Browser Extension, Desktop, Mobile, Hardware, Paper
Connectivity: Hot vs. Cold
Key-Pair Storage: Custodial vs. Non-Custodial
Data Storage: Full node vs. Remote Client
Record Keeping: UTXO vs. Account-Balance

Source: Binance Research

Trends to Watch in Crypto Custody

While the user experience of holding crypto has come a long way since the first wallet (the "Bitcoin-qt" made by Satoshi), there still requires further innovation to achieve mainstream adoption. Today, as made clear in **Comparing Wallet Options**, there are significant trade-offs between convenience and security when using a particular wallet option. Wallet developers, dApps, financial institutions, and regulators are all working towards a future in which crypto users do not need to sacrifice the security of their holdings for convenience, and vice versa.

In this section, we discuss some of the most anticipated trends in the crypto custody space. More specifically, we discuss how custody options will be impacted by these trends, and whether or not these trends are serving to further the convenience/security trade-off or rather, help mitigate the convenience/security tradeoff.

Account Abstraction

As discussed in the **Code Logic: External vs. Contract** section, in any smart contract blockchain today, there exists two kinds of wallet accounts: (1) Externally owned accounts (EOAs), which are simplistic wallet accounts that execute transactions using a wallet holder's private keys. and (2) Contract Accounts, are combination of an EOA and a smart contract. The EOA component of contract accounts is used to store private keys and trigger transactions by sending fees/gas to the smart contract. The smart contract component of contract accounts executes transactions sent to it by the EOA in an programmable and customized way. For example, Argent (social recovery of private-keys) and Gnosis (multi-signature verification), have used the smart contracts in contract accounts to enhance the functionality of wallets.

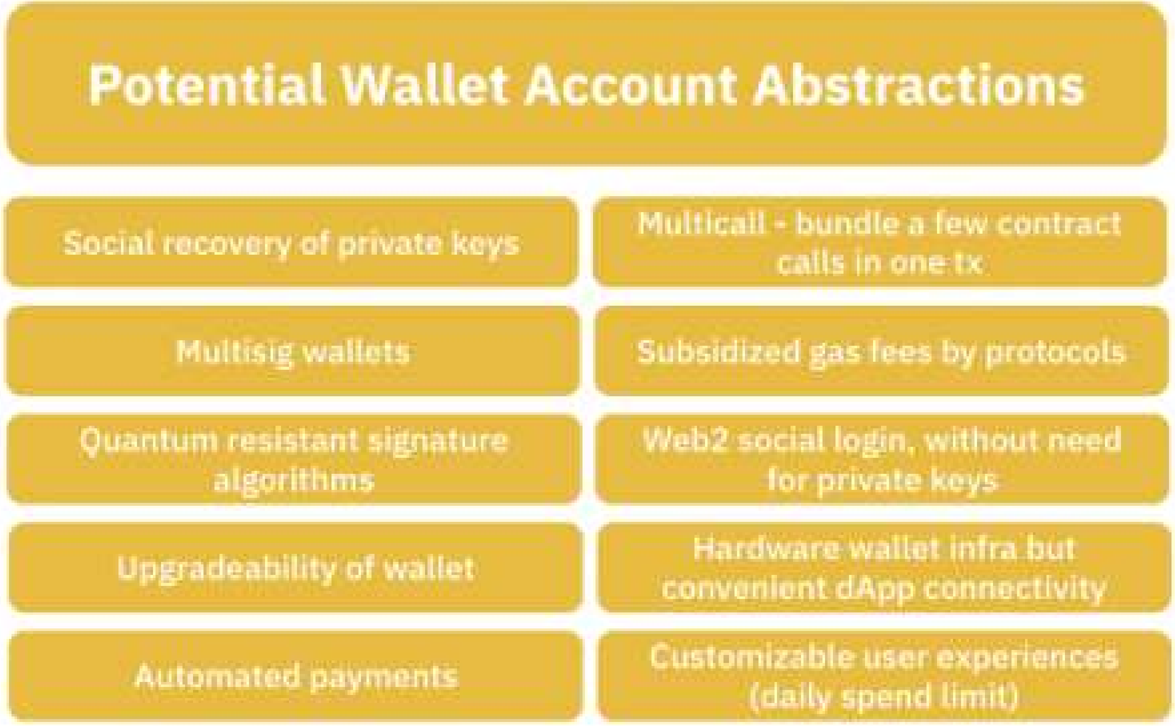
However, despite the innovations made by contract accounts thus far, contract accounts aren't as popular as conventional EOA based wallets such as Rainbow or Phantom. This may be due to the high costs associated with deploying the smart contract associated with a contract account or the lack of standards of implementing such contract accounts.

Protocol developers have acknowledged the potential of contract account wallets, and in turn, have sought to address existing drawbacks through a solution called "account abstraction."

Account abstraction seeks to "eliminate the existence of two types of accounts on smart blockchain platforms (EOA and contract) by unifying them." As such, every account will become a smart contract that can contain logic, implement flow, and maintain private keys.

The benefits that can arise from account abstraction are wide ranging. The chart below depicts a list of potential enhancements that account abstraction could bring to wallets. Most enhancements focus on improving the convenience or security of using a wallet.

Figure 29: Summary of customized account wallets and use cases



Potential Wallet Account Abstractions

Social recovery of private keys

Multicall - bundle a few contract calls in one tx

Multisig wallets

Subsidized gas fees by protocols

Quantum resistant signature algorithms

Web2 social login, without need for private keys

Upgradeability of wallet

Hardware wallet infra but convenient dApp connectivity

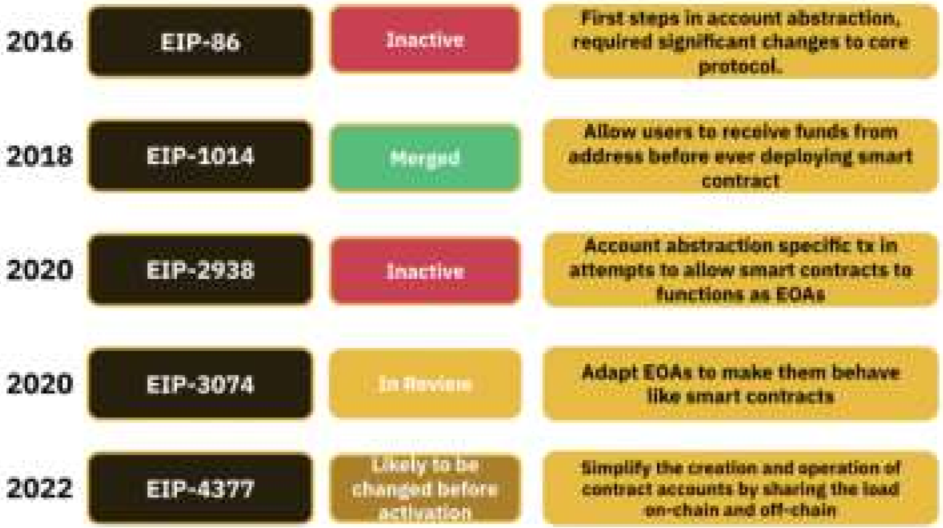
Automated payments

Customizable user experiences (daily spend limit)

Source: Binance Research

On Ethereum, there have already been a number of Ethereum Improvement Proposals (EIPs) moving closer towards full account abstraction.

Figure 30: EIPs related to account abstraction



2016	EIP-86	Inactive	First steps in account abstraction, required significant changes to core protocol.
2018	EIP-1014	Merged	Allow users to receive funds from address before ever deploying smart contract
2020	EIP-2938	Inactive	Account abstraction specific tx in attempts to allow smart contracts to functions as EOAs
2020	EIP-3074	In Review	Adapt EOAs to make them behave like smart contracts
2022	EIP-4377	Likely to be changed before activation	Simplify the creation and operation of contract accounts by sharing the load on-chain and off-chain

Source: Ethereum Foundation, Binance Research

Layer 2 chains (L2) are farther along with account abstraction.

- Optimism, through its very own OVM, has fully implemented a basic form of account abstraction. Optimism even tried to introduce three new functions in the OVM's execution manager that would provide users the ability to continuously upgrade their smart contract wallets. However, soon after, Optimism core developers removed this feature in concern that the upgrade wouldn't be compatible with the EVM.(11)

- StarkNet has also already implemented account abstraction. Furthermore, use cases of the account abstraction wallet model on StarkNet have already taken form. Argent, the L1 contract account wallet released a new wallet called Argent X on StarkNet in 2021, which is an account abstraction version of their mobile wallet. More recently, Visa announced that they have built an auto payment feature for Agent X also using account abstraction.(12)(13)

> *"Account abstraction has many potential use cases, especially on how the user experience on a digital wallet may be substantially enhanced with more flexibility embedded into user account to function more like a smart contract"*
>
> *- Catherine Gu, Visa(14)*

The reason why L2s are farther ahead with account abstraction development than L1 could be explained by two reasons. First, L2s haven't had to focus on protocol lawyer developments like a lot of L1s have, especially in the past couple of years. Second, since account abstraction relies on calling a smart contract to execute transactions, it is on average more computationally expensive to send a basic transaction with an account abstraction wallet as compared to a EAO wallet. Since gas price on L1 is much higher than L2s, it makes more sense to do computationally expensive transactions of account abstraction wallets on L2s rather than L1s.

In efforts to keep up with the innovations being made by account abstraction wallets, Metamask, a contract wallet, has recently released Metamask Snaps. Snaps is a pre-release software that plugins to Metamask allows users to extend the functionality of their wallet. Snaps do not execute like the smart contracts in the account abstraction model, rather they are executed in an isolated, sandboxed environment. Metamask users can use snaps to add new APIs to Metamask, add support for different blockchain protocols, or modify existing functionality using internal APIs.

Fiat On Ramps

As crypto becomes more institutionalized, fiat-on ramps are becoming more directly available for wallets.

For example, a payments infrastructure called Ramp, allows wallet developers to integrate geo-based fiat on-ramps into their products. With a few lines of code, wallet developers can integrate Ramp. After which, the users of the wallet can purchase crypto directly from their non-custodial wallet. Ramp handles all the relevant KYC, fraud, and compliance that goes into user requests to purchase crypto with a credit card, debit card, Apple Pay, or bank transfer. Ramp is also expanding quickly as it already provides coverage in 35 US states and territories and will expand to Europe and Global coverage in January 2023.[15] Some wallets like Trust Wallet and Argent are already using Ramp to provide fiat on-ramps to their users.

Another example of the acceleration of fiat on-ramps has been Stripe's recently announced fiat-to-crypto widget. The payment giant is going to offer a new product that "can be embedded in any crypto product so that users can enter their card information and acquire crypto."[16]

Vertical and Horizontal Scaling

Another trend to watch is how companies are vertically and horizontally scaling by offering wallet products.

Wallets that have historically been available only on one chain, are now horizontally scaling to become multi-chain. Self-custodial wallets such as Metamask and Trust Wallet have previously distinguished themselves for offering access to a number of different blockchains and cryptocurrencies. Now, wallets that have been previously isolated to one chain, like the Phantom Wallet and Casa, are expanding to other chains. Phantom announced in November that it would add support for Ethereum and Polygon, instead of solely Solana.[17] Casa, a popular Bitcoin self-custody firm, is adding Ethereum support to its platform in January 2023.[18]

Companies that have previously been isolated from the wallet market are vertically scaling to include wallets in their product offerings. Telegram, a popular encrypted instant-messaging platform is building out a self-custodial wallet. The wallet seems to complement Telegram's messaging app which provides users with encrypted, self-ownership over their messages. Users on the Telegram will be able to use their crypto wallet to similarly own their own data and their own private keys. The wallet will also provide convenient usage, allowing users to send crypto to one another within the app's interface.[19]

Privacy and Security

For custodial and non-custodial wallet options, privacy and security will continue to be a topic of focus.

Over this past year, there have been cases of centralized custodians leaking customer information and misusing customer deposits. As a result, paranoia around privacy and security around custodial wallet options is at an all time high. In response, centralized custodians have attempted to offer more transparency into their holdings. For example, Proof of Reserves (PoR) of centralized exchange balances has become standard over the course of 2022. As time goes on, there remains questions around if PoR should be a standard for centralized custodians, and how to best present PoR accounting publicly.

Decentralized, non-custodial wallets over the past year have faced criticism endangering users privacy and the security of the blockchain. For example, in November 2022, Infura, the centralized and primary node provider for Metamask wallets, announced that it would collect Metamask user's IP and Ethereum addresses. This prompted many Metamask users to question the wallet's devotion towards the privacy of its users. Furthermore, Infura has been said to control a large number of the nodes on Ethereum. Users also questioned whether an overarching, centralized node provider could serve as a single point of failure to Ethereum.[20]

However it should be noted that some non-custodial wallets are actively making steps to improve privacy and security. For example, just recently, in December 2022, Trust Wallet announced that it would be introducing a feature called the "Trust Wallet Security Scanner." The scanner is a built-in security feature that informs wallet users of potentially risky transactions. If a wallet user engages in a transaction with a risky or flagged address, a notification is prompted to the user asking them if they would like to continue with the transaction or cancel the transaction. As time goes on, many wallets will look towards privacy and security features like the Trust Wallet Scanner, to bolster the safety of their user's assets.

Wider dApp Accessibility

Lastly, dApps are becoming more accessible to wallets.

WalletConnect, a communications protocol for Web3, offers dApp access to a wide range of wallet formats. Version 1 of WalletConnect will be deprecated in March 2023 and will be replaced by a chain agnostic version of WalletConnect. Version 2 of WalletConnect will provide more coverage to wallets that are not widely interoperable with dApps or only have compatibility with a single-chain.[21]

Another story that may have implications for dApp accessibility is Apple's plans to let rival app stories on iPhones in the EU. Apple is preparing to "allow alternative app stores on its iPhones and iPads in Europe as soon as" 2023 to "comply with a new European competition law it had fought." For mobile wallets, this may allow broader access to dApps who wish to coalesce in alternative mobile app stores.[22]

Conclusion

The events that have gone on over the course of 2022, including centralized contagion, hacks, and frequent loss of private keys, have cultivated a pivotal moment and a time of increased focus on crypto custody. The space is rapidly evolving, with market participants attempting to find solutions to mitigate the convenience/security tradeoff, enhance the functionality of wallets, and overall, create a better UX of using the blockchain.

Understanding the complexities of crypto custody, from how a wallet works, to the different wallet options available, to future trends in the space, will allow you to better understand the transformation of crypto custody space as it unfolds before your eyes. Additionally, it will help you keep your crypto safe and find the best custody option for you.

To achieve widespread adoption, it seems clear that we must start by understanding crypto custody. Wallets are truly the portal to the blockchain and thus, must be tailored to the specific risk and UX preferences of each user. Wallets, even if abstracted, will forever remain a cornerstone of the user experience of blockchain technology. As time goes on, the wallet space will continue to evolve with its users and maintain options that suit the heterogeneous nature of a decentralized network.

References

1) https://cointelegraph.com/news/world-population-reaches-8-billion-but-how-many-are-in-crypto
2) https://research.huobi.com/#/ArticleDetails?id=358
3) https://www.redbooks.ibm.com/redbooks/pdfs/sg248525.pdf
4) https://open.spotify.com/show/3ibvcrJ87PAso4DBIiE5gn
5) https://cointelegraph.com/news/only-1-of-people-can-handle-crypto-self-custody-right-now-binance-ceo
6) https://twitter.com/vxunderground/status/1609969671179993088
7) https://www.gemini.com/cryptopedia/crypto-wallets-mobile-desktop#section-mobile-wallet-pros-and-cons-and-more
8) https://bitpay.com/blog/hardware-wallets-explained/
9) https://www.binanceinstitutional.com/
10) https://newsbtc.com/news/bitcoin/chainalysis-up-to/
11) https://medium.com/nethermind-eth/the-history-and-future-of-account-abstraction-10cb097ebdc8
12) https://www.argent.xyz/argent-x/
13) https://www.coindesk.com/tech/2022/12/20/visa-proposes-automatic-payments-using-ethereum-layer-2-solution-starknet/
14) https://twitter.com/catgu_/status/1604896035616264205
15) https://twitter.com/RampNetwork/status/1600112843134709762
16) https://stripe.com/en-gb-cy/blog/crypto-onramp
17) https://techcrunch.com/2022/11/29/solana-focused-crypto-wallet-phantom-adds-ethereum-and-polygon-support/
18) https://www.coindesk.com/tech/2022/11/30/bitcoin-custody-firm-casa-to-add-ethereum-support/
19) https://www.forbes.com/sites/ninabambysheva/2022/12/02/telegram-to-build-crypto-wallet-decentralized-exchange-following-ftx-collapse/?sh=968c49e59e98
20) https://decrypt.co/115486/infura-collect-metamask-users-ip-ethereum-addresses-after-privacy-policy-update
21) https://medium.com/walletconnect/walletconnect-v2-0-protocol-whats-new-3243fa80d312
22) https://www.reuters.com/technology/apple-prepares-allow-alternative-app-stores-iphones-ipads-bloomberg-news-2022-12-13/
23) https://en.cryptonomist.ch/2022/11/16/ledger-trezor-sales-grow-300/
24) https://www.alchemy.com/overviews/mpc-wallet
25) https://www.fireblocks.com/blog/mpc-vs-multi-sig/
26) https://aprendeblockchain.wordpress.com/a-comparison-between-utxo-and-account-based-models/
27) https://xangle.io/en/insight/research/62a830eee74de2fd402eafe3
28) https://www.horizen.io/blockchain-academy/technology/expert/utxo-vs-account-model/#:~:text=The%20UTXO%20model%20is%20a.constructions%2C%20as%20well%20a%20sharding

29) https://jcliff.medium.com/intro-to-blockchain-utxo-vs-account-based-89b9a01cd4f5
30) https://docs.safepal.io/blockchain-tutorials/utxo-what-is-it-and-how-to-use-it
31) https://academy.binance.com/en/glossary/unspent-transaction-output-utxo
32) https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/
33) https://dl.ebooksworld.ir/motoman/Mastering_Ethereum_Andreas.M.Antonopoulos.www.EBooksWorld.ir.pdf
34) https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/
35) https://www.blockchain.com/explorer/charts/blocks-size
36) https://ethereum.org/en/developers/docs/nodes-and-clients /
37) https://bitpay.com/blog/hardware-wallets-explained
38) https://www.gemini.com/cryptopedia/hardware-wallets-crypto-security#section-non-custodial-and-cold-wallets
39) https://www.gemini.com/cryptopedia/paper-wallet-crypto-cold-storage#section-wheres-my-change
40) https://academy.binance.com/en/articles/crypto-wallet-types-explained
41) https://dune.com/degenerate_defi/exchange-wallet-balances
42) https://beincrypto.com/crypto-wallets-users-grew-by-over-6-in-2022-huobi/
43) https://cryptoslate.com/research-2nd-december-the-15m-bitcoin-just-went-into-self-custody/
44) https://www.investopedia.com/tech/explaining-crypto-cryptocurrency
45) https://www.kraken.com/learn/how-do-cryptocurrencies-use-cryptography
46) https://www.gemini.com/cryptopedia/public-private-keys-cryptography
47) https://www.educative.io/answers/how-is-sha-256-used-in-blockchain-and-why
48) https://cointelegraph.com/podcasts
49) https://resources.infosecinstitute.com/topic/blockchain-and-asymmetric-cryptography
50) https://metamask.zendesk.com/hc/en-us/articles/360020091432-How-does-MetaMask-generate-your-keys-
51) https://www.blockplate.com/blogs/blockplate/list-of-bip39-wallets-mnemonic-seed
52) https://medium.com/free-code-camp/how-to-generate-your-very-own-bitcoin-private-key-7ad0f4936e6c
53) https://medium.com/the-capital/what-is-crypto-wallet-encryption-and-private-public-keys-part-2-of-3-9044592940e1
54) https://cryptoslate.com/research-2nd-december-the-15m-bitcoin-just-went-into-self-custody/
55) https://www.gemini.com/cryptopedia/crypto-wallets-mobile-desktop#section-mobile-wallet-pros-and-cons-and-more
56) https://bitpay.com/blog/hardware-wallets-explained/
57) https://www.coindesk.com/tech/2023/01/11/ethereum-upgrade-could-make-it-harder-to-lose-all-your-crypto/
58) https://hackernoon.com/what-is-account-abstraction-and-why-is-everyone-talking-about-it

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to, the crypto ecosystem, blockchain technologies, and the latest market themes.

Mac Naggar, Macro Researcher Intern

Mac is currently working for Binance on their Macro Research team. Prior to joining Binance, he worked as a Web3 Product Manager for HSBC's Global Ventures, Innovation, and Partnerships team. Additionally, Mac has had experience on the trading side, spending time with Morgan Stanley's Fixed Income Division, Algorand's Capital Markets Team, and CrossTower's Digital Assets Trading Desk. Mac is currently a student at Cornell University, where he is studying Industrial Labor Relations, CompSci, and Business. His sector interests primarily lie in Blockchain Design & Interoperability, DeFi, DeSo, and Institutional Adoption.

Read more

https://research.binance.com/en/analysis

Share your feedback

https://tinyurl.com/bnresearchfeedback

General Disclosure: *This material is prepared by Binance Research and is not intended to be relied upon as a forecast or investment advice, and is not a recommendation, offer or solicitation to buy or sell any securities, cryptocurrencies or to adopt any investment strategy. The use of terminology and the views expressed are intended to promote understanding and the responsible development of the sector and should not be interpreted as definitive legal views or those of Binance. The opinions expressed are as of the date shown above and are the opinions of the writer, they may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources deemed by Binance Research to be reliable, are not necessarily all-inclusive and are not guaranteed as to accuracy. As such, no warranty of accuracy or reliability is given and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by Binance. This material may contain 'forward looking' information that is not purely historical in nature. Such information may include, among other things, projections and forecasts. There is no guarantee that any forecasts made will come to pass. Reliance upon information in this material is at the sole discretion of the reader. This material is intended for information purposes only and does not constitute investment advice or an offer or solicitation to purchase or sell in any securities, cryptocurrencies or any investment strategy nor shall any securities or cryptocurrency be offered or sold to any person in any jurisdiction in which an offer, solicitation, purchase or sale would be unlawful under the laws of such jurisdiction. Investment involves risks.*