BINANCE RESEARCH

Road to One Billion On-chain Users

JUNE 2024

Joshua Wong

Table of Contents

1 Key Takeaways

- The rate of adoption of blockchain networks has been significantly slower than the rate of adoption of social media networks. Since the launch of Bitcoin in 2009, the total cryptocurrency users has reached approximately 560 million as of today. TikTok and Facebook only took 5 and 8 years respectively to reach 1 billion users each.

- Decentralized systems are by nature more complex than centralized systems. Multiple decentralized systems embodied by the multi-chain world we live in scales complexity exponentially from the end user's perspective. Improving blockchain UI/UX and cross-chain interoperability is the next step to onboarding the masses, whether institutional or retail.

- Many blockchain projects today are focused on creating decentralized alternatives to existing centralized products and services. The DeFi summer of 2020 gave us the basic building blocks for on-chain financial systems. For decentralized applications ("dApps") to gain significant market share from their centralized counterparts, they must at least be as convenient, user friendly, and easy to use, if not more so.

- This report will look at three categories of future users: (1) Institutions, (2) Retail Users, and (3) Crypto Skeptics. It will analyze the various infrastructure-related obstacles each group faces in adopting decentralized systems, and dive into prominent projects addressing some of these user pain points. These infrastructure pieces are essential building blocks which will pave the road to one billion on-chain users.

2 Introduction

Blockchain technology allows for the existence of trustless, verifiable digital ownership. This has the potential to revolutionize the way the Internet works. As the Internet becomes ever more intertwined with industry and commerce, the demand for verifiable digital scarcity and ownership enabled by blockchain technology will likely continue to grow.

In order for blockchain technology and the concept of 'digital ownership' to reach mass adoption and usage on a global scale, two things are required:

- First, there must be on-chain applications that people want to use.
- Second, people must be able to understand and easily access these applications.

The advancements sprouting from the **DeFi summer of 2020 gave us the basic building blocks for on-chain financial systems** - the beginnings of on-chain applications that people want to use. Moving forward towards a world where blockchain usage is globally widespread, the blockchain industry must now **create the additional tools, rules, and technology required to make digital ownership convenient, safe, and accessible to the masses.** These infrastructure pieces are essential building blocks which will pave the road towards the onboarding of the next billion on-chain users, and will be the focus of this report.

The idea of 'ownership' is fundamental to the modern world of commerce and industry. In the physical world, we created laws, houses, locks, safes, trusts, and all other manner of inventions to make ownership possible, feasible, and enforceable. If 'digital ownership' is to come into existence and be widely adopted, **the blockchain industry will need to invent the digital equivalents of these locks, safes, trusts etcetera** - tools which make ownership in the physical world readily available to the masses. This report will focus on some of the most prominent technological and ideological hindrances to the mass adoption of digital on-chain ownership, and how the crypto industry is working to address them on its road to mass adoption.

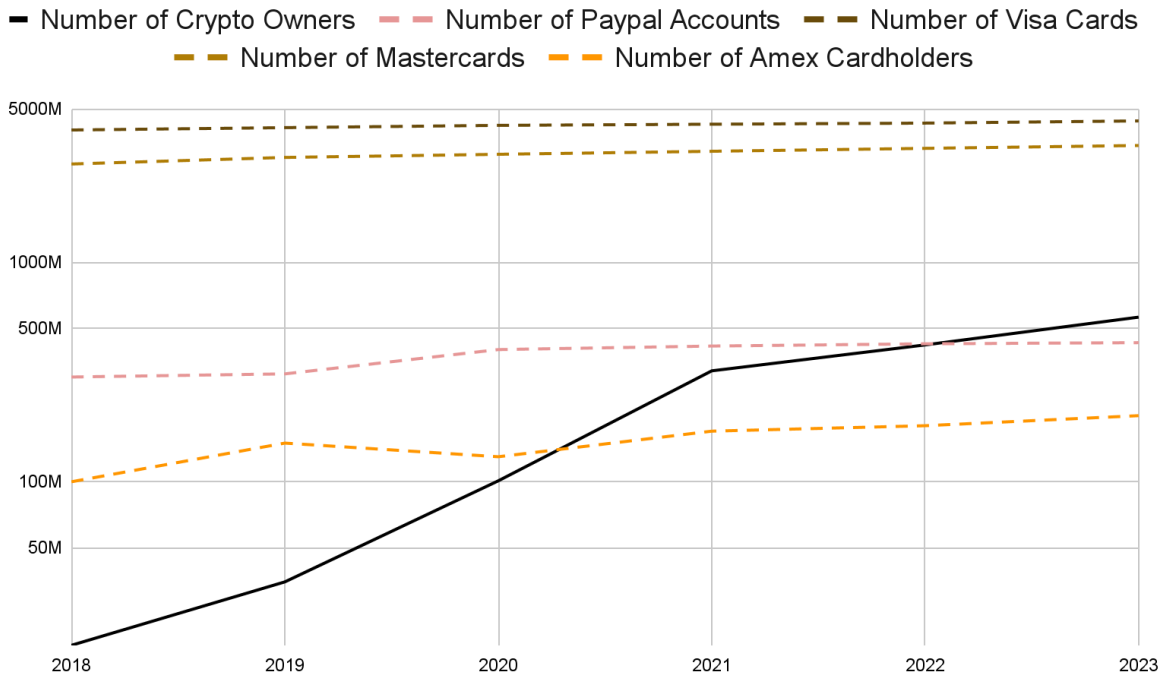
Please note that the mention of specific projects in this report does not constitute an endorsement or recommendation by Binance. Instead, the projects cited are merely used for the purpose of illustrating the aforementioned concepts. Additional due diligence should be taken to better understand the projects and associated risks

3 The Current State of Crypto Adoption

The modern world can be described as being in the Exponential Age of technology. New technology is being adopted at faster rates than ever before. OpenAI's ChatGPT became the fastest growing application to ever launch, with the web application reaching 1 billion monthly visitors just 3 months after launch. TikTok launched in 2016 and reached 1 billion users in just 5 years by 2021. Facebook, which launched in 2004, took 8 years to reach 1 billion users in 2012. The Internet itself became available for public use in 1993 and only crossed the 1 billion user mark in 2005, taking 12 years. There is no doubt that new technology is being adopted and proliferated at a faster rate than ever before.

While the rate of crypto adoption has not matched that of the social media giants or ChatGPT's, its growth has certainly been nothing to sneeze at. Fifteen years since the launch of Bitcoin in 2009, **we currently sit at around 560 million crypto owners worldwide.**[1] This is an exponentially faster rate of growth than that experienced by the largest traditional payment networks in the past five years.

Figure 1: Number of Crypto Owners Compared to Traditional Payment Networks in Logarithmic Scale

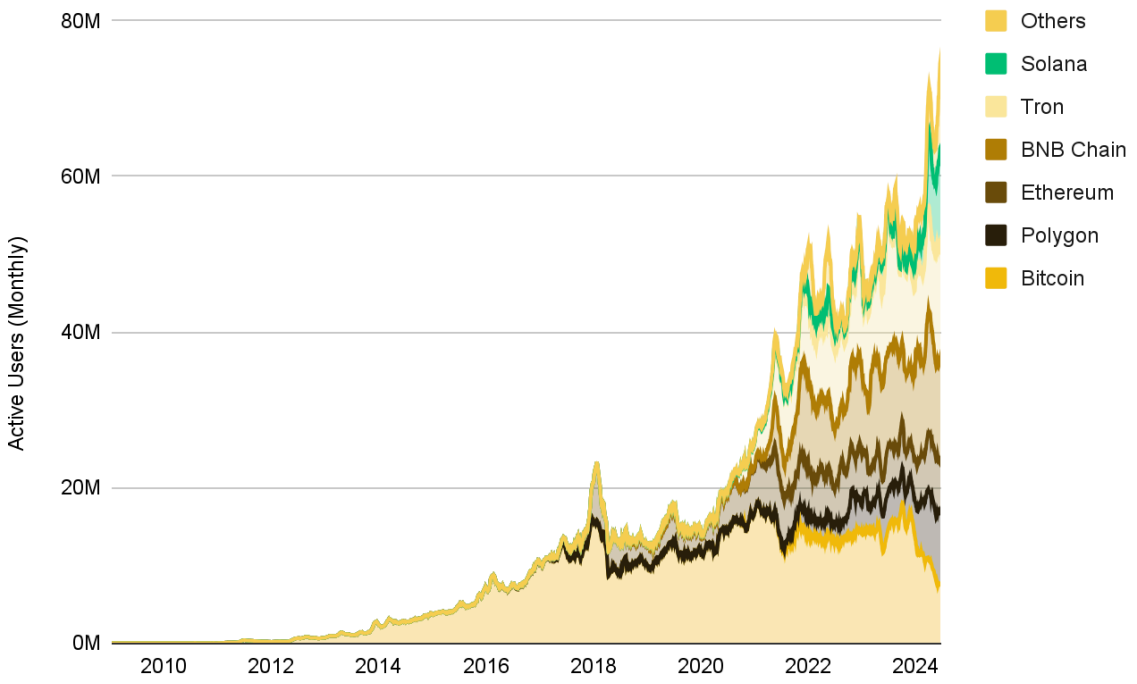


Source: Triple-A, Binance Research, as of May 2024

This 560 million figure however is inclusive of a large proportion of users who hold their assets on centralized exchanges or other digital asset custodians. Looking at on-chain

metrics, the combined monthly active users across the top 20 Layer 1 blockchains **adds up to only just above 75 million on-chain users** as of 2024.

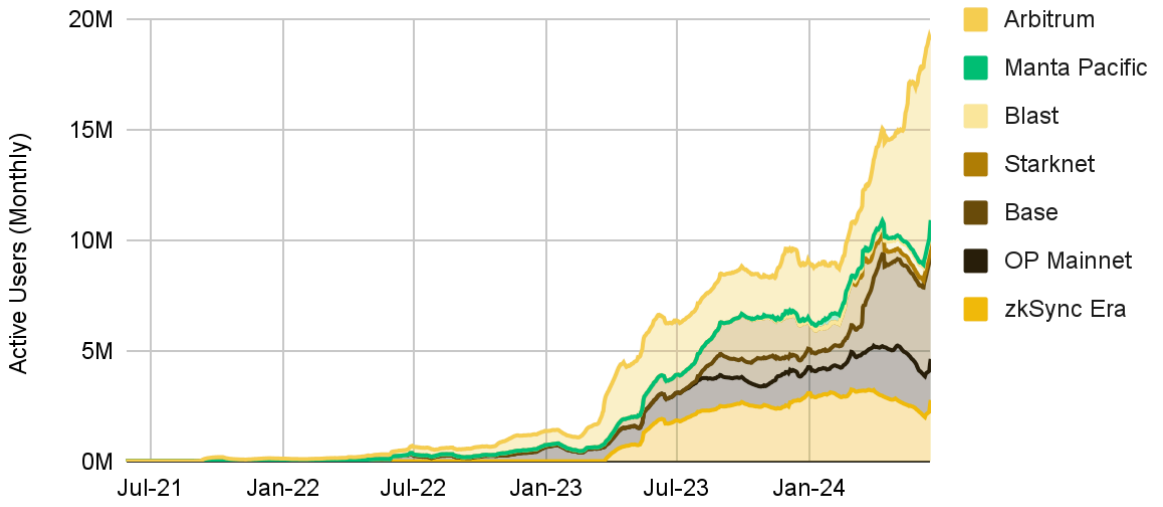
Figure 2: Monthly active users of the top 20 Layer 1 blockchains



Source: Token Terminal, Binance Research, as of June 20, 2024

Even if we add active addresses across the most popular Layer 2 chains (which total just under 20 million monthly active users), we would have a grand total of only around **100 million on-chain users across all the major Layer 1 and Layer 2 chains combined**. This 100 million figure may also be inflated, as many crypto users use multiple addresses which could lead to a significant degree of double counting, particularly between the Ethereum and Ethereum Layer 2 active user addresses.

Figure 3: Monthly active users of the top 7 Ethereum Layer 2



Source: Token Terminal, Binance Research, as of 20 June 2024

While the familiar user experience offered by centralized exchanges ("CEXes") makes it simple for new users to purchase crypto assets, **this intuitive experience is still lacking in on-chain applications**, creating more friction for new users to bring their funds on-chain. While centralized crypto solutions undeniably play an important role in the ecosystem, bringing users on-chain is of crucial importance and is key to unlocking the full potential of blockchain technology. As the popular maxim goes: "not your keys, not your coins".

One plausible explanation for the slower rate of growth of blockchain adoption when compared to that of social media networks could be the **relative lack of useability that on-chain crypto applications and blockchains suffer from**. This would also explain why more crypto owners still choose to custody their assets on CEXes, rather than bring them into on-chain self-custody. **Setting up a Facebook or CEX account using an email address is much simpler than setting up a self-custodial wallet.** As the crypto industry continues its march towards global adoption, it will need to develop infrastructure and tooling that **allow people and institutions to onboard onto blockchains just as easily as they might create an Instagram account.**

This report will look at some of the most prominent pain points which hinder mass adoption of blockchains, categorized into those faced by three main categories of potential future users:

1. **Institutions**
2. **Retail**
3. **Crypto Skeptics**

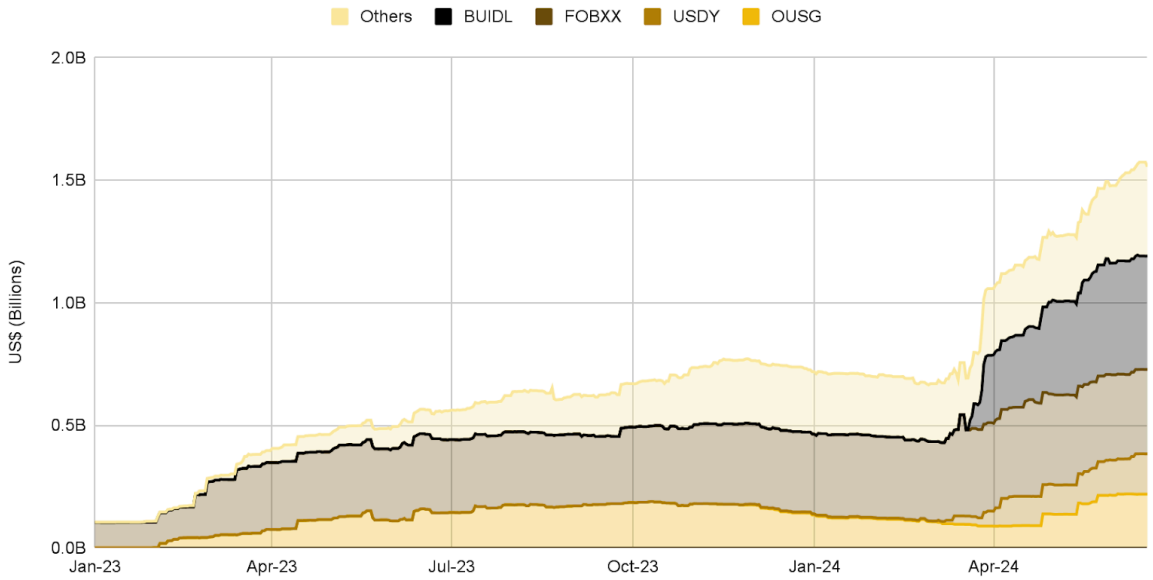
We will also highlight several projects as case studies, to illustrate how some teams are working on improving the on-chain experience, and in driving on-chain adoption.

4 Institutions

Much like the early days of the Internet, **crypto adoption was largely driven by retail users during its early days** following the launch of Bitcoin in 2009. Since then, blockchain technology and the crypto asset class has taken large steps towards global recognition and adoption, garnering significant interest from the largest institutions in the world.

A prominent recent development was **BlackRock's foray into the tokenized U.S. treasury space**, with the launch of its BlackRock USD Institutional Digital Liquidity Fund ("BUIDL") fund in March of this year. BUIDL is available to KYC-ed institutions for investment through Securitize, a tokenized real world asset platform built on Ethereum.

Figure 4: Market capitalization of tokenized US treasury products



Source: rwa.xyz, Binance Research, as of 20 June 2024

The growth of BUIDL has outstripped other tokenized treasury products, overtaking Franklin Templeton's Franklin on-chain U.S. Government Money Market Fund's total market capitalization ("FOBXX") within just a few months of its launch. The total on-chain market capitalization of such **tokenized U.S Treasury products now sits at over US$1.5B.**

Apart from tokenized real-world assets ("RWAs"), institutions have also demonstrated their appetite for native digital assets, namely Bitcoin and Ethereum. Inflows to the BTC and ETH ETFs have been consistent, with the **combined market capitalization of each ETF sitting at US$80B and US$269M** respectively. In 2024, two publicly traded companies, Semler Scientific and DeFi Technologies followed in Microstrategy's footsteps, adopting Bitcoin as their companies' primary treasury asset.

Institutions are beginning to recognize the potential and value blockchains bring with their ability to provide a trustless and global environment to custody and transact tokenized real world value. There is also a growing institutional movement towards recognizing the value of digitally native assets like BTC and ETH. However, in order to achieve widespread institutional adoption the crypto industry will need to ensure **the necessary tools** are made available to institutions to **allow for convenient and low risk custody, and management of digital assets and tokens.** The useability of on-chain accounts must be improved to match the convenience offered by banks.

To achieve widespread institutional adoption, the crypto industry must address these two fundamental functions of institutional-grade on-chain usage:

1. Institutional custody

Institutional-grade custody solutions are crucial to onboarding institutions en-masse onto blockchains. The majority of the traditional finance and banking world is built to service institutions. For institutions to feel comfortable moving even part of their assets or business onto distributed ledgers, the on-chain products and services available must be equally robust, if not more so.

2. Transactions and chain abstraction

Liquidity fragmentation across the current multi-chain world is a significant hindrance to institutional adoption. Multiple distributed ledgers written in multiple coding languages accessed by multiple wallets is also far too complex for the majority of institutions looking to adopt distributed ledgers at scale. Improving on-chain abstraction capabilities and cross-chain interoperability will make it significantly less costly and resource intensive for institutions to adopt blockchain technology.

4.1 Institutional Custody

As more institutions invest in digital assets and tokens, the institutional demand for on-chain functionality will naturally increase, as will the demand for custody solutions that offer greater security and greater flexibility. Blockchains have the unique capability over traditional financial systems of having inherent interoperability. For example, once an institution obtains on-chain custody of the Blackrock-issued BUIDL tokens, they could theoretically **trade or borrow against those tokens** via another Ethereum smart-contract application (eg. Uniswap or Aave) **without the need to engage any additional intermediaries.**

The native interoperability and seamless global settlement environment that blockchains offer open up a new world of possibilities for the institutional management of their digital financial assets. To access these capabilities however, institutions must be brought

on-chain and granted convenient and secure self-custody of their digital assets. Digital asset storage solutions should **allow institutions to benefit from the interoperability of holding their assets on-chain, whilst not compromising on security.**

Some of the most widely used wallet and self-custody solutions (eg. MetaMask, Phantom, Ledger etc.) may work well for the average retail user, but institutional users who typically deal with much larger asset valuations will likely require greater levels of security.

Broadly speaking , there are three ways to manage an on-chain account and its associated private key.

1. **Single signer systems** are used in many of the most popular retail-targeted crypto wallets like Metamask or Phantom. **They allow anyone with possession of a given private key full access to any funds stored in its associated on-chain account.**
2. **Multi-signer ("Multi-Sig") systems** are used by many DAO treasuries, most popularly through the Gnosis Safe decentralized application. **A Multi-Sig wallet is an on-chain smart contract that acts as a collaborative escrow account.** It requires the signature of x/n whitelisted private keys in order to execute transactions using the assets stored inside it.
3. **Multi-party computation ("MPC") systems** were designed with institutional use cases in mind, intended to offer improved flexibility over Multi-Sigs. An MPC wallet exists on-chain as a single wallet address with a single private key. That **private key is broken up into shares, encrypted, and divided off-chain among multiple parties.**

Figure 5: Comparing Single, Multi-Sig, and MPC Systems

	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

While single-signer wallets may serve retail users well. Institutions which generally require a greater level of security often opt for Multi-Sig wallets, or in more recent times MPC wallets.

MPC wallets possess certain capabilities over Multi-Sig wallets which are particularly useful for institutions. As shown in the figure above, MPC wallets are protocol agnostic. MPC wallets divide the private key off-chain rather than using smart contracts like the Multi-Sig wallet. Multi-party computation works on the standardized cryptographic signature algorithm (ECDSA or EdDSA) that is used across most blockchains. This means that **institutions using MPC can quickly bring new cryptocurrencies and blockchains onto their systems,** without needing to ensure the new blockchain or wallet supports multi-sig smart contracts.

This is crucial towards widespread institutional adoption of blockchains in a multi-chain world, where institutions are reluctant to commit resources to integrate with a single blockchain, when there is the risk that they will need to switch blockchains in the future. We will touch more on this topic and chain abstraction in the next section.

Apart from being chain agnostic, **MPC technology allows for greater operational flexibility for institutions compared to Multi-Sig wallets.** Multi-Sig wallets are pre-set smart contracts. Once a Multi-Sig wallet is created, the 'M of N' transaction approval structure is fixed. If a new employee is hired and an institution wants to change the signature of a Multi-Sig wallet from '3 of 4' to '3 of 5', for example, an institution would need to:

1. **Create a new Multi-sig wallet** with the new configuration
2. **Move all their assets** from the old to the new wallet
3. **Notify all counterparties** that their wallet address has changed

Step (3) is extremely challenging and costly, especially for institutions with numerous counterparties. It is also risky as counterparties could accidentally send funds to the old deposit address, where those funds could be lost forever.

In contrast, MPC wallets enable ongoing modification and maintenance of the signature scheme. For instance, changing from a '3 of 4' configuration to a different set-up would require the current shareholders' agreement on the new distributed computation and the inclusion of a new user share. Throughout this process the blockchain wallet address (deposit address) is maintained, so that:

1. **Institutions do not need to create a new wallet**
2. **Institutions do not need to move any funds**
3. **Their counterparties can continue to use the existing address**

We covered the topic of crypto custody in our previous report "Wallets: A Deep Dive into Crypto Custody". Check it out for a more detailed dive into the world of crypto wallets.

Fireblocks

Fireblocks is one of the companies pushing the forefront of institutional-grade custody. In 2020, they released MPC-CMP, an open-source, free to use MPC protocol developed by the Fireblocks R&D team. **The MPC-CMP, while based on its predecessor Gennaro and Goldfeder's MPC, allows for transactions to be signed up to 800% faster.**

In MPC algorithms, the primary factor that slows down signing is the communication latency between the devices holding the key shares. Every communication round introduces additional latency. By using non-interactive signing and pre-processing, **Fireblocks' MPC-CMP reduces the signing process to just 1 round**. This is a significant improvement in the time it takes to complete the signing process compared to the previous algorithms such as Gennaro and Goldfeder (9 rounds), Lindell et al. (8 rounds), and Doerner et al. (6 rounds).

Figure 6: Comparing MPC Algorithms

Algorithm	Transaction Rounds	Universally Composable	Cold Storage Compatible	Peer-Reviewed	Open-Source
Gennaro and Goldfeder	9	✘	✘	✔	✔
Lindell et al.	8	✘	✘	✔	✘
Doerner et al.	6	✘	✘	✔	✘
MPC-CMP	1	✔	✔	✔	✔

Source: Fireblocks, Binance Research

Ceffu

Ceffu is another player in the institutional digital asset custody space. Ceffu also makes use of MPC algorithms to ensure the safety of their clients' funds. With cold, warm and hot wallets, **Ceffu offers a variety of solutions to suit a wide range of institutional customer needs** including cold storage staking as well as liquid staking through its hot and cold wallet solutions, **allowing institutions to generate yield on their treasury assets.**

Ceffu also offers **off-exchange settlement through its partnership with Binance Exchange**. Ceffu's MirrorX solution allows its institutional clients to delegate a specified amount of their assets held in Ceffu's custody to a designated Binance sub-account

instantaneously. Through MirrorX, institutions can **trade on the world's largest crypto exchange by volume, whilst retaining the full security offered by Ceffu's custody solution.** Ethena, the project behind the USDe synthetic dollar, announced its partnership with Ceffu in March 2024, making use of MirrorX to manage its collateral whilst retaining maximum security.

4.2 Transactions and chain abstraction

Considering their scale and volume, institutions require deep liquidity in order to execute transactions in an effective and capital efficient manner. **The multi-chain world we currently live in results in liquidity being fragmented across multiple siloed distributed ledgers and Layer2s.** This reduces accessibility for institutions looking to adopt blockchains. The lack of blockchain interoperability also necessitates that institutions decide on a specific blockchain ecosystem to adopt. **This requires a high set-up cost which also siloes that institution into the initially chosen blockchain ecosystem.** Institutions may be reluctant to put in the time and money to integrate with a specific blockchain, when it remains unclear whether they will still want to utilize that blockchain down the line, or move to a different one, which would require significant re-investment.

For these reasons, **chain abstraction has become an important development in the journey to bring institutions on-chain**. Projects focused on chain abstraction are building the necessary infrastructure to **unify multi-chain asset and account management**. This would allow users to more easily and conveniently access decentralized applications and assets that exist across the multitude of distributed ledgers currently in existence. Currently, users need to set up and maintain a separate account and private key for accounts on different blockchains. **Chain abstraction has the potential to allow users to control accounts and assets held on multiple blockchains using a single private key.** This creates a much more attractive and easily adoptable on-chain environment for institutions to integrate with.

Axelar

Axelar, developed using the Cosmos SDK by the team at Interop Labs, is a Proof-of-Stake ("PoS") network that acts as a communications layer for decentralized applications to interact across both the EVM and Cosmos ecosystems. **It enables the transfer of tokens, smart contract calls, and general messaging, all overseen by a network of validators.** These validators operate nodes to monitor the state of the network, authenticate transactions, and manage cross-chain communication. As of today, Axelar connects over 50 blockchains via its secure, scalable network.

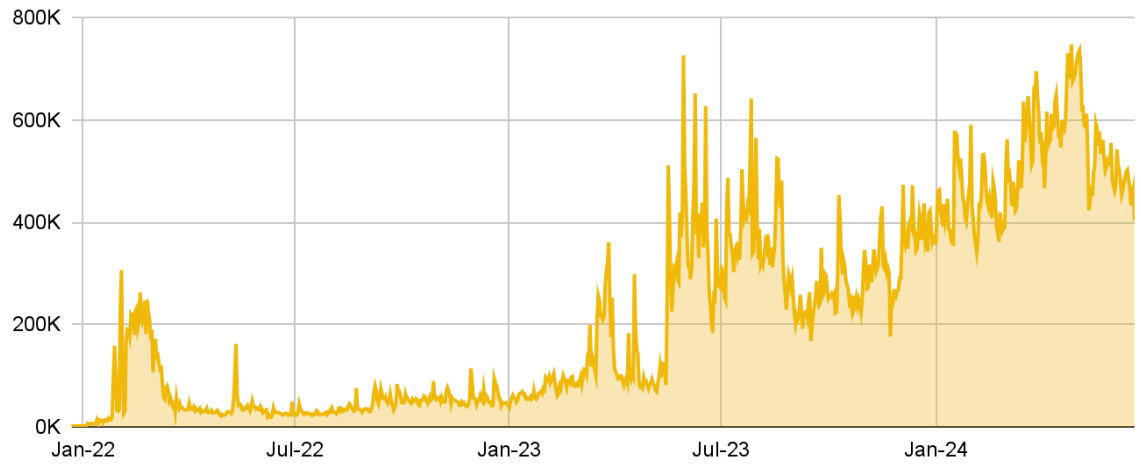
We covered Axelar alongside some of the other prominent cross-chain interoperability projects in one of our previous articles ‘Decoding cross-chain interoperability’.

Notably, Axelar has witnessed some initial success in partnering with institutions to drive blockchain developments:

- In May 2024, Deutsche Bank announced their partnership with Interop Labs, the team behind the Axelar Network Project. Interop Labs will support Deutsche Bank’s effort as it joins Project Guardian, the initiative to test asset tokenization in a regulated environment, led by the Monetary Authority of Singapore (MAS). Within the Project Guardian framework, **Deutsche Bank aims to explore the functionalities of an open architecture and interoperable blockchain platform.**
- In November 2023, the Axelar team also made headlines with their successful proof-of-concept collaboration with Onyx, J.P Morgan’s blockchain platform. This collaboration was also part of Project Guardian. As part of the proof-of-concept, **Onyx leveraged Axelar’s cross-chain technology to enable interoperability with a private and permissioned blockchain**, allowing for the introduction of composability and programmability into cross-chain portfolio management.

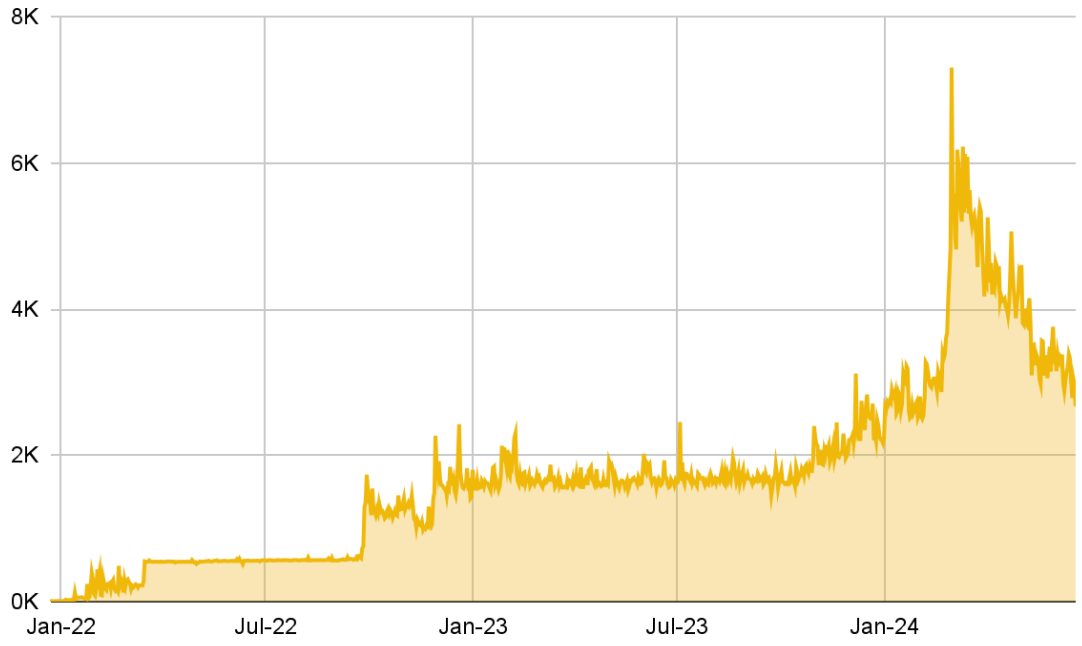
Since its involvement with Project Guardian, the Axelar network has experienced a consistent growth in its daily active addresses as well as daily transactions.

Figure 7: Axelar Daily Transactions



Source: Artemis, Binance Research, as of June 20, 2024

Figure 8: Axelar Daily Active Addresses



Source: Artemis, Binance Research, as of June 20, 2024

Project Guardian

Another notable initiative that has the potential to drive institutional adoption is Project Guardian. **Project Guardian is an initiative to test asset tokenization in a regulated environment**, led by the Monetary Authority of Singapore (MAS). As stated on their official website, the objectives of Project Guardian are to:

1. **Formulate industry standards** for asset tokenisation on a commercial scale.
2. **Establish policy guidelines and frameworks**. Define acceptable governance model or accountability; Technical standards for digital assets.
3. **To develop a sound and sustainable digital asset ecosystem** with commercial use-cases, guided by policy considerations and frameworks

It has the following **Focus Areas**, with open and interoperable networks being first on the list:

1. **Open and Interoperable Networks**

   Explore open, interoperable networks that enable digital assets to be traded across platforms and liquidity pools

2. **Trust Anchors**

   Establish a trusted environment through a common trust layer of independent trust anchors with risk management discipline to screen and onboard entities

3. **Asset Tokenization**

   Examine the representation of securities in the form of digital bearer assets and tokenized deposits issued by financial institutions.

4. **Institutional Grade Financial Protocols**

   Study the introduction of regulatory safeguards and controls into financial protocols to mitigate against market manipulation and operational risk.

As of 2024, Project Guardian has attracted an impressive amount of support and participation from some of the largest financial institutions around the world - **strong indication of the growing institutional interest in both tokenization as well as building open, global, interoperable distributed ledger networks.**

Figure 9: Logos of financial institutions involved in Project Guardian

Source: Project Guardian, Binance Research

5 Retail

On a whole, retail users would benefit from the same improvements that institutions would, namely greater convenience and greater security. Compared to institutions, the average retail user often prioritizes convenience, but it is essential to ensure that user-friendly solutions do not compromise on security.

For retail users in particular, **building intuitive mobile-enabled applications UI/UX is crucial**. As of 2023, **nearly 98 percent of internet users aged 16 to 64 worldwide owned a mobile phone**. Whereas only approximately 58 percent of the global population aged 16 to 64 and using the internet possessed a laptop or desktop computer.[2] The growing trend in people accessing the Internet via mobile device is strong. Today, the most popular Web3 wallets allow users to browse and access other dApps directly within the mobile application (eg. Binance Web3 Wallet, Metamask, Phantom).

Crypto software built for retail users needs to be intuitive to use, and widely accessible. This report will focus on two key pieces of crypto infrastructure that are essential for mass adoption of blockchains by retail users:

1. Account management

With the rise of fintech and neobanks, retail users have become used to easily accessing their finances via mobile applications. At the current stage, many crypto wallets still have significant room to improve. For example, requiring the user to manage their own seed phrase is difficult for many as it is an entirely alien concept to a large part of the population. The crypto industry must continue to innovate on user UI/UX, particularly on the mobile front, in order to build intuitive applications that are easy to pick up and use right away.

2. Accessible on/off-ramps

Successfully onboarding a billion on-chain users requires ensuring that average users can transfer funds on-chain both cheaply and quickly. Fiat on/off-ramps are the bridge between the massive world of traditional finance, and the comparatively tiny but blossoming on-chain world. For the on-chain world to flower, it needs a constant supply of liquidity to flow to it from traditional finance rails. Globally accessible and affordable fiat on-ramps are crucial to getting more retail users on-chain en masse.

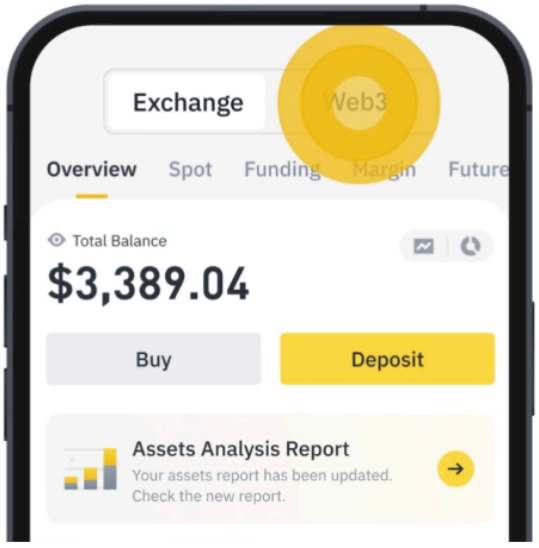
5.1 Account management

On-chain account management, and the management of seed phrases in particular, is a significant pain point hindering the widespread retail adoption of blockchains. Retail banking services have accustomed the general public to 'digital-ownership-as-a-service'. **Banks provide services such as customer support lines and password recovery mechanisms.** They also maintain a centralized mobile application that allows customers to view and spend their balances of digitally-represented money. While these exact services cannot exist in the decentralized on-chain space as they do in traditional banking, some Web3 projects are taking the steps to bridge the gap. To make users' transition to self-custody as painless as possible, **the industry must build products which offer familiar and intuitive user interfaces that allow for self-custody without sacrificing security.** Many Web3 companies have taken reference from the fintech and digital banking revolution that has occurred, building sleek and intuitive crypto mobile wallets which allow for seamless access into the on-chain world.

Binance Web3 Wallet

The Binance Web3 Wallet, which launched in November 2023, is a self-custody crypto wallet built as an extension to the Binance mobile application. **Housing the Web3 Wallet within the existing Binance application makes it easy for Binance's existing ~200 million users to transition into on-chain self-custody.** The Binance Web3 Wallet allows users to access the on-chain world of dApps via a familiar centralized exchange login and mobile application.

Figure 10: Binance Web3 Wallet accessible within the existing Binance mobile application



Source: Binance

The Binance Web3 Wallet **removes the need for seed phrase management** via its use of multi-party computation. Binance Web3 Wallet is **secured by three key-shares and a recovery password** chosen by the user. These key-shares are automatically generated when a new wallet is created and stored in three different locations for added security:

Share 1: Secured by Binance

Share 2: Stored on the user's device

Share 3: Encrypted using the user's chosen recovery password and backed up to the user's personal cloud storage (iCloud or Google Drive)

To access the wallet, the **user must have at least two of the three key shares.**

5.2 Accessible on/off-ramps

Widely accessible fiat-to-crypto on and off-ramps are crucial to mass adoption of blockchains. **Retail users need to be able to exchange fiat from their traditional bank accounts for digital assets on-chain.** Per-transaction fees also cannot be prohibitively expensive, as individual retail users generally would be exchanging much lower amounts than institutions.

The world is currently in a transition phase between the traditional finance model of centralized custody, and the blockchain-enabled model of decentralized digital ownership. It is highly likely that for the foreseeable future, most crucial financial operations such as day to day payments, receiving of salary, paying of health insurance etc. will continue to occur on traditional finance rails. As the blockchain environment continues to evolve and build out a purportedly more transparent, decentralized, and secure financial environment, **fiat on/off bridges will be crucial to allow users to make use of both blockchains and traditional finance systems for their various needs.**

Centralized exchanges currently serve as some of the most widely used fiat on/off-ramps access points for retail users. However, this report will focus on two projects that facilitate the direct interaction between fiat and on-chain wallets. The first, Moonpay, allows for the purchase of crypto using fiat, which is then directly deposited into the user's on-chain wallet. The second, Gnosis Pay allows users to spend funds directly from an on-chain wallet using a Visa card.

Moonpay

Moonpay allows users from over 160 countries (including most US states) to purchase and deposit crypto directly into their self-custody wallet using their debit or credit card. **Moonpay has integrated with over 250 crypto wallets, exchanges, and applications** to allow their users to purchase crypto with fiat without needing to navigate to a different site.

Moonpay also supports selling of crypto directly from a self-custody wallet, and will deposit fiat from the sale into a bank account provided by the user.

Figure 11: Comparison of crypto on-ramp fees

Platform	Fees	Supported Cryptocurrencies
Moonpay	4.5% (Card Payments) 1% (Bank Transfers)	100+
Binance	0.65-3.3%	350+
Gemini	1.49%	90+
Ramp Network	1.99-3.9%	50+

Source: Chaindebrief, Binance Research

Moonpay will also charge a **network fee** for each transaction. This fee covers the costs associated with asset transfer, and may vary depending on a number of factors, such as blockchain network congestion and operational costs.

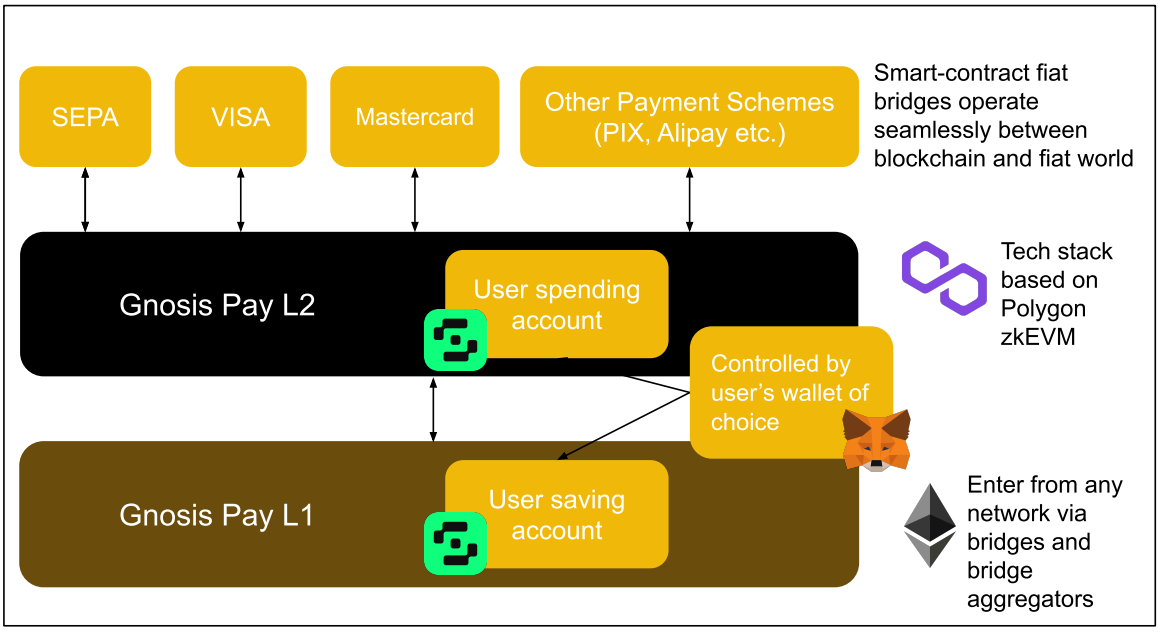
Although Moonpay charges relatively high fees, **the business network they have built has proven valuable for allowing users from a wide range of countries to purchase crypto.** Moonpay serves users from these countries as a valuable alternative bridge between traditional finance and blockchains. In August 2023, Binance U.S partnered with Moonpay to give its U.S customers the option of buying USDT using their debit cards, Apple pay, or Google pay. This allowed Binance U.S customers to continue to bridge fiat over to crypto despite Binance U.S' loss of its support from its U.S banking partners. The loss of banking support occurred during a period of regulatory scrutiny faced by the exchange.

Gnosis Pay

Gnosis Pay, developed by the team behind widely popular Gnosis Safe multi-sig (now known as Safe), **allows users to spend assets held in self-custody directly using a Visa card.** Gnosis Pay is built on top of Gnosis Chain, a zkEVM-based proof-of-stake Layer1 network, operated by a diverse set of over 200,000 validators around the world. The Gnosis Chain underpins the Gnosis ecosystem, which is a collective of aligned projects revolutionizing payments infrastructure to make decentralized financial tools accessible and usable for all. The Gnosis Pay Card is the latest addition to the Gnosis product suite.

Gnosis Pay also provides a set of developer tools that allow crypto wallets to create a version of their Gnosis Card for users without having to jump through all the hoops of building an online payments system. For instance, MetaMask could issue a MetaMask card with relative ease by utilizing Gnosis Pay's APIs and toolings.

Figure 12: Gnosis Pay High-Level Architecture



Source: Gnosis, Binance Research

A solution like Gnosis pay helps to lower the bar in terms of initial set-up cost for projects to enter the decentralized fintech field. This opens the door for more innovation as the lowered barrier to entry allows more new players to enter the on-to-off-chain payments space. **As more players enter, accessibility of on/off-ramps to retail users should increase, and prices should decrease.**

6 Crypto Skeptics

While acceptance of new crypto technology and the industry is growing, some skepticism remains, partly due to past incidents involving certain centralized exchanges and projects that have attracted negative attention. **However, the industry is making significant strides to enhance transparency, security, and reliability** to build trust and confidence among users.

There are two significant ways the crypto industry has begun to utilize to combat some of the skepticism as distrust directed at the industry:

1. Increase Transparency

> **The crypto industry must continue to put in place systems and processes that promote fairness and transparency,** allowing users to verify information independently without relying or trusting a third party.

2. Education

> **Education and knowledge-sharing is crucial** to the global adoption of blockchain technology. As more people begin to understand how the technology works and the benefits of decentralization, more demand and more innovation will spring forth.

6.1 Increase Transparency

The collapse of FTX as well as Terra UST has resulted in significant losses for investors. Customers have reportedly lost access to nearly US$8B in assets as a result of the FTX collapse, and investors in the Terra ecosystem are estimated to have lost almost US$40B.

Past instances of unsustainable business practices, and fraud have contributed to distrust for the crypto industry among blockchain skeptics. Die-hard blockchain enthusiasts might say ‘don’t trust, verify’, but the reality is that most of the general public do not possess the technical know-how to verify the legitimacy of and assess the risks associated with on-chain applications for themselves. To onboard the next billion users to crypto, the industry must continue improving and to put in place the necessary conventions and systems to increase transparency and accessibility for the general public.

Binance Proof-of-Reserves

Proof-of-reserves is a good example of how the crypto industry has increased transparency and created new conventions in the wake of FTX’s collapse. **Proof-of-reserves allow crypto users to verify the amount of assets that centralized exchanges or other crypto**

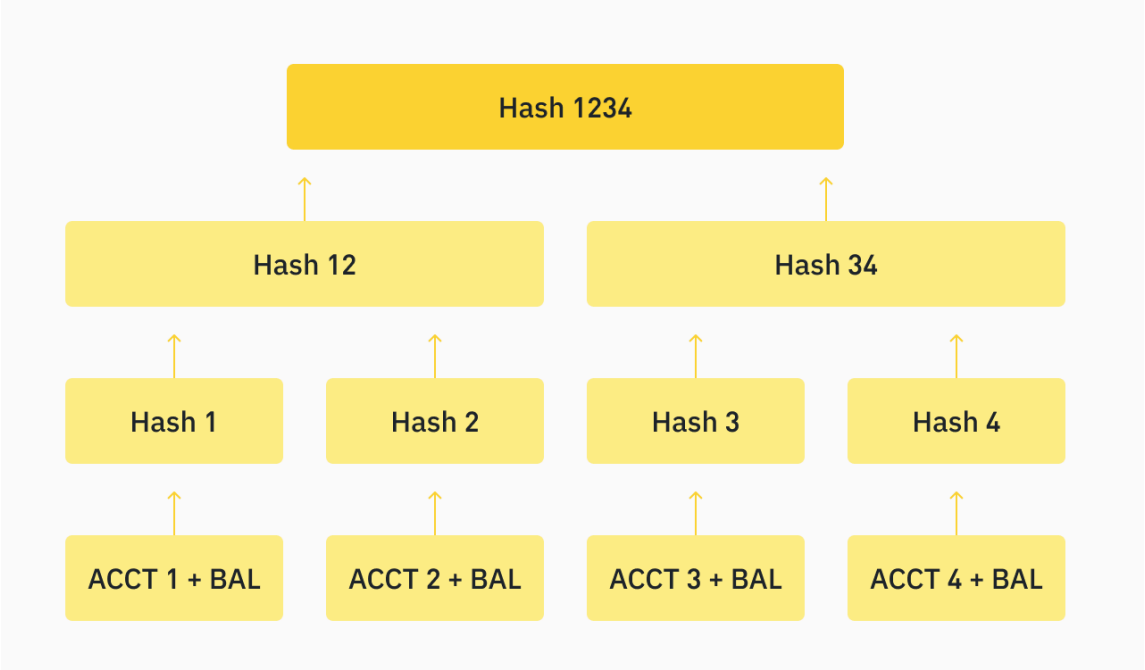
custodians have. Immediately following the crash of FTX, many crypto exchanges committed to the implementation of proof-of-reserves.

The move on the part of centralized exchange to implement proof-of-reserves is a great example of how crypto companies can improve to bring greater transparency and a better overall experience to users. In the long run, **striving to make the industry more transparent to users should go a long way towards building widespread public goodwill towards blockchain technology and blockchain companies.**

Broadly, there are two ways an exchange could implement proof-of-reserves. The first would simply be to have a trusted third party attest that the exchange has custody over sufficient assets to cover client deposits. This method still requires trust to be placed in the legitimacy of the third party attestor, and offers little in the way of additional transparency for the end user.

The second, which Binance utilizes for its proof-of-reserves, would be to make use of Merkle Trees. **A Merkle Tree is a cryptographic tool that enables the consolidation of large amounts of data into a single hash.** This single hash, called a Merkle Root, acts as a cryptographic seal that "summarizes" all the inputted data. Merkle Trees also give users the ability to verify specific contents that were included within a particular set of "sealed" data. Binance uses these properties of Merkle Trees during its Proof of Reserves assessments to verify individual user accounts are included within the liabilities report inspected by the auditor.

Figure 13: Merkle Tree Visualization



Source: Binance Research

Read more about how Binance implements proof-of-reserves, and how you can verify your own transactions and account balances on Binance here.

6.2 Education

Without the invention of the Internet, there would be no blockchains. The Internet of today has grown into a treasure trove of information, readily available to any curious learner with a smartphone and an Internet connection. **Open source and blockchain technology go hand in hand.** This means that much of the technical source code and documentation to be found in the crypto industry is freely available online. As blockchain becomes a globally relevant technology however, **it becomes increasingly important that online educational resources catered to non-technical users are readily available.** As of 2024, there are only 28.7 million software developers globally, less than 0.5% of the global population. For blockchain technology and the concept of digital ownership to truly go mainstream, thought leadership and education catered to the non-technical majority is essential.

Binance Academy

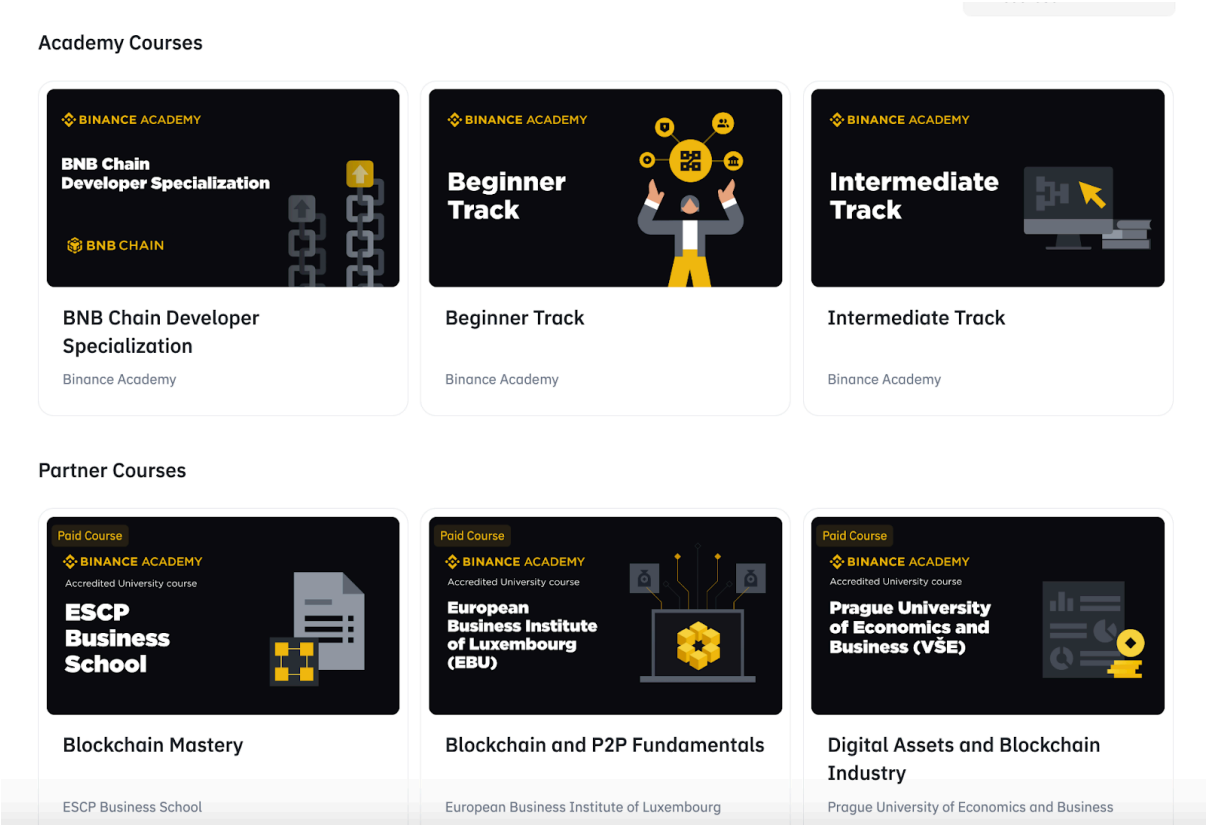
Binance Academy is a leading blockchain and cryptocurrency education platform featuring over 800 articles and glossary entries, plus courses on blockchain, cryptocurrencies, Web3, and more. Launched in 2018, it serves millions of learners across the world in more than 30 languages. Binance Academy's educational initiatives also include Learn and Earn, the University Outreach Program, Student Ambassador Program, as well as partnerships with top online learning platforms, professional associations, and industry alliances.

The free courses are designed by the Binance Academy team and currently include:

- Beginner Track (consisting of 6 fixed courses);
- Intermediate Track (consisting of 6 fixed courses); and
- Specialization Track (consisting of various specialized courses).

While the free courses are comprehensive and cover a wide variety of topics, users can also choose to enroll in paid courses to further develop their crypto knowledge. The paid courses are university courses curated and accredited by leading educational institutions.

Figure 14: Binance Academy Courses



Source: Binance Academy

Binance Research

Binance Research is an initiative launched by Binance in order to enhance online educational resources for the general public. As of today, Binance Research has published over 150 in-depth reports, spanning a wide range of topics across the entire crypto industry from DeFi, to Infrastructure, to Gaming and NFTs.

Each Binance Research article is crafted to be useful and educational for any reader, be they institutional, retail, or crypto skeptic.

7 Closing Thoughts

The Internet revolutionized the world by enabling the borderless digital exchange of information. Initially, the global public was skeptical of the Internet's potential, and much of the early content was undervalued. Today, the Internet is a valuable source of information for people around the globe.

Building on the foundation of borderless exchange of information that is the Internet, **blockchains enable borderless, permissionless, verifiable, digital ownership.** In the recent past, many deemed blockchains as a niche technological development. The types of digital assets stored on distributed ledgers in the past have been labeled as non-serious and merely speculative. Today, Blackrock, the largest asset manager in the world, is tokenizing assets on Ethereum.

In order for blockchain technology to reach mass adoption and usage on a global scale, two things are required. Firstly, there must be on-chain applications that people want to use. Secondly, **people must be able to understand and easily access these applications.** The DeFi summer of 2020 saw a Cambrian explosion of new on-chain applications, many of which found product-market fit, and are still being widely used to this day (eg. Uniswap, Aave, MakerDAO). Now that the fundamental DeFi building blocks have been put in place, **some of the momentum within the blockchain industry seems to have shifted in the direction of making on-chain applications more easily accessible and usable** by the general public.

On its road to one billion on-chain users, **the crypto industry must build the necessary infrastructure, tooling, and public recognition to make the concept of 'digital ownership' understandable and easily accessible** to global human society.

References

1. https://triple-a.io/cryptocurrency-ownership-data/
2. https://www.statista.com/statistics/1380075/global-digital-device-ownership/
3. https://www.axelar.network/blog/jp-morgan-bridge-apollo-cross-chain-portfolio-management
4. https://cryptoslate.com/deutsche-bank-selects-axelar-developer-as-partner-in-joining-project-guardian-singapore/
5. https://www.binance.com/en/web3wallet
6. https://www.binance.com/en/research/analysis/wallets-deep-dive
7. https://www.fireblocks.com/what-is-mpc/
8. https://www.fireblocks.com/blog/7-reasons-why-mpc-is-the-next-generation-of-private-key-security/
9. https://ncw-developers.fireblocks.com/docs/main-capabilities
10. https://app.rwa.xyz/treasuries
11. https://www.binance.com/en/research/analysis/institutional-custody-in-crypto
12. https://www.mas.gov.sg/schemes-and-initiatives/project-guardian
13. https://www.axelar.network/institutional-interoperability
14. https://chaindebrief.com/the-cheapest-way-to-on-ramp-funds-on-exchanges-in-2023

New Binance Research Reports

Navigating Crypto: Industry Map

An overview of different verticals in crypto

Monthly Market Insights - June 2024

A summary of the most important market developments, interesting charts and upcoming events

The Future of Bitcoin #3: Scaling Bitcoin

A detailed and technical breakdown of a selection of Bitcoin scalability solutions

Breakthrough DeFi Markets

An in-depth analysis of the emerging trends transforming DeFi

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.

Joshua Wong

Macro Researcher

Joshua is currently working for Binance as a Macro Researcher. He has been involved in the cryptocurrency space since 2019. Prior to joining Binance, he worked as a product manager at a Web3 fintech startup, and a market analyst at a DeFi startup. He holds a Bachelor of Laws (LLB) from Durham University.

Resources

Read more here

Share your feedback here