Trading Places:

The Rise of DEXs and The Way Forward for Centralized Crypto Exchanges

Hex Trust Insights

April 2023

The Evolution of Exchanges

Exchanges have been a fundamental part of finance for centuries. They are the backbone of every economic system, serving as marketplaces that enable the trading of securities, commodities, derivatives, and other financial instruments (source). With the primary aim of ensuring fair and orderly trading, exchanges play a vital role in centralizing the communication of bid and offer prices to all direct market participants for a given asset being traded.

There are several reasons as to why exchanges are pivotal in any economic infrastructure. Such marketplaces provide companies, governments, and other institutions with a platform to sell securities to the public. This means new companies that need to grow and expand, can raise capital via the exchange through selling stocks.

As the financial intermediary between buyers and sellers of financial assets, exchanges vet market participants and set the institutional rules that govern trading, and the information flows of trading. For example, exchanges enforce listing requirements for companies or groups that wish to offer securities on the marketplace including regular financial reports, audited earning reports and minimum capital requirements.

FROM BONDS TO BYTES

Belgium boasted a stock exchange as far back as 1531 in Antwerp, dealing exclusively in promissory notes and bonds. Founded in 1602, the Amsterdam Stock Exchange is considered to be the oldest, still-in-operation stock exchange in the world, acting as the marketplace for various East India trading companies that issued stock to investors. With the launch of the London Stock Exchange (LSE) in 1773, there was a wave of other jurisdictions following the same path and forming their own stock exchanges such as the Philadelphia Stock Exchange, New York Stock Exchange (NYSE), Chicago Mercantile Exchange (CME), Tokyo Stock Exchange (TSE) and a number of European counterparts.

	Traditional Exchanges	Crypto Exchanges
Regulation	Regulated through licenses; focus on providing trading liquidity to investors in stocks/bonds of particular region	**Off-shore** - offer liquidity to global crypto assets to global audience **On-shore** - compliance with country-level regulations **DEXs** - not regulated
Broker-dealers	Deal with brokers; brokers manage margin accounts for users	No broker-dealers; investors directly access exchanges; exchanges offer margin trading directly & control credit risk
Custody	The Exchange's Assets are held by third party custodians	The Exchange holds custody of Assets internally or via a third-party custodian
Settlement	Broker involved, so clearing house settles inter-broker balances	No brokers & clearing houses; settlement done directly by exchange

Then came the Nasdaq, a revolutionary exchange that forever changed the game. The emergence of Nasdaq was the pivotal moment that shifted the paradigm of exchanges from physical places to virtual platforms. The exchange's electronic trading solutions made financial transactions more efficient and reduced bid-ask spreads - a spread that other exchanges were not profiting from (source).

Since then, all major stock exchanges have transitioned to electronic trading systems - upgrading individual parts of the engine without having to rethink its design. This allowed more trades to be matched per millisecond, but the number of financial intermediaries involved in the trading process remains high; you still need brokers that provide access, clearinghouse to settle trades days after, and banks to transfer funds between players for a fee.

Crypto exchanges arguably mark the next step in this evolutionary journey.

Crypto exchanges serve the primary function of enabling the trading of digital assets between different parties. They have similar functions to traditional exchanges in that A) they act as financial intermediaries between buyers and sellers, B) they centralize communication of bid and offer prices to all market participants, and C) they provide tokenized projects the opportunity to sell their tokens, and for companies, institutions, or individuals to purchase those tokens.

However, they are also different in many ways. Alongside facilitating trades, crypto exchanges often provide additional services such as custody, settlement, and borrowing and lending. By consolidating all financial intermediaries onto one single stack, crypto exchanges have not only upgraded individual parts of the engine, but have also redesigned the way it works. Traders can access the global crypto marketplace directly, trades are settled instantaneously, and funds are transferred using blockchain networks – without relying on other financial intermediaries.

For crypto exchanges, with great responsibilities comes great risks. Before delving into this, we must first clarify the different types of exchanges on the centralized-decentralized spectrum, as they each present different advantages and risks.

Crypto Exchanges

WHAT ARE CENTRALIZED EXCHANGES?

Centralized exchanges (CEXs) are exchanges owned by private entities that also run the operations of the centralized exchange system. Prominent examples include Binance, Coinbase, Huobi and OKX. CEXs can be thought of as entities that run a master wallet on the blockchain, and host sub-wallets for different users on a private, centralized database. Aside from acting as an exchange, CEXs also frequently offer broker-dealer services, as well as risk and derivative products.

Within CEXs, there are two types of business models: offshore and onshore.

- **Offshore exchanges** are ones located in tax or compliance favorable jurisdictions to serve a more global user base. This is why prominent global exchanges are often headquartered in regions such as the Cayman Islands or the Bahamas. Examples of offshore exchanges include Binance, Huobi, and OKX, all of which are headquartered in either Cayman Islands or Seychelles.
- **Onshore exchanges** are country-specific exchanges that have licenses to operate in a respective jurisdiction, most often the jurisdiction it is headquartered in. Examples of onshore exchanges include Binance US, Kraken, Gemini and Coinbase, all of which are headquartered in the United States.

WHAT ARE DECENTRALIZED EXCHANGES?

On the other hand, Decentralized Exchanges (DEXs) are code-based, decentralized finance applications built on the blockchain. In place of a centralized entity overseeing price information and trade execution, DEXs use code to provide traders with liquidity, and to determine pricing and execution models.

Some DEXs use the **Automated Market Maker (AMM) model** which prices and executes trades with a two-token liquidity pool instead of centrally managed order books. Trades are conducted as a swap between the asset being sold and the assets in a given liquidity pool. Trading prices are then based on the depth of the liquidity pool, demand and supply for a token pair, and the size of the order. By allowing trades to be priced based on swaps, asset values can maintain balance even after the trades are done. Prominent examples of DEXs that adopt the AMM model include Uniswap and SushiSwap.

As its name suggests, the **hybrid order-book model** combines the centralized with the decentralized. A centralized entity collates limit orders meaning the order book is centralized, but trade settlements are done on-chain meaning settlements are decentralized. An example of a DEX using the hybrid order-book model is dYdX, one of the largest DEXs to date in terms of trading volume.

An Index of DEXs

MAKER

Founded in 2017, MakerDAO enables users to borrow DAI stablecoin against ETH. It was the first DeFi project which allowed people to borrow digital assets without using a centralized entity.

EtherDelta

Founded in 2017, EtherDelta was one of the first decentralized exchanges enabling users to trade ETH and Ethereum-based tokens with other users. EtherDelta was built to be a peer-to-peer exchange and didn't hold users' funds or use a centralized administrator - users could deposit, withdraw, and trade all via smart contract.

dYdX

Founded in 2017, dYdX is a decentralized exchange focusing on perpetual, margin and spot trading. The exchange enables traders with off-chain order books with on-chain settlement, using StarkWare's Layer 2 to facilitate usability with fast transactions and low fees.

SYNTHETIX

Founded in 2017, Synthetic is a decentralized protocol which issues synthetic assets on the Ethereum blockchain such as gold, silver, stocks, cryptocurrencies and fiat. The protocol uses oracles to track the prices of the assets represented, enabling users to hold the value of the asset without having to hold the underlying asset itself.

Compound

Founded in 2018, the platform built on Ethereum enabled users to borrow against depositing collateral and lend assets to earn yield. The platform was built to be permissionless, meaning anyone could be a borrower or lender. The amount you could borrow only depends on the amount of collateral that you deposit, and doesn't take into account credit scores or KYC, unlike traditional borrowing and lending centralized platforms which were available at the time. If the value of one's collateral fell below a certain threshold, the collateral would be liquidated.

UNISWAP

Uniswap was founded in 2018, based on an idea from Ethereum founder Vitalik Buterin. Uniswap is a decentralized exchange which uses an automated market making system rather than a traditional order-book. Instead of market-makers who provide liquidity on a centralized exchange, on Uniswap, anyone can provide liquidity by depositing assets into a pool and earning fees from the trading activity.

SushiSwap

Founded in 2020, SushiSwap started as a fork of Uniswap. The main difference was that SushiSwap offered a governance token (SUSHI), which Uniswap didn't offer at the time. By incentivizing users to earn SUSHI, the protocol gained significant traction and rose in popularity.

GMX

Launched in 2021, GMX is a decentralized and permissionless spot and perpetual exchange which first launched on Arbitrum in September 2021, and then on Avalanche in early 2023. The exchange facilitates trading via a multi-asset pool called GLP. Anyone can be a supplier to this pool and earn fees in return.

The Journey of Crypto Exchanges

2009
Birth of Bitcoin

2010
Birth of first BTC exchange - bitcoinmarket.com & Mt. Gox (the largest BTC exchange at the time)

2011
Mt. Gox hack (large amount of BTC stolen from user accounts and dumped for sale on the exchange)

2011-2012
Influx of alternative exchanges like Coinbase, Kraken, Bitfinex, Huobi, Poloniex & Bitstamp (with the wave of new alt coins)

2012
Tradehill (one of the largest US exchanges at the time) shut down

2014
Birth of the first decentralized exchange: NXT Asset Exchange

2014
Mt. Gox filed for bankruptcy (customers faced trouble with withdrawals, later disclosed that the exchange faced multiple hacks and lost $460M USD in assets)

2017
Birth of new CEXs Binance, OKX, Huobi and DEXs MakerDAO, EtherDelta, dYdX, Synthetic

2017
Altcoin/ICO boom, rise of Ethereum

2018
Birth of Uniswap, Compound & perpetual futures trading via BitMEX

2019
Birth of FTX

2020
DeFi Summer, birth of SushiSwap & GMX

2022
Collapse of Terra, 3AC, Voyager Digital, Celsius, FTX

THE CENTRALIZED VS THE DECENTRALIZED

	CEX	DEX
Governance	A centralized entity regulates, manages & authorizes the platform	Smart contracts govern the platform; connects users & liquidity providers
Verification	User verification required for AML/KYC compliance	No user verification required; traders can remain anonymous
Custody	Custodial; exchanges in control of assets	Non-custodial; investor retains full control of assets
Risk	Counterparty risk; cyber attacks, data manipulation, hacking are possibilities	Considered more secure; relies on smart contracts & validators cross verify each trade
Cost	Higher transaction fees	Lower transaction fees*
Audience	Caters to crypto beginners; easy user interface	Caters to crypto-natives; complex & not as user friendly

*DEXs have lower transaction fees, but overall fees may be higher depending on gas fees of a respective blockchain network.

Advantages of CEXs

- ✓Fiat onramps, enabling users to deposit fiat via mainstream payment options including wire transfers and credit cards.
- ✓Better user experience: simple, easy to use. No knowledge of wallets, seed phrases, or smart contracts needed.
- ✓No gas costs.
- ✓Quicker as there is no need to wait for blockchain transactions to confirm.
- ✓Better liquidity since larger trading volume on CEX means there is deeper liquidity and less slippage.
- ✓Customer support teams, available to help with any account related issues.

Advantages of DEXs

- ✓Larger number of tokens available. CEXs only list high volume and larger tokens.
- ✓Permissionless: anyone can access, regardless of location.
- ✓Transparent: everything is recorded on the blockchain.
- ✓Self-custodied assets, which means users do not send funds to a centralized entity's wallet.
- ✓No KYC needed, ensuring privacy.
- ✓No single point of failure, unlike a centralized entity.

What Happened In 2022?

THE 2022 MARKET CRASH

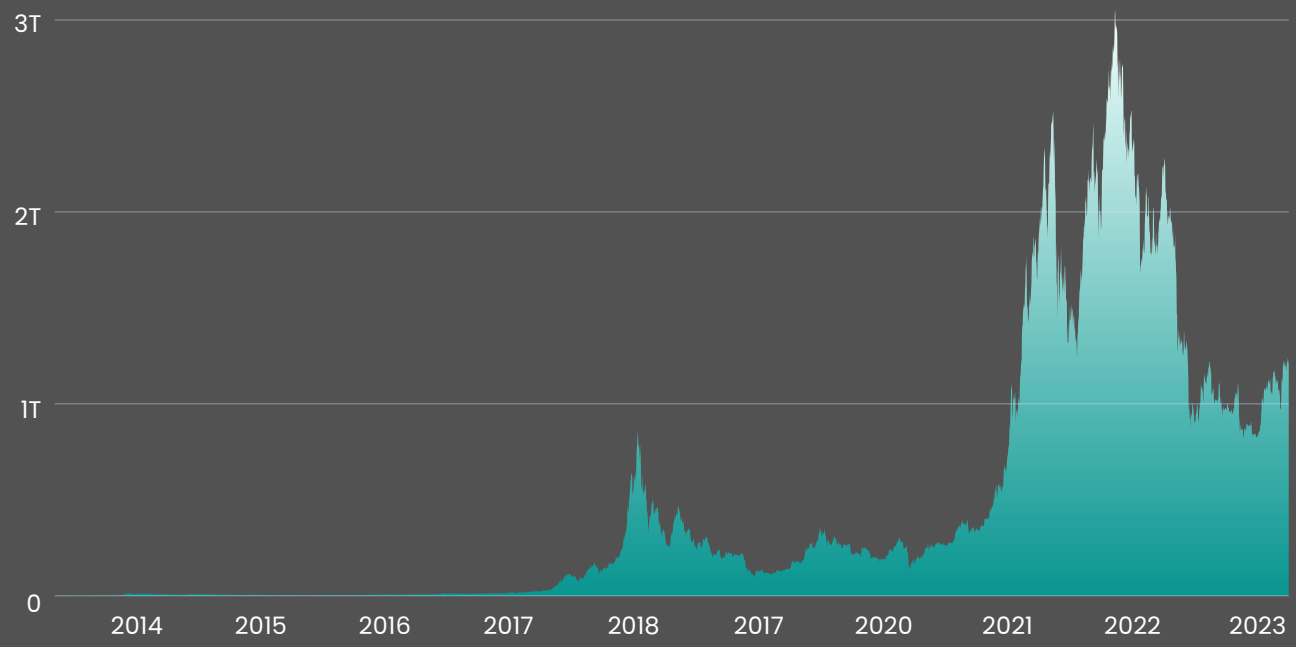
2022 was an extremely volatile year for the crypto industry - including for exchanges, which are a core infrastructure piece for the entire space. There are several events that occurred to contribute to the fame of 2022 as the year of Crypto Collapses.

Late 2021 to the start of 2022, crypto was at its peak, with an all-time-high market cap of over $3 trillion (source). Bitcoin, usually a good indicator of the broader crypto market, had also hit its all-time-high of $65,000. The year was starting off on a good note.

Then came increasing pressure from macroeconomic conditions, and the Federal Reserve began increasing interest rates to fight inflation. Many at this time believed the crypto market wouldn't be affected by inflation. Much to everyone's surprise, the crypto market also began going on a downward trajectory alongside broader macroeconomic conditions, and token prices began steadily dropping by the day.

In March 2022, the Ronin bridge hack occurred, which drained a total of $625 million worth of crypto (source). Two months later, the industry witnessed the downfall of the second largest blockchain in the crypto space: Terra. Its algorithmic stablecoin UST depegged in May 2022, with investors losing over $60 billion in a matter of days.

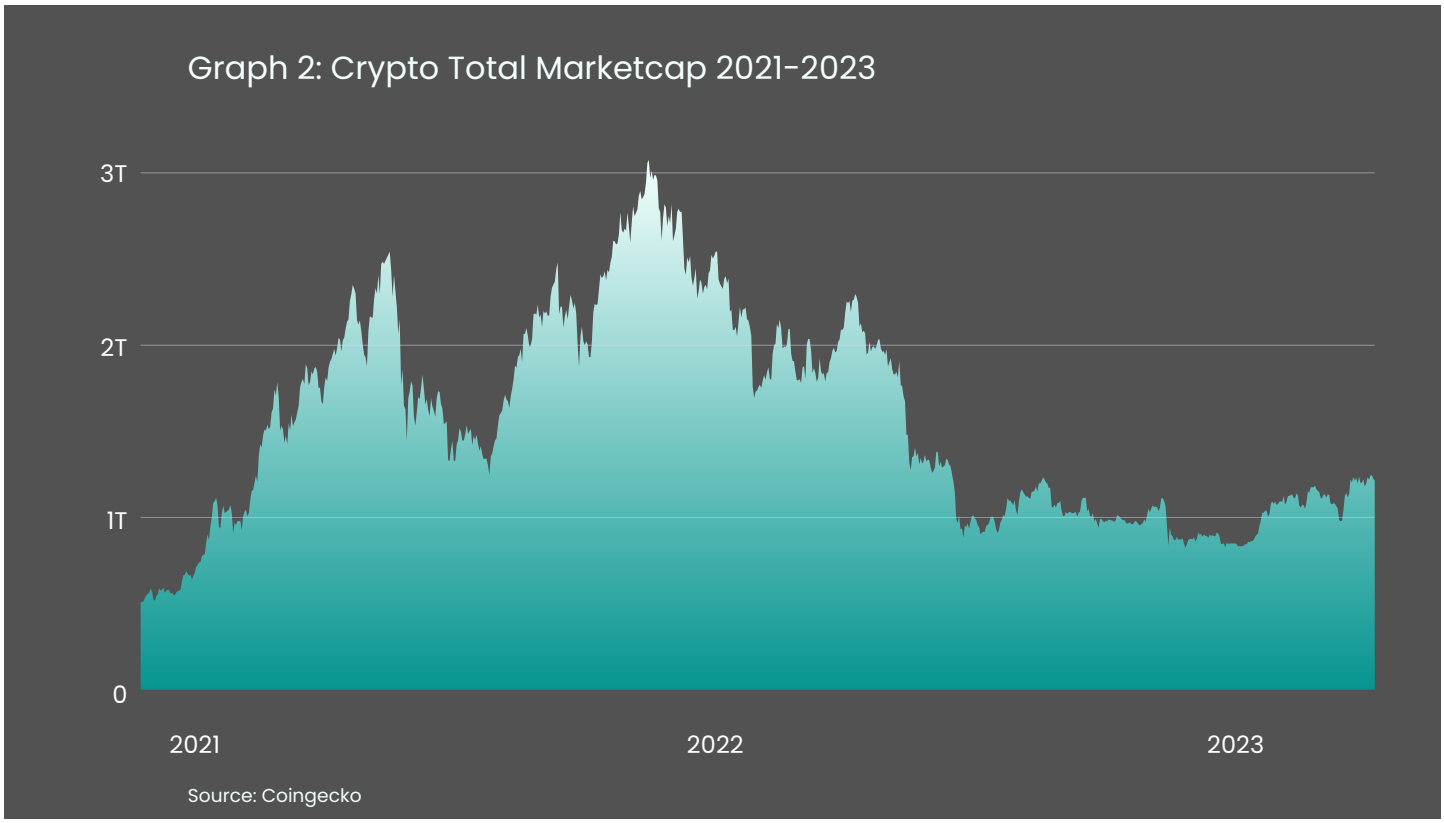
Graph 1: Crypto Total Marketcap 2013-2023



Source: Coingecko

By Q2 2022, the crypto bear market was in full swing.

After Terra, other companies began falling like dominoes. Many firms had invested in, or had a relationship with the company. One example was Three Arrows Capital (3AC), a former crypto hedge fund which collapsed in June 2022 due to excessive leverage on long positions across various cryptocurrencies and derivative products. 3AC had been impacted heavily by Terra's downfall, and the firm was unable to repay their margin loan calls to lenders seeking repayment. The firm then declared itself bankrupt in June 2022, with a deficit of $3.5 billion. Shortly after, Voyager Digital filed for bankruptcy as 3AC defaulted on its $350 million loan, as well as Celsius Network which shut down shop following market downturns and a string of frantic customer withdrawals.



The list of companies that had defaulted on loans and failed to return customer deposits eventually led to the fall of the biggest and most prominent CEX in 2022: FTX. One of the world's largest exchanges clocking in $807 million during a 24-hour period on Sept. 7 at its peak, FTX and its US arm FTX US, officially filed for bankruptcy in November 2022 with a deficit of $9 billion. The once-prominent exchange was forced to close shop as a result of having "misappropriated customers' deposits", diverting these funds to its sister company hedge fund, Alameda Research (source). Aside from the firms' filing for bankruptcy, its infamous CEO Sam Bankman-Fried, was also arrested in the Bahamas on December 12, 2022 for embezzlement and fraud.

The contagion caused by the fall of FTX led to more downfalls of companies in the crypto industry, with crypto firm BlockFi having filed for bankruptcy in November 2022 with a $1.3 billion debt to FTX US and 100,000 creditors. Most recently, the crypto lending subsidiary of DCG Group, Genesis, also filed for Chapter 11 bankruptcy in January 2023 with aggregate liabilities estimated at $1.2 billion to $11 billion (source).





The Crypto Catastrophes of 2022

Crypto's all-time-high market cap of over $3 trillion (BTC all-time-high of 65K)

Q4 2021 - Q1 2022

January 2022

The Federal Reserve starting to raise interest rates to fight inflation, triggering the crypto bear market

Ronin's cross-chain bridge hack for $625M

March 2022

Ronin

May 2022

Terra/Luna crash with UST depegged

Terra

3AC collapse due to high exposure of Terra/Luna (deficit of $3.5B)

June 2022

Babel Finance (HK based crypto lender) collapse with a deficit of $280M

THREE ARROWS CAPITAL

BABEL FINANCE

Voyager Digital files for bankruptcy with a deficit of $1.3B

July 2022

Celsius Network declared bankruptcy with a deficit of $1.2B

VOYAGER

Celsius

FTX and FTX US filed for Chapter 11 bankruptcy with a deficit of $9B

November 2022

BlockFi declared Chapter 11 bankruptcy with a deficit of $1.3B

FTX

BlockFi

Genesis Global filed for Chapter 11 bankruptcy

January 2023

Genesis

Where are CEXs today?

USER CONFIDENCE & TRUST LOST

2022 witnessed the fall of several centralized platforms in the crypto industry, and for one principal reason: lack of risk management and transparency. The fallen companies were unregulated, and failed to have the appropriate internal controls and procedures in place to serve their customers. Asset segregation was absent, and entities that were once trusted had failed to deliver on that trust.

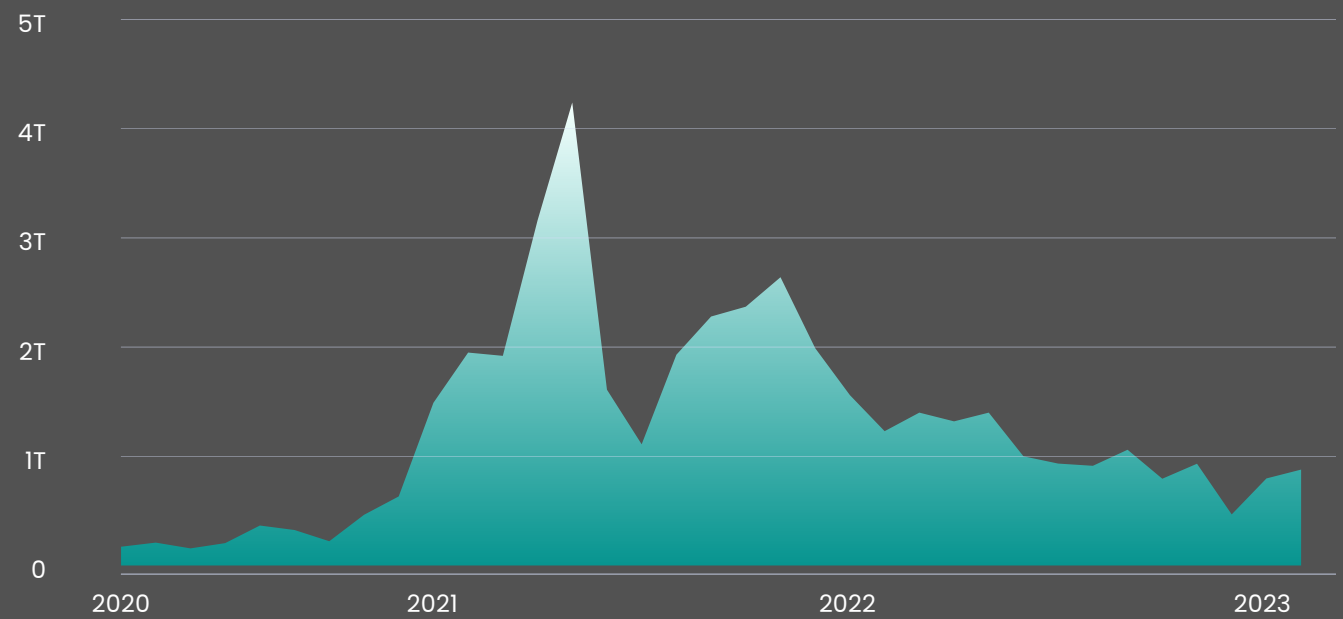
Out of all incidents however, the implosion of the FTX scandal was by far the most monumental moment of the year, if not in crypto history. It impacted both institutional investors and millions of retail investors. Just prior to its downfall, FTX was ranked by Coinmarketcap and Coingecko as the 3rd largest crypto exchange in the world in terms of trading volume, and hosted over 1 million users (source).

An exchange of such credibility at the time had collapsed in a matter of days, which inevitably had consequences for the entire crypto industry. User confidence was lost, regulatory scrutiny drastically increased, and affiliated crypto companies experienced a tarnished reputation. The turn of events was purely due to the fault of centralized entities that were unregulated, and had nothing to do with blockchain technology in any way.

The year's outcomes unveiled some fundamental issues that remain in the crypto industry, largely due to the lack of regulatory frameworks guiding businesses' internal controls and processes. Unlike the traditional finance world, the crypto industry still lacks guiding principles and laws that forbid, for example, the commingling of clients' assets. This puts all investors at risk of having their funds used for purposes aside from the designated purpose of their investments – and most importantly, without their knowledge.

It is no surprise that users' trust and confidence in the crypto industry has been lost following the likes of FTX and others. These firms were unable to return customer deposits as a result of malpractices, resulting in many investors pulling their funds off centralized platforms. In particular, investors have been increasingly skeptical of having their funds held in exchange-hosted wallets such as FTX, a centralized exchange which offered a hot wallet solution for clients and held their private keys on their behalf.

Graph 3: Crypto Monthly Exchange Volume



Source: The Block

SELF-CUSTODY BECOMES PRIORITY

Graph 4: 7-day average of daily movement of funds from centralized exchanges to personal wallets

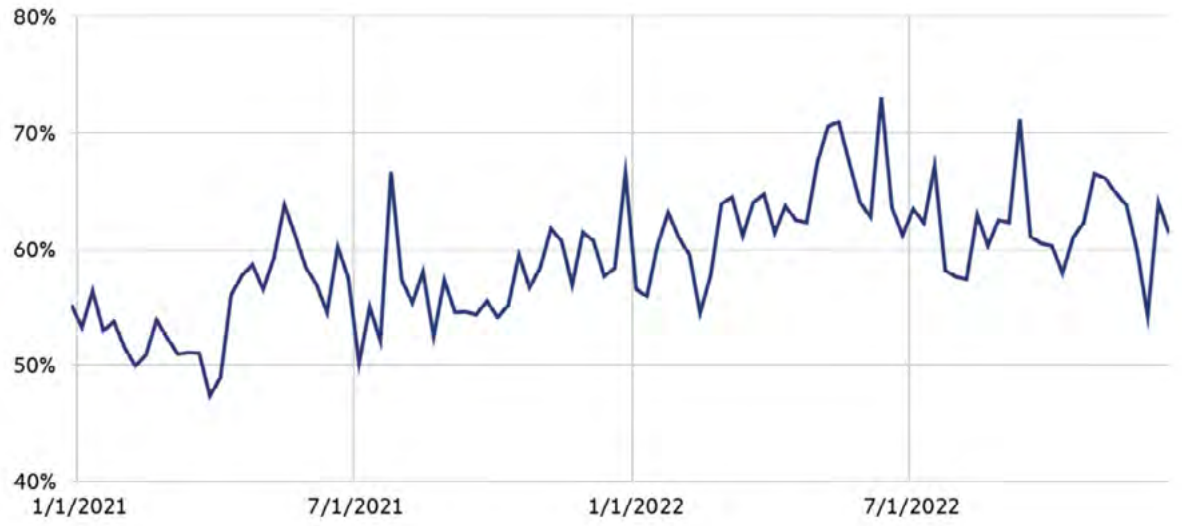


Source: Chainalysis

As investors increasingly lost confidence in their assets' safety, they started looking towards self-custody. This is made very clear from data released by Chainalysis on the seven-day moving average of total value withdrawn from CEXs to personal wallets throughout the year (Graph 4). The first major outflow of around $12 billion occurred right after the UST collapse. The same pattern emerged following the bankruptcy of Celsius Network where around $8 billion was moved, and during the FTX crash, which saw an outflow of around $9 billion worth of funds.

According to Chainalysis, the spikes of fund withdrawals were closely aligned with market volatility, and data patterns insinuate that users were worried about the respective CEX's solvency. This encouraged investors to withdraw their funds from CEXs to personal wallets fully under their control to ensure that they maintain access to their funds (source).

Graph 5: Weekly share of cryptocurrency moving from CEXes to personal wallet in institutional transfers (>100K)



Source: Chainalysis

Additionally, the data also showed the institutional composition of the volatility-driven withdrawals to personal wallets, particularly the percentage of institutional CEX-to-personal wallet transfers. 77%, 69% and 68% of CEX-to-personal wallet transfers were attributed to institutional transfers following the collapse of Terra, Celsius Network and FTX respectively (Graph 5). This indicates that following every collapse, institutions were reminded of the risks of holding funds on exchange wallets where they do not hold control of their private keys and assets.

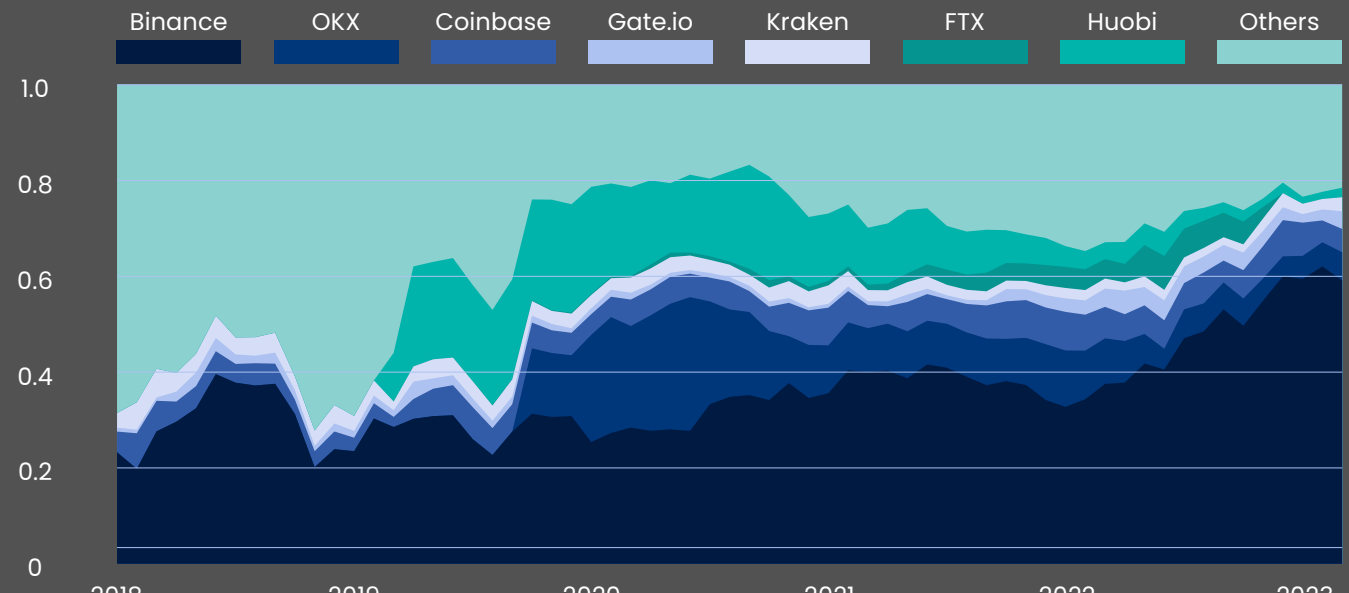
It's important to note however, that institutions should not be safekeeping these funds on personal wallets either. Institutional investors must select trustworthy and credible third-party custodians to hold their assets on their behalf, where they maintain control over their private keys while leveraging enterprise-grade security frameworks. This is the only way to ensure that institutional funds are fully protected from internal and external threats such as theft, loss or misuse.

As an inevitable consequence of multiple centralized entities having mismanaged clients' funds, investors across the crypto space have responded by demanding increased transparency from CEXs. One such way that transparency has been demanded is through a Proof of Reserve (PoR) system, which will be elaborated in detail at a later section. This allows all users to see and verify a CEX's solvency by evaluating their total assets as well as liabilities. PoR is just one of the many things that CEXs have undertaken to increase transparency and restore confidence, reassuring that client funds are safe from misuse or management.

CEX INDUSTRY LEADERS HOLD UP DURING FTX DOWNFALL

Several CEXs have benefited from the FTX collapse, as a result of having responded appropriately to the public's demands for increased transparency. Binance is one such CEX that has increased its market share post-FTX, as indicated by monthly exchange volume market share data (Graph 6). In October 2022, Binance held ~50% volume market share as compared to ~62% in February 2023, representing a 25% increase before and after the fall of its competitor FTX. The same pattern was observed for Kraken, which saw a 24% increase in exchange volume market share post-FTX. According to Kaiko, many US-regulated CEXs like Coinbase and Bitstamp also saw drastic increases in market share in December 2022 shortly after the FTX scandal (source).

Graph 6: Monthly Exchange Volume Market Share



Source: The Block

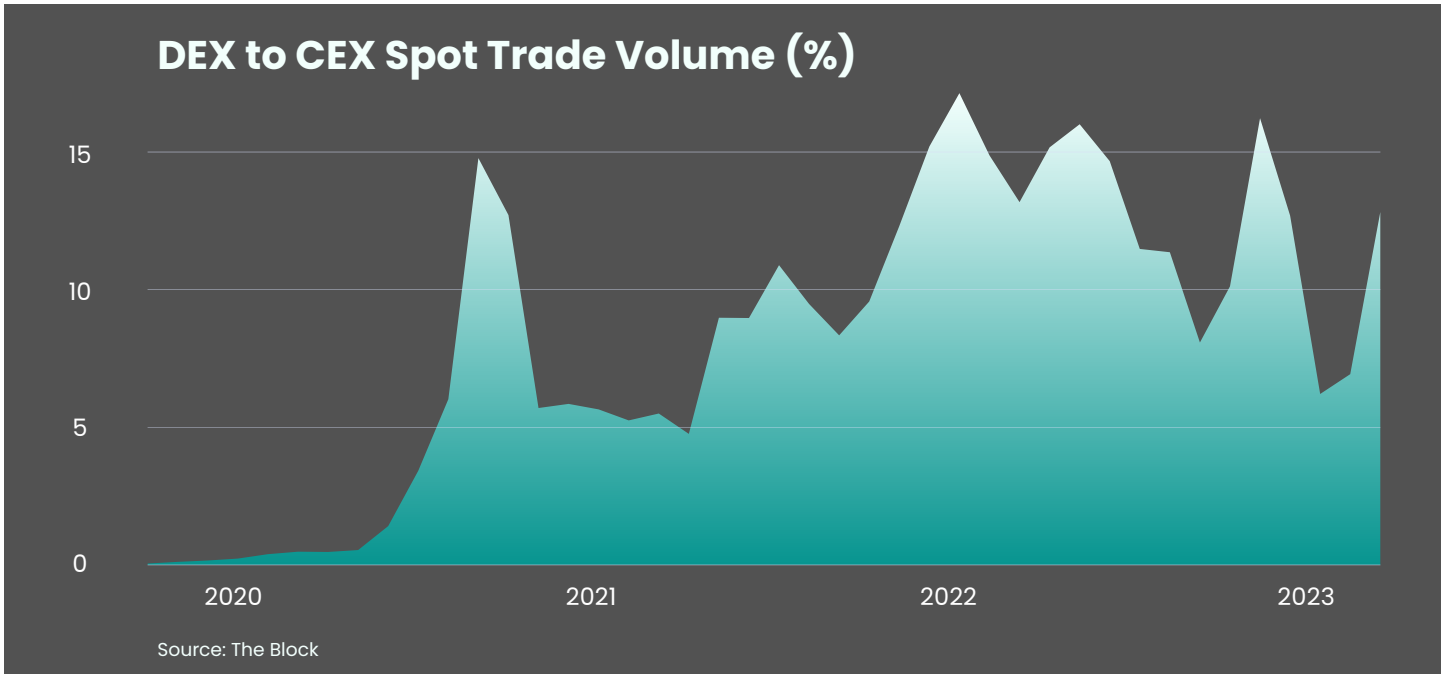
There are several reasons as to why Binance was able to increase its market share following the FTX crisis, despite the fairly diluted CEX market today. First off, it proved its solvency and stability via its PoR system which shows >$55 billion in verifiable cold wallet addresses (source). Additionally, the CEX also holds a long history of putting customers first – it has made customers whole following different hacks, and has overcome regulatory challenges (e.g. pulling out of the Chinese market) with appropriate timelines.

However, Binance is an off-shore exchange which serves a global customer base, and it is likely that regulatory scrutiny towards the CEX will continue. As more regulatory frameworks emerge for CEXs, Binance will have to keep upholding the most robust compliance, security and risk standards to continue holding its market share.

Onshore exchanges that undergo regular regulatory examination such as Kraken and Coinbase have also seen positive developments post-FTX, and are expected to be well-positioned to continue capturing market share (source).

DEFI AND DEXES AS A SAFE HAVEN - WILL DEXS FLIP MARKET DOMINANCE?

On the other side of the story, DEXs have also seen positive performance. Since the DeFi boom in 2021, there has been a steady increase of DEX vs. CEX trading volume on average (Graph 6). Worth noting here is the spike in DEX trading volume during the period of the FTX collapse in November 2022, and its steady rise up till March 2023.



As compared to its centralized counterparts, DEXs only provide self-custody wallets, which, as previously mentioned, seems to have been deemed safer and more reliable for retail investors. Post-FTX, DEXs have seen a jump in volumes and revenues, with Uniswap, the largest DEX platform, having seen a daily revenue of $6.32 million on 3 November (source). The general increase of DEX vs. CEX spot trading volume indicates that investors across digital assets are increasingly shifting towards on-chain transparent decentralized exchanges as opposed to off-chain centralized exchanges.

Additionally, the recent downfall of several traditional banking institutions such as Silicon Valley Bank, Credit Suisse and Silvergate seems to have further pushed investors of all stripes towards decentralized finance. Decentralized exchanges saw a record high of $250 billion in daily trading volume on 11 March, shortly after the depeg of the 2nd largest stablecoin USDC (source). The banking crisis was yet another testament to the fragility of the existing financial system, and that counterparty risk should be thoroughly vetted even for institutions that have been trusted for many decades.

Decentralized finance was built as an alternative to the existing financial system, and is proving to be a safe haven for many investors during times of uncertainty. It is likely that DeFi adoption will continue to strengthen as centralized entities in and outside the crypto space remain opaque, and fail to safeguard customer trust.

With DEXs being a key pillar of DeFi, it will play a big role in broader DeFi adoption. If current trends continue holding up, it is likely this adoption will happen very soon, at a rapid pace. However, it remains uncertain whether DEXs will be able to flip market dominance, as many improvements are still needed.

First, improved connectivity to fiat onramps need to be addressed. An example of this effort is Uniswap's web app connectivity to credit cards, debit cards, and bank transfers. Additionally, transfer fees must reduce over time, which can be expected to be naturally addressed with Ethereum's upgrade lowering gas costs, Layer 2 technologies increasingly emerging, and more fast/cheap Layer 1s like Solana, Avalanche, Cosmos and Fantom growing in prominence.

The Way Forward For CEXs

For CEXs to maintain market dominance, they must now prioritize increasing customer confidence which plummeted after the 2022 market crash. Initiatives like CEXs publishing their assets on-chain have helped, but it is only part of the puzzle as they must work towards publishing liabilities to give the full picture of their solvency. Additionally, CEXs must collaborate with fully licensed, independent custodians to safekeep customer assets as a big step in regaining trust.

THE DEMAND FOR TRANSPARENCY

As previously mentioned, CEXs have begun to take steps towards increasing transparency by providing PoR. This is an audit method that shows a CEX indeed holds 1:1 reserves for all customer deposits on their platforms through publicly available on-chain wallet holdings.

The verification method for PoR so far has been Merkle trees, which are data structures designed to encrypt data securely and verify user deposits on exchanges. Many CEXs have published Merkle trees on their websites which allow users to verify ownership of their on-chain wallet assets relative to the CEX's total wallet holdings. For full degree of transparency, users must also be able to verify the exchange's reserve ratio (total user asset holdings vs. total exchange assets).

To go through the verification procedure, users can simply visit the respective CEX site hosting its Merkle tree. Each user with assets on a CEX are given a unique anonymous user hash ID (Merkle leaf) which represents the respective user's total balance. Each user's Merkle leaf is combined to produce a Merkle root, a cryptographic signature representing the total sum of all users' assets. Any changes to an individual user's assets will be reflected in the Merkle root, which eliminates the possibility of data tampering or manipulation.

The use of Merkle trees shows that exchanges are starting to leverage blockchain technology to regain user trust and confidence. Since the introduction of Merkle trees, the concept of PoR has further developed into Proof of Solvency to encompass assets as well as liabilities. This was a result of voiced concerns around the limitations of PoR, and how it fails to take into account an exchange's liabilities which not only includes client assets, but also the exchange's credit lines and other financial obligations. Many exchanges now have their Proof of Solvency available for public viewing on blockchain analytics platforms such as Nansen and Dune Analytics.

It seems there may be further developments to strengthen Proof of Solvency systems, as suggested by Ethereum co-founder Vitalik Buterin in his latest proposal to improve the current Merkle tree method in verifying an exchange's solvency (source). Buterin mentions that although the Merkle tree technique is a good way to verify proof of liabilities, it may not be the safest option when it comes to protecting privacy.

As a result, Buterin proposes the use of Zero Knowledge Proofs, particularly ZK-SNARKs, to prove reserves and liabilities while protecting user data. He also further predicted that in the future, there may be cryptographically constrained CEXs and half-custodial exchanges that hold fiat, but not crypto. The path forward for CEXs doesn't seem to be solidified just yet, but it is clear that many more steps are being planned to achieve the industry's objective of restoring user trust.

CEXS ARE STARTING TO MAKE MOVES

As mentioned, CEXs have collaborated with blockchain analytics platforms like Nansen and Dune Analytics to host their Proof of Solvency, alongside publishing Merkle trees on their respective domains. Users today can access publicly available Proof of Reserves for most prominent exchanges including Binance, Kucoin, OKX, Huobi, Crypto.com and others, on both Nansen and Dune Analytics. The data currently includes on-exchange total balances, balance breakdowns, token inflows and outflows, and more. Working with blockchain-based applications like Nansen signals CEXs are aiming to provide full degree of transparency of their centralized databases.

Binance was one of the first CEXs to publish their Proof of Reserves in November 2022 using the Merkle tree method. Shortly after Buterin's proposal, Binance also implemented zk-SNARKs in February 2023 to allow users to verify their holdings and the exchange's holdings in a more private and secure manner.

OKX also published their Proof of Reserves following the FTX collapse using the Merkle tree method. The team has stated future plans to implement zk-SNARKs in 2023 following in the footsteps of Binance. Other off-shore exchanges such as Gate.io, Huobi, Kucoin, Bybit have taken similar approaches and provide a fully verifiable Merkle tree on their domains as well as other blockchain applications.

Heavily regulated CEXs such as Coinbase have taken alternative approaches by making frequent public statements to reassure their community. Coinbase has always had a traditional approach of audited financials in place prior to FTX, and is subject to quarterly external auditor reviews, with regular filings of audited financial statements with the US SEC. In response to FTX, Coinbase now also provides third party audited Proof of Solvency on a quarterly basis.

REGULATORY FRAMEWORKS EMERGING FOR CEXS

One of the key highlights of the FTX crisis has been the increasing regulatory intervention across different jurisdictions to increase investor protection. While regulatory intervention has been scrutinized for its role in inhibiting innovation in the crypto space, the outcomes of the FTX scandal proved that regulatory developments are necessary to ensure investors are protected when interacting with crypto as a yet-nascent asset class.

In particular, the downfall of FTX has made CEXs the primary target of concern for most regulatory bodies. Since FTX's bankruptcy, some actions have been taken against several CEXs regarding their products and services:

- The US Securities and Exchange Commission (SEC) charged Gemini for the unregistered offer and sale of crypto asset securities through the Gemini Earn Lending program (source).
- The US SEC charged Kraken for failing to register the offer and sale of their crypto asset staking-as-a-service program. The charge was settled with a $30 million fine (source).
- Coinbase was forced to release a public statement regarding their staking products, and how they are fundamentally different from Kraken's yield products (source).
- The US SEC denied Binance US's deal to purchase the assets of shutdown lender Voyager Digital (source).
- CoinEX was charged by the New York Attorney General's office to stop serving all US customers due to mismatch of regulatory requirements (source).

Additionally, more regulatory frameworks for CEXs are being developed worldwide:

- The Hong Kong Securities and Futures Commission (SFC) will require exchanges to obtain a Virtual Assets Service Provider (VASP) license for exchanges to offer services to retail traders starting 1 June 2023 (source).
- The US SEC proposed a new framework to require any investment adviser including crypto service providers to use a qualified custodian in order to increase investor protection. This will require all CEXs and crypto service providers to use an independent licensed custodian to hold its assets on its behalf (source).
- The United Kingdom government proposed a new framework to regulate crypto asset activities, more specifically placing responsibility on crypto exchanges to define detailed content requirements for admission and disclosure documents (source).
- The European Union is developing the Markets in Crypto Assets Regulation (MiCA) framework to regulate crypto activities at the EU level. Post-FTX, the framework is being questioned on whether it will encompass all levels of investor protection, and may be up for further evaluation (source).

- Individual jurisdictions such as France, Taiwan, Israel and India are developing new regulatory frameworks or improving existing ones in response to the FTX scandal (source).

WHY CUSTODIANS ARE PARAMOUNT TO RESTRUCTURING FINANCIAL MARKETS

The past year has seen bankruptcies and asset losses both in the crypto world and the traditional finance world. Investors are starting to realize that their assets may not be as safe as they are made to believe, even with institutions that have been trusted for many years. Such outcomes have once again reminded stakeholders to conduct thorough evaluation of counterparty risk, and have pointed to a need for fundamental restructuring of financial markets to better protect investors and customers.

The bankruptcies and asset losses in the crypto world have not been a problem of blockchain technology, which by default provides full transparency and instantly verifiable information. But blockchain technology can only deliver on that value if centralized platforms actually use it properly. One such way that centralized exchanges have done so is by providing PoR or on-chain asset holdings. This was also taken a few steps further, with exchanges now looking at implementing zk-SNARKs to prove liabilities as well as assets.

Custodians have played a key role in safeguarding traditional financial assets for many years in some of the riskiest markets in the world. Their virtual counterparts remain equally relevant in the crypto world, and will only likely accelerate in the wake of the recent FTX turmoil.

A custodian's principal raison d'être is to safeguard clients' assets. A professional custodian provides a highly secure environment and ensures that any movement of assets out of the client's own wallet takes place only on the explicit instructions of the client. The custodian acts solely as an agent for client assets, never as a principal. Client assets do not form part of a custodian's own balance sheet.

A professional custodian provides infrastructure to ensure the safety of client assets, which includes:

- Fully regulated and audited environment
- Full segregation of client assets from its own
- Secure technology using the latest standards against unauthorized access
- Bank-grade controls (no single person can move assets)
- Independent internal governance and checks and balances
- Regular reconciliation of client positions
- Internal and external management of risk and security — continuous review and improvement

Regardless of whether it relates to traditional finance or digital assets, the best practice is for assets to be held by an entity that does not itself indulge in risk-creating activities. This ensures that not only are clients' assets segregated and therefore safe, but it also makes them bankruptcy remote, i.e. minimizing the likelihood of any prolonged lock-up of assets caused by, for example, the bankruptcy of the custodian.

The only way forward for centralized exchanges is to leverage fully licensed, insured custodians that offer enterprise-grade security frameworks with full visibility of on-chain asset holdings in-segregated accounts. As the past year has proven, the new and improved financial system being built around the core tenets of decentralization and verifiable ownership has no place for unlicensed centralized exchanges running black box operations that keep users in the dark. The crypto industry must now consolidate the lessons learnt from past events, and do better in protecting investors moving forward.

HexTrust

Digital Asset Custody
Meets Innovation

