Tips For Making The Most Of Blockchain Analysis

By **Nicole Moran, Robert Letson and Abe Chernin** (May 26, 2023)

Nicole Moran

Robert Letson

Abe Chernin

Blockchain analysis is a powerful tool that provides insight into what is happening on a blockchain network.

Who is trading with whom? Which wallets are most active on decentralized finance exchanges? Which wallets are sending and receiving funds from centralized exchanges? What validators are confirming new blocks, and what are the associated rewards?

These are all questions that can be answered by examining blockchain data, and with the right expertise, a clear and concise factual record of events can be established.

How Blockchain Analyses Can Help Verify SaaS Composition

As part of its recent settlement with the U.S. Securities and Exchange Commission, Kraken agreed to discontinue its staking-as-a-service, or SaaS, program for U.S. customers. This case is among the more recent examples of U.S. regulators' push into digital asset enforcement, and in particular, the happenings of the blockchain.

Recognizing that much ink has already been spilled discussing the Kraken settlement from a legal perspective, including which components of Kraken's service might satisfy Howey test requirements, we aim to provide a somewhat different perspective.

Specifically, by bringing to light the underlying blockchain transactions, tracing flows from user to exchange and exchange to blockchain, and examining the details of validator rewards and payouts, we can more fully understand the structure and composition of an exchange's staking service.

Staking is a necessary component of many blockchains. Some of the largest blockchains, including ethereum, cosmos and solana, rely on a proof-of-stake mechanism to validate transactions. Here, users deposit tokens in an escrow-like account — i.e., they "stake" cryptocurrencies — in exchange for the ability to validate transactions and add new blocks to the chain.

Users who successfully propose or validate blocks are rewarded with the blockchain's native cryptocurrency — e.g., ethereum on the ethereum blockchain. Validators are not guaranteed a profit, however. If validators make mistakes, they can be "slashed," a process through which they lose a portion of their staked assets.

Although simple in theory, staking requires technical expertise and sufficient startup capital. Ethereum, for example, requires users to stake 32 ethereum to create a validator node — the software that validates transactions — and gain the opportunity to earn etereum tokens.

At a current value of over $1,800 per ethereum, more than $50,000 in initial capital would

be required — a significant sum for the average crypto market participant. Additionally, staking requires knowledge of complicated software systems that may be inaccessible to an average market participant.

Observing that market participants have the desire to participate in blockchain validation but may not have the technical expertise or necessary capital, many exchanges have sought to broaden staking accessibility by offering SaaS to their customers.

SaaS programs stake specific crypto tokens on behalf of customers using customer deposits. The exchanges lower the startup capital requirements for individuals by aggregating customer assets and handling all the technical efforts that staking entails, such as running a validator node, in exchange for a fee.

Users earn interest on their deposits into the program based on the rewards earned from the staking validation determined by the blockchain. The exact details of the programs vary by exchange.[1]

Looking at the blockchain, one can observe which address proposed each block and how much that address received in rewards.[2] Combining this data with a list of staking addresses would allow for the computation of staking revenue received by each validator node. See the stylized example in Figure 1.

FIGURE 1
STYLIZED EXAMPLE OF ON-CHAIN STAKING REWARDS

Date	Node #	Node Address	Staking Rewards	Slashing Penalties
1/1/18	1	0x001	2.01 ETH	0 ETH
1/1/18	2	0x123	3.00 ETH	0 ETH
1/1/18	3	0x321	1.05 ETH	0 ETH

The next step would involve comparing aggregate staking revenues with, for instance, the exchange's payments to users who participated in the SaaS program.

FIGURE 2:
STYLIZED EXAMPLE OF STAKING REWARDS AND PAYOUTS

Date	Staking Rewards Accrued by Exchange	Staking Rewards Distributed to Users	Percent of Staking Rewards Distributed to Users
1/1/18	6.06 ETH	3.0 ETH	49.5%
1/8/18	5.10 ETH	2.5 ETH	49.0%
1/15/18	7.40 ETH	3.5 ETH	47.3%

As seen in the stylized example in Figure 2, payments to users are closely related to on-chain rewards, indicating that the exchange did not simply smooth over idiosyncratic rewards distribution with arbitrary award allotment.[3]

In other words, rewards were generated by the staking itself, and not a "fixed-rate of return" provided by the exchange, a result that could be useful in examining aspects of the Howey test.

Understanding Blockchain Data

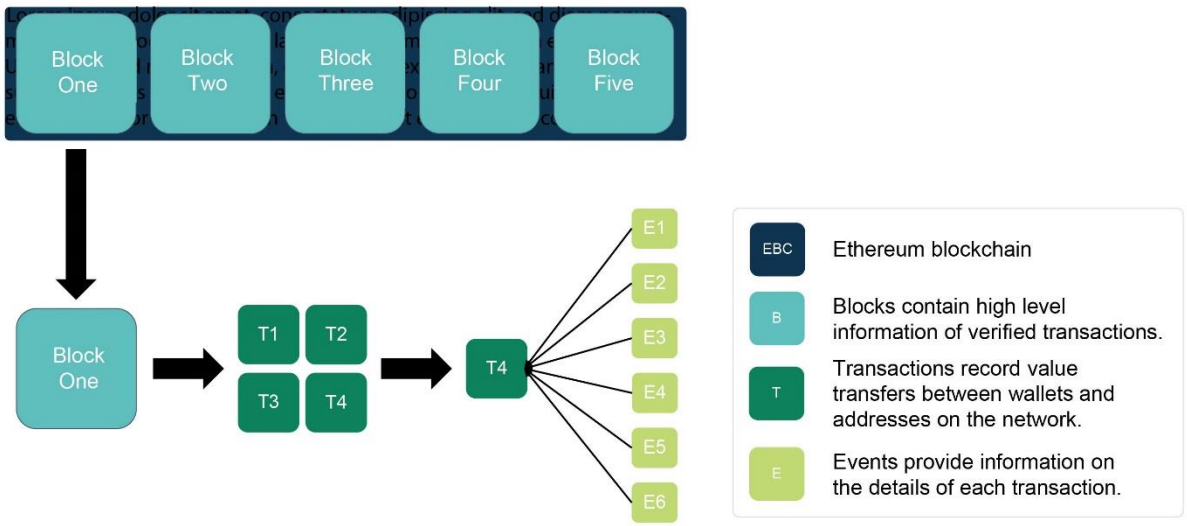
Evaluating staking rewards is just one application of blockchain data analysis. Questions regarding trade activity, liquidity provision, value transfers and more can all be answered by tapping into the underlying blockchain data, provided that one knows where to look.

In the context of class action litigation, identifying user participation and tracing flows of funds back to users may also help identify potential class members.

Blockchain data is a black box to many, so it is worthwhile to understand at a high level how they are stored and how they can be put to use.

Using ethereum as an example, Figure 3 depicts the blockchain structure. Ethereum blockchain data is stored across multiple tables. These tables can be linked based on the block number and transaction hash in each table.

FIGURE 3:
ETHEREUM BLOCKCHAIN STRUCTURE



For the gastronomes, you might think of the blockchain like how a restaurant records its food service operations.

A block is analogous to a restaurant's nightly ledger. It holds receipts of the meals that were served and drinks that were consumed, the tips earned, and who provided service. Blocks record the summary information but none of the details.

The transactions that comprise the blocks are more analogous to each table's receipt. On the blockchain, we observe value going from one wallet to another wallet, similar to how a table of diners might pay for their meal. Just as a receipt can contain multiple line items — appetizers, drinks, main courses, etc. — transactions on the blockchain can involve multiple arguments.

For example, transacting on popular decentralized finance exchanges requires inputs such as which coins are to be traded and the prices at which the transaction is to occur. In order to consummate a transaction, traders have to provide these necessary components.

Receipts at a restaurant contain clear records of what was served. Transactions on the blockchain contain clear records of the functional requirements for transactions to occur. Both involve the transfer of value.

In contrast to the high-level data recorded at the block and transaction level, events provide the real detail as to what is happening in each transaction, analogous to what happens in the kitchen as a meal is being prepared: cooking proteins, making sauces or assembling the plate.

The events record each component to a transaction — where the coins were sent and what happened to them along the way. This could involve multiple smart contracts, token swaps or liquidity pools. The contracts that wallets interact with will govern the number and type of events that are stored.

Put together correctly, blockchain data can be used to tell a compelling story and establish fact patterns.

Blockchain Transactions Will Remain in Focus

Given the breadth of transactions on the blockchain and the proliferation of ways participants can trade, it is unsurprising that regulators want to be more involved. The SEC is by no means the only governmental body seeking to have a heavier hand in regulating crypto-assets; Congress seems interested as well.

The Digital Asset Anti-Money Laundering Act of 2022, introduced by Sens. Elizabeth Warren, D-Mass., and Roger Marshall, R-Kan., proposes to "[e]xtend Bank Secrecy Act (BSA) responsibilities, including Know-Your-Customer requirements, to digital asset wallet providers, miners, validators, and other network participants that may act to validate, secure, or facilitate digital asset transactions by directing FinCEN to designate these actors as money service businesses (MSBs)."[4]

Putting aside the potentially far-reaching implications of what that means, it is worth noting that the common theme between the bill introduced by Warren and Marshall and the SEC action against Kraken is a desire to better understand what is happening on blockchains and by whom. Although the pseudo-anonymity of blockchain makes it complicated to answer these questions, it is not always impossible.

One of the great benefits of blockchain data is that it is a complete and freely available historical record. Although the data is publicly available, it still requires expertise to collect, decode and make sense of it.

Moreover, the abundance of blockchains and the sheer size of the data stored on each can make processing and analyzing them even more challenging. Yet, with data in hand, the

blockchain mystery begins to unravel, and the transactions, value transfers and smart contract events are there in plain sight.

As SEC Chair Gary Gensler said in his now famous "s-t-a-k-e, not s-t-e-a-k" "office hours" video:

> Whether they call their services lending, earn, rewards, APY, or staking, that relationship should come with the protections of the federal securities laws. Investors should receive important disclosures. For example, what do they actually do with your tokens?[5]

Blockchain analyses can often provide answers to that question.

Nicole Moran is a vice president, Robert Letson is a senior manager and Abe Chernin is a vice president at Cornerstone Research.

[1] Two of the most prominent U.S. exchanges, Coinbase and Kraken, are prime examples of how SaaS programs can differ, and how those differences can be important in the context of SEC's enforcement action. Whereas Kraken possesses, pools, and allocates users' staking deposits, Coinbase users maintain ownership over their deposited assets. See Coinbase User Agreement at https://www.coinbase.com/legal/user_agreement/united_states; SEC complaint at https://www.sec.gov/litigation/complaints/2023/comp-pr2023-25.pdf. This leads to key differences with respect to the timing of bonding/unbonding, staking rewards, and the use of unstaked assets.

[2] For example, one can observe that Hiveon Pool proposed block #15537386 on Ethereum and received 2.071 ETH as a reward. See https://etherscan.io/block/15537386. Blockchain data allow one to observe reward information at the transaction level as well. See https://etherscan.io/tx/0x660daa64a1cec6ad92790b90b732dd5a18c8eddc07e21f0dce55f9704f7377dd#statechange.

[3] The SEC complaint against Kraken alleged that Kraken's pooling of assets and proportional rewards met the criteria for the Howey Test.

[4] See https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations.

[5] See https://www.sec.gov/news/sec-videos/office-hours-gary-gensler-staking-a-service.