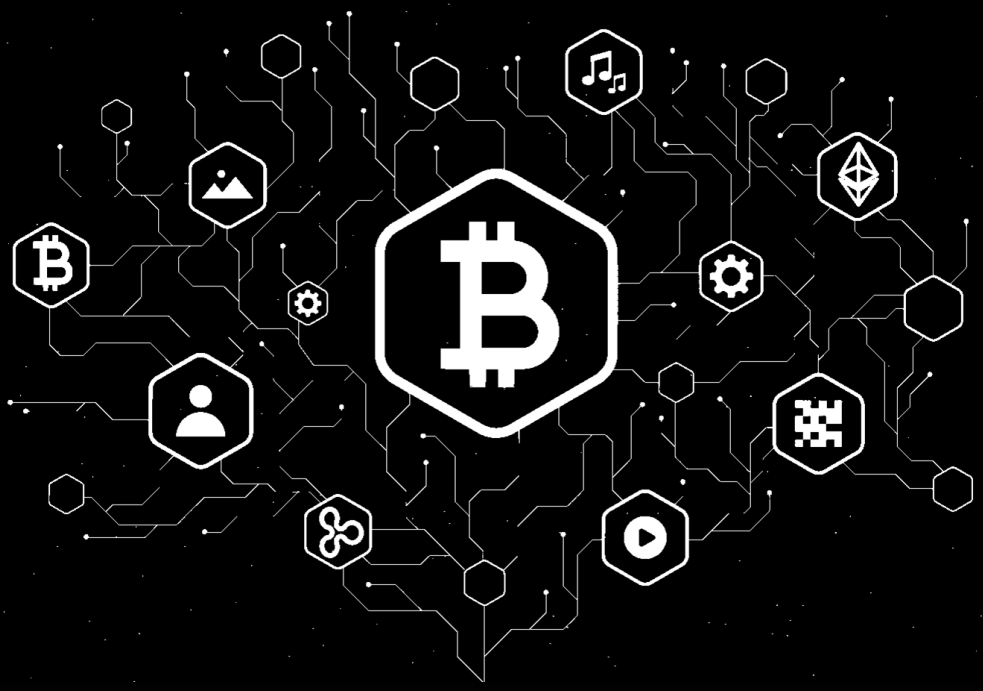
PEAK BLOCKCHAIN



MARKET INTELLIGENCE

The Fall of Genesis, Ethereum Releases ‘Shadow Fork’, What is Proof of Reserve Audit Method+ More

Published by Duke Banerjee

TABLE OF CONTENTS

Research Disclaimer	3
The Fall of Genesis	4
Ethereum Releases ‘Shadow Fork’	7
What is Proof of Reserve Audit Method	9
Venture Capital Deals	12

RESEARCH DISCLAIMER

The information developed in this report is intended to be as reliable as possible at the time of publication and is prepared by a team of professionals. This information does not constitute managerial, legal, or accounting advice, nor should it be considered a corporate policy guide, laboratory manual, or an endorsement of any product, and the nature of the information is not speculative, but based on fundamental research and available market data. Peak Blockchain and the author assume no responsibility for any loss or damage that might result from reliance on the reported information or its use.

The Fall of Genesis

Genesis, a prominent cryptocurrency lender, has declared bankruptcy, dealing a significant blow to the crypto industry. Genesis is being charged by the SEC for illegal cryptocurrency sales. Genesis is part of the DCG conglomerate, which includes over 200 crypto-focused businesses.

Unsurprisingly, the bankruptcy is linked to FTX's collapse last November amid fraud allegations. This is a warning to the cryptocurrency industry, and it emphasizes the importance of proper regulation and oversight to avoid similar situations in the future.

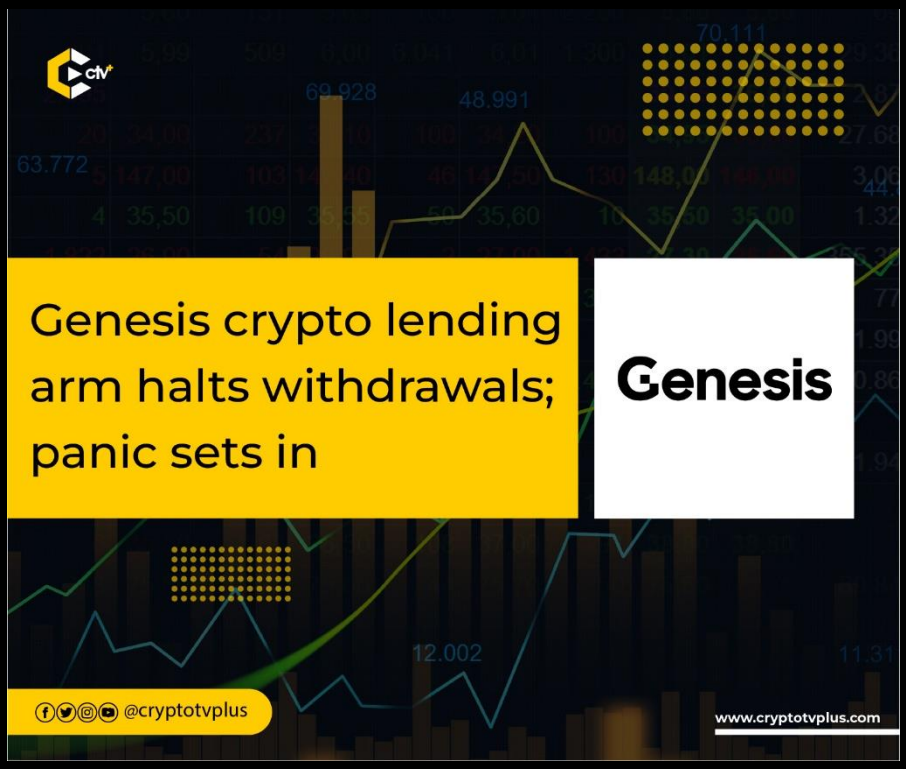
The Bankruptcy of Genesis

Genesis, a cryptocurrency lender, declared bankruptcy after being investigated by the US Securities and Exchange Commission. It was charged with illegally selling cryptocurrency. Genesis' default was linked to the failure of another cryptocurrency firm, FTX. Furthermore, FTX went bankrupt last November amid allegations of fraud. The SEC charges and the bankruptcy of FTX both played a significant role in Genesis' demise.

The Impact of Other Collapses

Genesis' fall is not an isolated incident. Meanwhile, the failure of another cryptocurrency firm, Three Arrows Capital, impacted Genesis. Furthermore, Three Arrows declared bankruptcy in June of last year, and Genesis claimed that Three Arrows owed them $1.2 billion.

In May, Three Arrows was brought down by the collapse of the cryptocurrencies Luna and TerraUSD. This exemplifies how the failure of one company can have a cascading effect on the industry. Some analysts refer to the ongoing downfall of crypto firms as the "crypto winter."



Genesis Ongoing Dispute with Gemini

Genesis is embroiled in a high-profile dispute with Gemini over $900 million in assets. Gemini sold a product called "Gemini Earn" to investors, promising 7.4% interest on cryptocurrency holdings. Since November, when Genesis halted withdrawals due to crypto market volatility, 340,000 Earn users have been unable to access funds. The dispute with Gemini demonstrates how one firm's failure can negatively impact the industry and individual investors.

The Need for Proper Regulation and Oversight

The significance of proper regulation and oversight in preventing similar incidents from occurring again cannot be overstated. The SEC's charges against Genesis for illegal cryptocurrency sales, as well as the ongoing dispute with Gemini, demonstrate how a lack of proper regulations and oversight can have a negative impact not only on the industry but also on individual investors. Furthermore, it reflects the need for increased crypto oversight, enforcement, transparency, and disclosure for crypto firms.

As the crypto industry grows and evolves, we must put proper safeguards in place to ensure market integrity and investor protection. As a result, the crypto industry must take this warning seriously and take action to prevent similar incidents from occurring in the future. We can create a more secure and reliable crypto market by implementing stricter regulations, increased oversight, and industry-wide self-regulation. Furthermore, it will boost trust and confidence in the cryptocurrency industry.

Ethereum Releases ‘Shadow Fork’

Blockchain developers have successfully launched a 'shadow fork' in the Ethereum blockchain for the upcoming Shanghai upgrade. The shadow fork - a test model for the actual mainnet that allows developers to see if the proposed upgrade's code works correctly on a real blockchain - occurred Monday at 5:30 a.m. ET.

The Shanghai upgrade will be the first hardfork on Ethereum since the "Merge" in September last year when the blockchain switched from a "proof-of-work" (PoW) to a "proof-of-stake" (PoS) consensus mechanism.

The Shanghai upgrade is scheduled for March, and one of the proposed changes is to allow for the withdrawal of staked coins, which occurred during the proof of stake transition. In the run-up to the network upgrade, Ethereum developers have also stated that more shadow forks will be released in the coming week.

Amidst the upgrade, technical problems were reported for some of Ethereum’s nodes.

The Next Update, a Testnet, Is Expected Before the End of February

A public testnet is also planned by the developers to take place before the end of February. The staking firms will be brought on board by the test network to test the Shanghai upgrade. The blockchain developers have also stated that additional forks would copy the network's data to the testing environment or the shadow fork before the update.

The Ethereum community has expressed concern about how soon they can access their staked assets. In the past, such forks in Ethereum have been delayed, including the most recent PoS merge. According to on-chain data, the number of staked Ether in the validator contract that has yet to be unstaked is 16,167,572. The counter-argument is that the 16 million Ether represents only 13.2% of the total circulating supply of the cryptocurrency, which is far lower than many other PoS tokens. Furthermore, other Ether staking options have been available to investors for quite some time.

The team behind the Shanghai update introduced the Shandong testnet in November, but it was later replaced with an improved alternative. Before last year’s significant change to the Ethereum network, the Merge, the blockchain underwent several test forks.

What is Proof of Reserve Audit Method

The FTX crash is one of the crypto industry's black swan events. Customers were not the only ones who faced increased losses; the industry's reputation, which was previously known for fraud and scams, was also at stake. However, the FTX's downward spiral necessitated greater transparency in the crypto industry. One of the solutions proposed by centralized exchanges was to implement Proof of Reserves to instill confidence and save them from damage control.

What is Proof of Reserves

Proof of Reserves is a public attestation that an exchange or crypto custodian publishes the actual underlying assets of assets displayed on their exchange. An independent third-party auditor uses the Merkle tree to conduct the proof of reserve audit. According to several stakeholders, the Merkle tree is a cryptographic data structure used for self-verification and PoR audits. As a result, rather than relying on the exchange or the auditor's report, users can independently verify.

Users are advised to make informed decisions about where they store their crypto assets because centralized exchanges have a history of fraudulent activities. The FTX collapse is a textbook example of an exchange openly mismanaging user funds and engaging in fraudulent activities. It is difficult to say whether Proof of Reserves could entirely prevent crypto exchanges' collapse. Nonetheless, it would increase transparency about how the exchange operates and manages user funds. It would instill a sense of accountability in the exchange to conduct their business with integrity.

Limitations of Proof of Reserves

There are also limitations in the PoR(Proof-of-Reserves) model; below are some of the areas we are going to look at :

❑ Dependence on Human Factors

The Reserves Proof A third-party auditor is usually used to conduct audits that are considered valid. The independent auditor will compare the exchange's finances to on-chain assets to determine whether the exchange has the claimed real asset backing. It means that the auditor entirely relies on the data provided by the exchange to conduct the audit. There is a possibility that the exchange intentionally or unintentionally supplied false information, resulting in audit inaccuracy.

❑ Lack of Real-time data

Proof of reserves is accomplished by capturing a snapshot of users' account balances at a predetermined time, and it must demonstrate that it has sufficient funds to cover its liabilities. As a result, the exchange can always borrow assets to manipulate the audit through unethical practices because it does not track real-time data.

❑ Users have no control over their Assets.

The ultimate form of security is self-custody. While Proof of Reserves can provide information about the exchange's finances and current assets, the exchange can always move user assets without its customers' knowledge.

❑ Inadequate Information

Although Proof of Reserves is an excellent way to understand the exchange's financial situation, more is needed to confirm the exchange's solvency. There is always the possibility that the exchange has other liabilities and financial obligations that could lead to insolvency.

Despite its limitations, Proof of Reserves establishes a high level of transparency for exchanges. It can help to reduce the likelihood of fund mismanagement and fraud if done on a regular basis.

Venture Capital Deals

Project	About	Funding Amount	Funded By
Candy Digital	Sports-focused non-fungible token (NFT) company	**$38 million**	Galaxy Digital, ConsenSys Mesh
PLAI Labs	company that builds social platforms for Web3	**$32 Million**	a16z
Nil Foundation	Nil is the developer of the Proof Market protocol, which enables Layer 1 and Layer 2 blockchains and protocols to generate zero-knowledge (ZK) proofs on demand	**$22 Million**	Blockchain Capital, Polychain Capital
Ulvetanna	a startup that builds hardware to increase the efficiency of zero-knowledge-proof generation	**$15 million**	Bain Capital Crypto, Paradigm
Intella X	ext-generation gaming platform aiming to remove high entry barriers and improve user experience in web3 through features such as streamlined wallet creation and meta transactions	**$12 million**	Polygon, Animoca Brands

PEAK BLOCKCHAIN

WANT TO LEARN MORE?

Our analysts are here to help.

Take a call directly with a blockchain analyst to get answers to your questions, or get access to more market intelligence reports at peakblockchain.com.

info@peakblockchain.com | www.peakblockchain.com