OULUN AMMATTIKORKEAKOULU

ONCHAIN ANALYTICS

A New Methodology for Cryptocurrency Analysis

Quyen Nguyen
Bachelor's Thesis
Autumn 2024
Degree Programme in Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology

Author(s): Quyen Nguyen
Title of thesis: Onchain Analytics: A New Framework for Cryptocurrency Analysis
Thesis supervisor(s): Janne Kumpuoja
Term and year of completion: Spring 2025
Pages: 43

This thesis deals with how blockchain technology, specifically by analyzing data from the blockchain itself, can help us better understand and value digital currencies. The main goal is to make it easier to grasp how the open and transparent nature of blockchains can improve how we determine the worth of cryptocurrencies. I look at various pieces of information from the blockchain, such as transaction volume, active addresses, network growth, to understand what they reveal about the health and usage of cryptocurrency networks.

We'll take a close look at Bitcoin, using past data to see how these measures can explain its price changes over time. Additionally, I demonstrate how a simple tool, such as a Telegram bot, can monitor significant wallet activity in real-time, making this analysis practical for everyday investors.

CONTENTS

GLOSSARY

BTC	Bitcoin
ETH	Ethereum
SAT	Satoshi (the smallest unit of Bitcoin)
TWh	Terawatt-hours (used for measuring energy consumption)
SHA256	Secure Hash Algorith 256-bit (a cryptographic hash function)
PoW	Proof-of-Work
PoS	Proof-of-Stake
PoA	Proof-of-Authority
Blockchain	A distributed database that maintains a growing list of records, called blocks, linked using cryptography
Mining	The process of confirming transactions and adding them to the blockchain ledger, typically involving solving cryptographic puzzles
Smart Contract	Self-executing contracts with the terms of the agreement directly written into code
Merkle Root	A hash of all the hashes of all the transactions in a block, used in block headers in blockchains like Bitcoin
Nonce	In mining, a number used once in cryptographic communication to produce a hash that meets the difficulty criteria

Wallets and Keys	Software or hardware tools used for managing and storing the private and public keys associated with cryptocurrency
Onchain Analysis	The study of data directly recorded on the blockchain to understand network health, user behaviour, and market trends
Exchange Inflows / Outflows	Refers to movement of cryptocurrencies into and out of trading platforms/exchanges
Market Value	The total market capitalization of a cryptocurrency, calculated by multiplying its current price by its circulating supply of coins
MVRV	Market Value to Realized Value, calculated as the market value divided by the realized value (the average price at which coins were last moved, multiplied by the total circulating supply)
NUPL	Net Unrealized Profit/Loss, measures the total unrealized profit or loss across all coins in circulation
LTH-SOPR	Long-Term Holder Spent Output Profit Ratio, looks at coins held for more than 155 days to gauge long-term holder behaviour
SOL	Solana, a blockchain network known for high transaction throughput and low costs
JS	JavaScript, a high-level programming language used in web development, particularly useful for real-time applications in blockchain
Cloudflare Workers	A platform for deploying serverless code, used here for running a bot to track blockchain transactions

Webhook	A method of altering the behaviour of a web page or web application with custom callbacks, used for real-time notifications

1 INTRODUCTION

In the current era of digital transformation, blockchain technology has revolutionized the way transactions are recorded and verified, offering unprecedented security and verifiability (Nakamoto, 2008).

Bitcoin, the oldest operational cryptocurrency, has the largest market capitalization, reaching 1.74 trillion of US dollars (Coinmarketcap, 12.11.2024). It allows people to send virtual money to each other without the need for a central authority. As the first of its kind, it solved the problem of how to prevent the double-spending of the same coins. The principles of its operation were described in 2008 by a person under the pseudonym Satoshi Nakamoto. A year later, the entire project of the decentralized cryptocurrency was launched, and it has been running continuously ever since.

Decentralization is the core idea on which Bitcoin is based. Simply put, it prevents any individual or group from altering or stopping the entire project (Davidson et al., 2018). Users send bitcoins in a peer-to-peer network where there is no central authority approving transactions for individual users. In this network, where trust among participants is minimal, there must be rules that the majority of users agree upon. With Bitcoin, these rules are set up in such a way that following them brings more benefits than breaking them. The implementation of these simple ideas has been functioning for years without major issues, and thanks to more advanced users, it becomes increasingly more secure. Attacking these principles is either impossible or not worthwhile for attackers due to decentralization. Therefore, it can be assumed that Bitcoin will continue to function, unlike most other cryptocurrencies.

The database where all transactions are recorded is called the blockchain. Unlike other fields, it is publicly accessible to all users. This attracts researchers from around the world who try to track the flow of virtual money, whether for purely scientific reasons or practical ones, like uncovering fraudsters or predicting Bitcoin price movements. However, users appear on the blockchain under pseudonyms called addresses, hiding their real identity from the outside world.

They can create virtually an unlimited number of these addresses. Despite this, there are methods to analyse this anonymous data and reveal at least some information. Our work deals with the possibilities of this analysis.

Understanding market dynamics in the cryptocurrency sector is crucial for investors due to the sector's volatility. Traditional financial analysis and price trend observation are supplemented by onchain analysis, which involves scrutinizing the data recorded directly on the blockchain for deeper insights. It provides a real-time view of network activity and health through metrics like transaction volumes and active addresses (Song et al., 2023). It cuts through the noise of crypto-related news by focusing on verifiable data, offering a clearer picture beyond market chatter. Certain onchain data can signal upcoming market movements, allowing to make strategic adjustments.

In Chapter 1, I introduce the fundamental elements that constitute the blockchain. Explaining how they interact to create a secure, decentralized ledger system. In Chapter 2 we have explored onchain analysis, focusing on the types of metrics available and discussed the various data sources used for these analyses. Chapter 3 then provides an overview of valuation methodologies for digital assets, contrasting traditional approaches with those utilizing onchain data.

2 BLOCKCHAIN

Bitcoin with a capital "B" refers to the complex set of decentralized nodes, protocols, and software that users utilize, while "bitcoin" (lowercase) refers to the unit of cryptocurrency that exists and functions within this network. One bitcoin can be divided into 100,000,000 parts. The smallest transferable unit was named after Bitcoin's creator, Satoshi Nakamoto. Therefore, the relationship is 1 BTC = 100,000,000 SAT, where BTC stands for bitcoin and SAT for Satoshi (Nakamoto, 2008).

The number of bitcoins in circulation follows clear rules. New bitcoins are released as rewards to so-called *miners*, who verify the validity of ongoing transactions and protect the network from attacks like the double-spending problem. Miners receive their rewards approximately every ten minutes, with the size of the reward halving every four years. Since 2009, the reward has decreased from an initial value of 50 BTC to 3.125 BTC as of mid-2024 (Figure 1). Over 19.7 million bitcoins have been mined so far, which represents 94% of the total cap of 21 million, that we are expected to reach around the year 2140 (River Financial Inc, 2024).

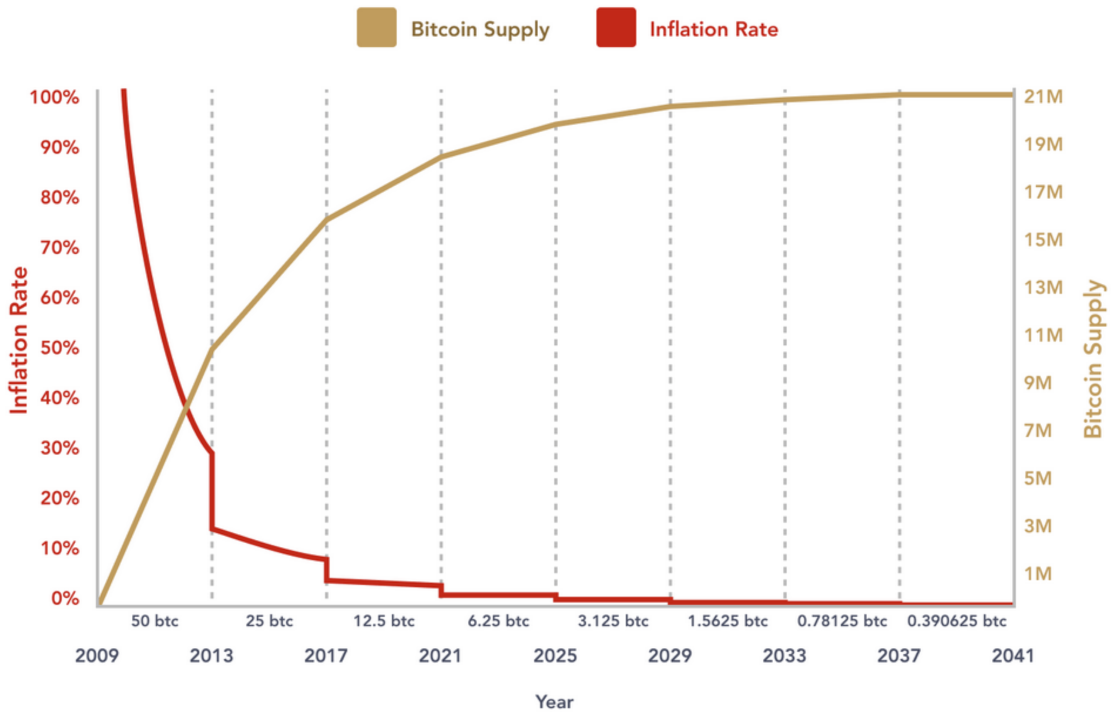


FIGURE 1. Bitcoin's block reward mechanism (River Financial Inc, 2024).

Users interact on the Bitcoin network under randomly generated pseudonyms known as *addresses*. These are used in transactions to transfer value from one address to another. However, a user does not have to use just one address; they can own practically an unlimited number of them. Indeed, Nakamoto recommended creating a new address for each incoming transaction (Nakamoto, 2008). This approach increases the network's anonymity and security because other users generally cannot connect a newly created address with those previously used by the same user. On the other hand, managing a large number of addresses individually would be impractical. Therefore, *wallets* were developed - software or hardware tools that can manage a set of such addresses. Users can also have multiple wallets.

Transactions are verified by miners and grouped into blocks with a maximum size of 1 MB. These blocks are then linked one after another in the mining process. This database, containing all completed transactions, is called the blockchain due to its structure. Along with the transactions, each block's header also includes, among other things, a hash of the previous block, preventing undetectable alterations of once-accepted transactions by potential attackers. Each block has a header that includes the hash of previous block header. Within each block header, there is a Merkle Root, which is a hash summarizing all the transactions in that block (Figure 2).

The mining process is computationally intensive. Miners must find a 32-bit *nonce* value so that the hash of the block containing this nonce starts with at least *n* zeros, where *n* is the mining difficulty parameter. The complexity of this cryptographic task changes over time based on the current mining power to ensure that, on average, it takes ten minutes to mine one block. Given that the hash function SHA256 used is one-way, the only efficient way to find the correct nonce is to try hashing one possibility after another. The energy expended guarantees the correctness and immutability of transactions recorded in the blockchain, as it serves as a barrier to potential attackers trying to alter transaction data. Verifying the correctness of hashes, on the other hand, is computationally light and can be performed by any user.

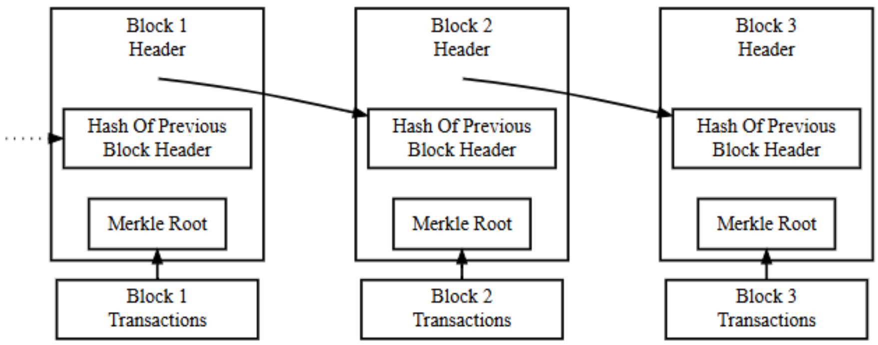


FIGURE 2. Structure of a blockchain (Bitcoin Project, 2009).

Bitcoin has no central authority that users must trust to manage the sequence of blocks correctly. Instead, the blockchain is stored across a large number of independent nodes simultaneously. For the majority of users to agree on the valid version of the blockchain without a central authority, two fundamental things are necessary. Firstly, the entire blockchain from the first mined block to the most recent one must be publicly accessible. This allows users to verify that the funds they're being sent on the blockchain actually exist. Secondly, there needs to be a method to distinguish the currently correct version of the blockchain from others. Bitcoin uses a consensus mechanism known as proof of work, under which the valid version is always the longest published chain of valid blocks.

2.1 Consensus Mechanism

To achieve consensus and verify the accuracy of data, various systems, or consensus mechanisms, are used. In principle, any user (if they participate in the network as a blockchain node) can propose adding new information, i.e., blocks, to the blockchain. Here, cryptographic proofs are used to confirm the authenticity of new information. This ensures its proper integration into the blockchain.

The leading consensus mechanisms include proof-of-word and proof-of-stake. However, in recent years, other methods like proof-of-authority have also come to the forefront. (Coinbase Global Inc, 2012)

2.1.1 Proof-of-Work

In the proof-of-work system, network participants must solve cryptographic puzzles to attach a new block to the blockchain, a process commonly known as "mining" (Nakamoto, 2008). These puzzles are generated from the cumulative data on the blockchain and the transactions slated for inclusion in the new block. Solving these puzzles involves submitting vast numbers of random guesses to algorithms, which then adjust these guesses until they match the new block's identifier. There's no shortcut to this guessing; it's purely computational, requiring miners to use brute-force methods. Upon correctly solving a puzzle, the miner earns a reward in digital currency, incentivizing participation in maintaining the blockchain's integrity.

This process, however, comes with a significant downside: the complexity of puzzles increases with each new block added, as each puzzle now includes more data from previous blocks, thereby demanding ever-increasing computational power from miners. This escalating demand for computational resources is one of the main criticisms of the proof-of-work system due to its substantial energy consumption. For example, in 2020, Bitcoin mining consumed an estimated 73 terawatt-hours (TWh) of electricity annually (Digiconomist, 2021), exceeding Finland's total electricity use of 61 TWh for the same year (Statistics Finland, 2021). This stark comparison illustrates the environmental impact of Bitcoin mining, outstripping the energy consumption of a country renowned for its high energy use due to its cold climate, vast distances, and energy-intensive industries. Consequently, this high energy requirement has led to the proof-of-work system being viewed as outdated, prompting newer blockchain projects to explore alternative, less energy-intensive consensus mechanisms.

2.1.2 Proof-of-Stake

Currently, the second most widely used and the most adopted consensus mechanism for new projects is the proof-of-stake, or proof of value. In this system, a validator is randomly selected to verify transactions. Only those who, within their node, stake a cryptocurrency asset as collateral through a smart contract, guaranteeing their honest behaviour, can become validators. The validator then uses pre-installed systems to validate blockchain transactions. If everything is done correctly, the validator receives a reward upon completing their participation in the validation system, similar to miners in a proof-of-work system. The more cryptocurrency assets a validator stakes, the higher the chance the system will select them to validate a transaction. At the same time, validators staking large amounts of cryptocurrency have a greater interest in the accuracy of the process, as they could lose the high value represented by their staked assets. This system has significant advantages over proof-of-work, such as reduced energy consumption, easier entry into the role of a validator as there's no need for highly powerful hardware, and a reduction in the risk of centralizing the blockchain. However, compared to proof-of-work, disadvantages might include the system's more complex implementation and its shorter history of use in the blockchain, which increases the risk of yet undiscovered security vulnerabilities (Ethereum, 2015).

2.1.3 Proof-of-Authority

Despite their widespread use, the two previously mentioned consensus mechanisms (proof-of-work and proof-of-stake) are not the only ones employed. Another one worth mentioning is proof-of-authority, which acts as an alternative to the proof-of-stake system, offering even lower energy consumption and reduced computational demands. In this system, the role of the validator is assumed by verified accounts. For this system, it's crucial to correctly set up the verification system for users who will be allowed to become validators. As mentioned earlier, the advantage of proof-of-authority lies in its minimal energy consumption and minimal computational requirements. A significant drawback, however, is a degree of centralization, which stems from the need to pre-approve validators, thus not sharing the decentralized nature that comes from allowing anyone to participate in the validation process of blockchain creation (Valente, 2020). Therefore, proof-of-authority is more commonly a system used in private or permissioned blockchains, though it can also be found in public blockchain projects. The suitability of a cryptographic proof thus depends on evaluating the needs of a specific project. Currently, we know of up to eight types of proofs, each with its unique advantages and disadvantages, and undoubtedly, with the further development of blockchain's popularity, we will encounter new ways to achieve consensus in blockchain networks (Cryptopedia, 2023)

2.2 Cryptographic Wallets and Keys

On the blockchain itself, no information is stored that could identify the owners of crypto assets. When acquiring a crypto asset, owners are provided with two different keys. The first is the so-called public key. We can think of this key as an email address or bank account number to which anyone can send transactions. However, these transactions cannot be validated without knowledge of the second key, known as the private key. The public key is derived from the private key. The only way to prove ownership is to know the unique private key. These keys serve as proof of ownership of the crypto asset and are also necessary for any manipulation with the asset. Currently, to manage and hold crypto assets, the technology of crypto wallets is almost always used (Nakamoto, 2008). Crypto wallets can come in the form of physical devices, software, or digital services. As such, they do not contain the crypto asset itself, which is part of the blockchain and thus decentralized, but are used to store private keys. Losing the private key makes it impossible to access or manipulate the crypto asset, and there is no way to recover access to the assets for an owner who does not know this key (Gomez, 2024) . Conversely, anyone who knows the private key can manipulate the assets as the legitimate owner. The private key can thus be compared to bearer securities and their abstract nature, where no verification of acquisition is required, and to exercise rights, only their presentation is sufficient. A wallet is not necessary for using a private key, but it greatly simplifies the handling of crypto assets and prevents unnecessary losses, which can cause significant financial damage. For example, it's estimated that up to 20% (Phillips, 2021) of Bitcoin cryptocurrency is permanently lost due to the loss of private keys needed to control these crypto assets. Essentially, crypto wallets function similarly to bank accounts, allowing for easy control and transactions with crypto assets while preventing losses.

2.3 Smart contract

Another widespread use of blockchain technology is so-called smart contracts. The definition of a smart contract is not currently standardized, but their purpose is clear – to minimize costs or to fully automate the transfer of value based on a general consensus about the state of affairs derived from a decentralized database. Each smart contract should consist of the following two parts: (i) a written document recording the agreements of the contracting parties and (ii) code that executes or enforces these agreements on a digital computer. Essentially, these are computer programs and the algorithms they contain, stored in the blockchain, which are executed upon the fulfilment of certain conditions. Smart contracts are predominantly utilized to automate and expedite the enforcement of contractual terms, where both parties can be certain that the agreed conditions will be met. They are most used to execute financial transactions, but in the future, they could also serve to enforce various types of securities, liens, or restrictions on property rights. (Szabo, 2018.)

3 ONCHAIN ANALYSIS

Onchain data refers to the volume of data that records all interactions with a blockchain network. This includes information related to all transactions occurring on a public blockchain network. Transaction details include sender and receiver addresses, transferred tokens, transaction amounts, transaction fees. It also contains block data such as timestamps, mining fees, rewards, and smart contract code (Nansen, 2024).

Investors often choose various analysis methods to evaluate crypto assets, including technical and fundamental analysis. However, these methods can be less effective when market makers manipulate charts or news is influenced (Investopedia, 2024). In contrast, onchain data is publicly transparent, immutable, and cannot be falsified, providing the most accurate information available. Similar to how fundamental analysis seeks to understand a company's true value, onchain analysis can be applied to value tokens or the blockchain itself. This type of analysis can be combined with technical analysis to determine appropriate short-term entry and exit points.

Onchain analysis is a research strategy that utilizes information directly from public blockchains to predict market movements. It's particularly useful in the crypto markets for understanding asset flows, miner behaviour, and large holder activities, aiding in investment decision-making. It can be combined with technical analysis for more precise market timing (Makori, 2023).

3.1 Onchain Metrics

Since onchain analysis is a relatively new field, there is not just one way to do it. Instead, there are several metrics for examining the different types of information available. Here, we will explore the most common approaches to get familiar with the data blockchains record and explain how this information can be useful for analysts.

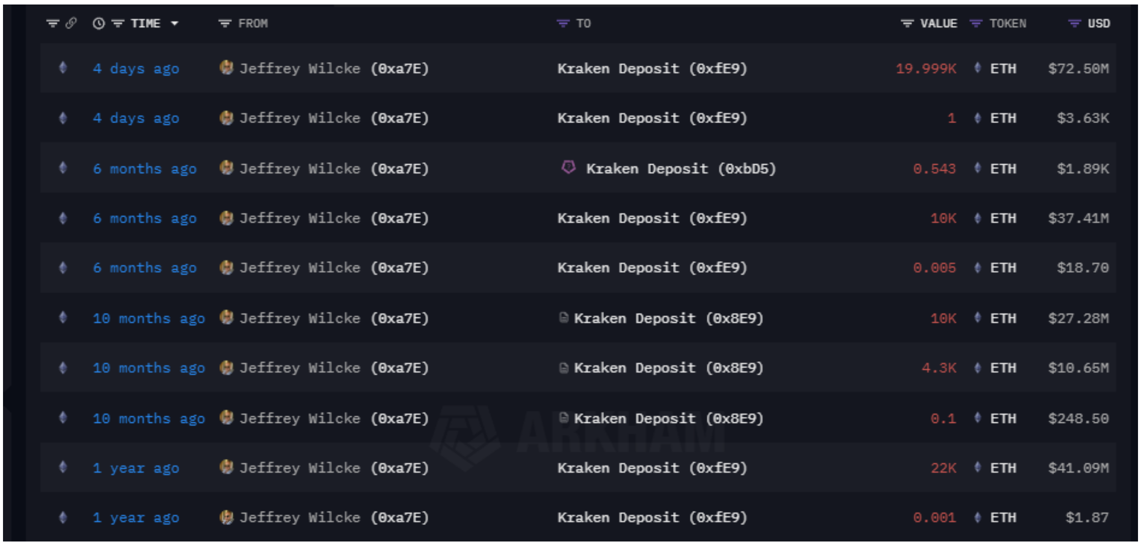
3.1.1 Transaction Metric

Blockchain technology tracks of every transaction that moves from one wallet to another. Each transaction has a unique *hash*, which specifies the sender, the recipient, the public key, the signature, the token ID, and the number of tokens involved (McCaffrey, 2019). Tracking transactions is a crucial aspect of onchain analysis, which enables the real-time observation of financial transactions

Analysing transactions provides insights into buying and selling behaviours. Since these details are updated on the blockchain immediately, analysts can react in real time to financial movements.

One can benefit from this by mimicking the strategies of successful investors and monitoring their movements. Additionally, we can keep an eye on suspicious wallets to prevent or track illegal money transfers.

Let’s take a look at Jeffrey Wilcke – one of the co-founders of Ethereum. He holds a substantial amount of ETH tokens. We can observe his recent transaction activities, which includes large transfers to exchanges like Kraken (Figure 3). In late November 2024, he transferred over $72 million worth of ETH to Kraken, which coincided with a peak price of ETH before it dropped by 5% over the next week. Analysts who followed this movement early could have potentially used this information for strategic trading decisions.



TIME	FROM	TO	VALUE	TOKEN	USD
4 days ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	19.999K	ETH	$72.50M
4 days ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	1	ETH	$3.63K
6 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xbD5)	0.543	ETH	$1.89K
6 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	10K	ETH	$37.41M
6 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	0.005	ETH	$18.70
10 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0x8E9)	10K	ETH	$27.28M
10 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0x8E9)	4.3K	ETH	$10.65M
10 months ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0x8E9)	0.1	ETH	$248.50
1 year ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	22K	ETH	$41.09M
1 year ago	Jeffrey Wilcke (0xa7E)	Kraken Deposit (0xfE9)	0.001	ETH	$1.87

FIGURE 3. Ethereum Transfers to Kraken Deposit by Jeffrey Wilcke (Arkham Intelligence, 2024)

3.1.2 Wallet Holdings Metric

While the balance in someone's bank account remains private, the quantity of a specific cryptocurrency token owned by a blockchain wallet address is openly logged on the blockchain. This transparency allows us to view both current and past holdings for various tokens, forming a foundational aspect of onchain analysis - understanding who owns which tokens and in what quantities (Nansen, 2024).

Wallets can belong to individuals, funds, exchanges, or even governments. Thus, observing the wallet's current and historical token balances gives us insight into the token holdings of these entities over time.

Although blockchain addresses are inherently pseudonymous, appearing as strings like B6QCDzxzBvCNMTGgzxSQ2kcnWHxtujvnFHsx3W1kqqFt. This linkage enables us to identify the probable owner of an address and monitor their token holdings, both current and historical (Investopedia, 2024).

With access to such onchain wallet data, you can verify claims and statements made on social platforms or in official releases. For example, you might question if an influencer genuinely supports a cryptocurrency project or if they're simply paid for promotion. Similarly, you can assess whether a venture capital firm holds tokens for the long term or is in the process of liquidating them. This data empowers us to conduct our own research (Nansen, 2024).

For instance, we can examine what might be Blackrock's holdings – a well-known global investment management corporation. The portfolio lists significant holdings in Bitcoin and Ethereum. The total value of portfolio is listed over 34,7 billion US dollars (Figure 4).

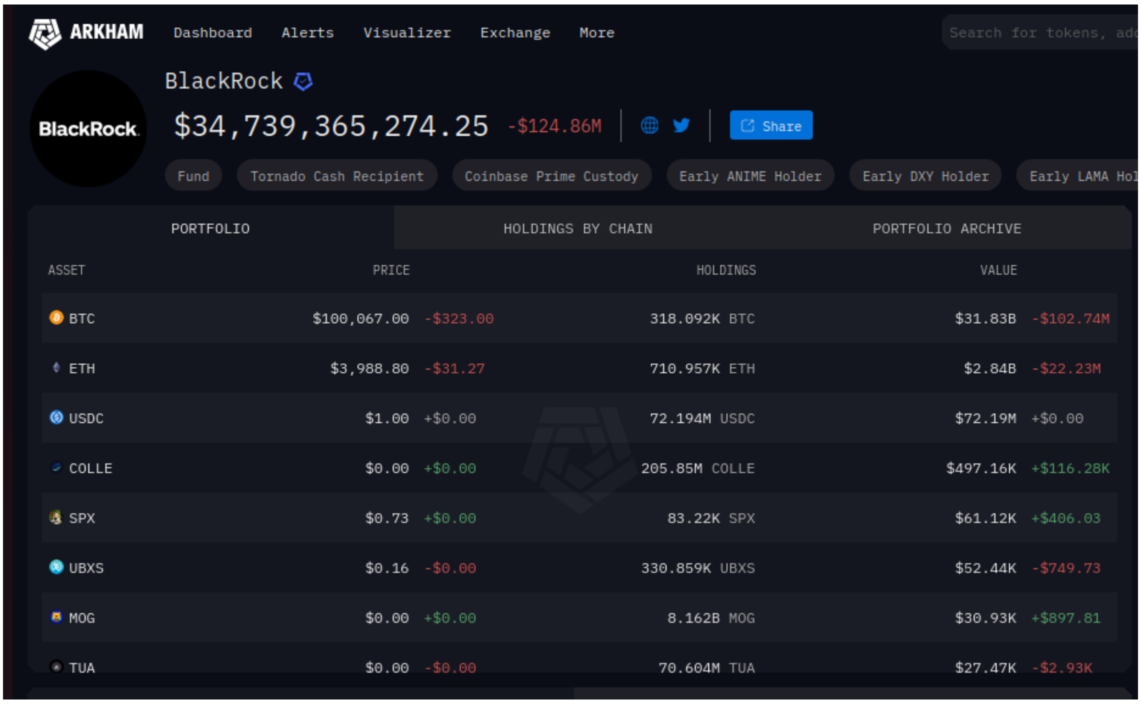


FIGURE 4. Blackrock's Holdings (Arkham Intelligence, 2024)

3.1.3 Largest Holders Metric

Onchain analysis allows us to examine the portfolios of all wallets, revealing who the primary holders of any given token are.

For instance, consider the leading wallets holding Jupiter tokens, as shown in Figure 5.

#	Account	Token Account	Quantity	Percentage	Value
1	Jupiter Team Cold Wallet	26ddLrqXDext6caX1gRxARePN4kzajyGiAUz9JmzmTGQ	2,149,366,668.17	30.70%	$1,994,706,840.
2	Jupiter Community Cold Wallet	6G4XDSge4txj5tBkA5gZqefXXE3BRxqA37Yb1pmrHv6N	1,700,000,000.00	24.28%	$1,577,674,800.
3	Any5gL74oUQy9Psb3goym9STaYMau4CMrTkryS37T7iz	64cmXBSdHeBQ4zK9yVXtVuLMcVUwGg3fvG7fooSqHwmk	429,344,964.49	6.13%	$398,451,018.2
4	Jupiter Community Hot Wallet	K6U4dQ8jANMEqQQycXYiDcf3172NGefpQBzdDbavQbA	357,349,634.36	5.10%	$331,636,184.0
5	Binance 3	GDijXRGfd1jhk5GkRPp1TDnEH2FfHURSRZeB5um3pUWk	188,743,162.29	2.69%	$175,161,959.3
6	Jupiter Team Hot Wallet	7bEL9XkPGNg7a3oSiUERKsZtFoJMqKh6VhGDCmMCPqdg	126,376,933.04	1.80%	$117,283,354.4
7	CPZmKkAhD2wv1Z21EUZvdH8ZeSD13geAnSfyVBwcW8XK	DWVtxR7oo3uTiuM3o1cCxTJ5wM8Wnjvu1apwMkQhdedY	104,479,516.84	1.49%	$96,961,588.73
8	6wsjaQTidXNqmPDw4st2yMtFmTk7yyBEox5SydFQeJe7	HG6XGeAwBueqMbubLbMMWRCfhC1wKjDJmQiJjjFdTJDc	94,414,766.37	1.34%	$87,621,057.44
9	27b4PRN7K37rpTywq65t29rjuNfQkYpxZUjkbtHc5VvZ	ASehmX2sjG1Qz7MQyLJu8wBoV2Xx8cCV3uU8VbBDGQJQ	58,002,761.65	0.82%	$53,829,114.93
10	Binance 2	E6FLdjDBtHvzhMGihcbec34KfcAqSYW67kfJV8RAKH1f	54,524,572.78	0.77%	$50,601,202.62

FIGURE 5. Top 10 holders of Jupiter token (Solscan, 2024)

Tracking these significant token holders can be useful for traders. Large holders have a greater impact on price movements compared to those with smaller stakes. Their substantial transactions can create more influence on a token's price, whether driving it up or down, and can also sway trading volume or the overall market sentiment towards that token.

Moreover, understanding how tokens are distributed among wallets can inform investors about the concentration of a token in potentially insider-held accounts. If many of the top holders are rival investment funds, this might indicate a bullish outlook or a shared positive sentiment among these competitors regarding the token. (Coinbase, 2012.)

3.1.4 Inflows and Outflows Metric

Exchange flows describe the transfer of assets between wallets of individual users and those controlled by cryptocurrency exchanges. Through onchain analysis, we can monitor the net flow of these assets to specific exchanges, which analysts often use to study trends over extended periods or focus on particular tokens.

Generally, an inflow of tokens into exchanges is viewed as a bearish signal since it typically suggests that these tokens are being added to exchange accounts with the intent to sell. Conversely, when tokens are withdrawn from exchanges to personal wallets, this is seen as a bullish sign, indicating that individuals might be planning to hold these tokens for an extended period, moving them away from platforms where they are commonly traded. (Wright, 2024.)

According to CoinShares, digital investment products experienced inflows amounting to $2.2 billion between October 26 and November 2, 2024 (Figure 6), contributing to a year-to-date total of $29.2 billion, setting a new record. (Butterfill, 2024). Given the range of week 44, Bitcoin's share in the total crypto asset flows is approximately 99.04%. This figure highlights Bitcoin's significant share among the listed cryptocurrencies, underscoring its leading position in the market as of the date provided in the figure 7.

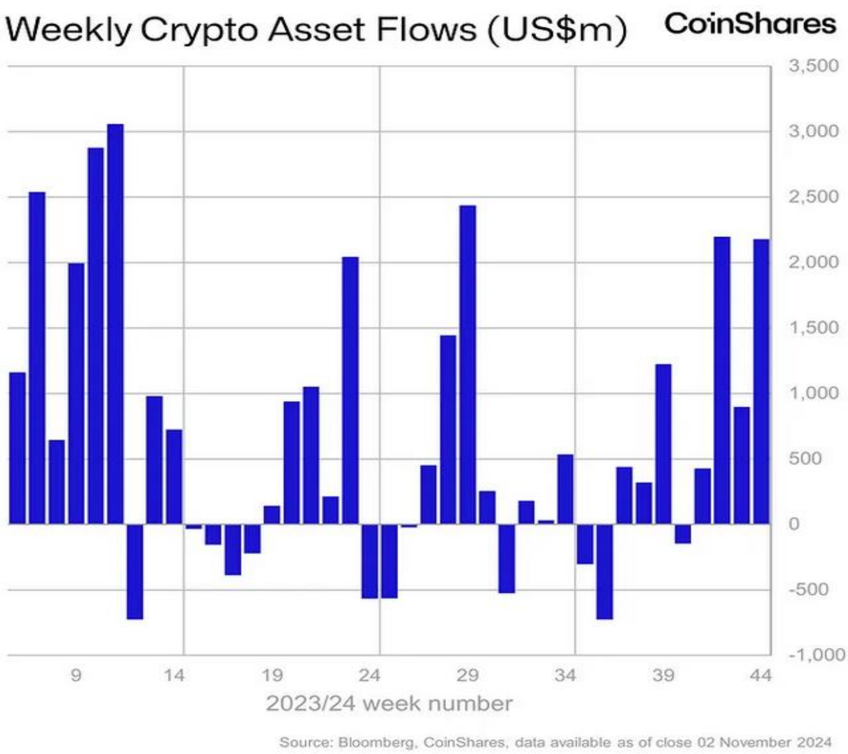


FIGURE 6. Total cryptocurrencies asset flows in millions of US dollars (Butterfill, 2024)

Flows by Asset (US$m)

	Week flows	MTD flows	YTD flows	AUM
Bitcoin	2,156	-67	27,622	83,656
Ethereum	9.5	-13.7	758	10,232
Multi-asset	-3.1	0.1	467	5,601
Solana	5.7	-0.6	69	1,431
Binance	-	-	-2	575
Litecoin	-0.8	0.1	42	148
Short Bitcoin	8.9	1.5	63	91
XRP	-0.1	-	26	86
Tron	-	-	1	49
Cardano	-0.0	0.0	11	47
Other	1.1	-	183	256
Total	**2,177**	**-79**	**29,241**	**102,171**

Source: Bloomberg, CoinShares, data available as at 02 November 2024

* Independent daily attestation by The Network Firm

FIGURE 7. Flows by asset in millions of US dollars (Butterfill, 2024)

3.2 Onchain Analytics Tools

Onchain analytics tools have become essential in the cryptocurrency ecosystems, enabling users to gain insights into blockchain transactions and monitor various network activities.

3.2.1 Dune Analytics

Dune Analytics is a collaborative platform that allows users to create and share queries to analyse Ethereum data. It provides a user-friendly interface for building visualizations and dashboards, facilitating the exploration of onchain metrics and trends. Users can leverage community-created queries or create their own to gain insights into specific blockchain events and behaviours (Stevens, 2023).

3.2.2 Arkham Intelligence

Arkham Intelligence positions itself as a leader in the crypto analytics space, offering tools to decode complex blockchain data. With features like entity-based intelligence, which analyses the real-world entities behind transactions, and the Arkham Oracle, a text-prompt-driven analytics tool, it aims to empower users to make informed decisions. Arkham also provides an API for advanced users to customize their data analytics processes and track onchain activity effectively (Kejriwal, 2024).

3.2.3 Glassnode

Glassnode specializes in onchain market intelligence, providing various metrics and analytics related to the Bitcoin and Ethereum networks. Users can access real-time data, historical insights, and customizable dashboards that help monitor network health and trader sentiment. Its analytics focus on key indicators, such as active addresses, transaction volumes, and miner activity, which are crucial for understanding market dynamics (Glassnode, 2024).

3.2.4 ChainExposed

ChainExposed positions itself as a specialized onchain analytics tool focused primarily on Bitcoin metrics and analysis, offering insights into the behaviour of different types of holders, like short-term and long-term holders, through its unique metrics and research. Additionally, it includes onchain indicators, which are essential for predicting cycle tops and bottoms (ChainExposed, 2025).

4 THE RELATIVE UNREALIZED INDICATOR (RUPI)

The Relative Unrealized Profit Indicator, commonly known as MVRV (Market Value to Realized Value), is a significant financial metric used primarily in the analysis of cryptocurrency markets. This indicator provides insights into the unrealized profits or losses held by investors by comparing the current market value of an asset to its realized value—the average price at which the asset was acquired. This tells us if the market is currently holding more profit or loss overall (Miłosierny, 2023).

The MVRV has become a key tool for understanding market mood and making investment choices. High MVRV values often indicate significant unrealized profits, suggesting an overvalued market that may soon correct. Conversely, low MVRV values can signal that the market is under stress, potentially offering good times to invest. This ability to indicate both positive and negative market trends makes MVRV an essential part of trading strategies for both individual and large-scale investors (CryptoQuant, 2024).

In essence, the relative unrealized profit indicator, or MVRV, is crucial for deciphering the inner workings of cryptocurrency markets. It sheds light on potential profit situations and investor sentiment, helping investors make smarter choices. However, its limitations mean that it should be interpreted carefully, especially in the ever-evolving financial landscape.

Beyond MVRV, other pivotal onchain indicators include the Net Unrealized Profit/Loss (NUPL) and the Long-term Holder Spent Output Profit Ratio (LTH-SOPR). NUPL quantifies the total unrealized profit or loss across all coins in circulation by subtracting the realized capitalization from the market capitalization, offering a broad perspective on market sentiment; high values suggest euphoria, while low values indicate market capitulation (Figure 8). On the other hand, LTH-SOPR looks specifically at coins held for more than 155 days, providing insights into the behaviour of long-term holders. When LTH-SOPR exceeds 1, it indicates long-term holders are selling at a profit, potentially signalling market tops, whereas values below 1 could mean long-term holders are capitulating, often seen at market bottoms. Together, these indicators complement MVRV, offering a nuanced view of market conditions and investor behaviour in the cryptocurrency space (CryptoQuant, 2024).

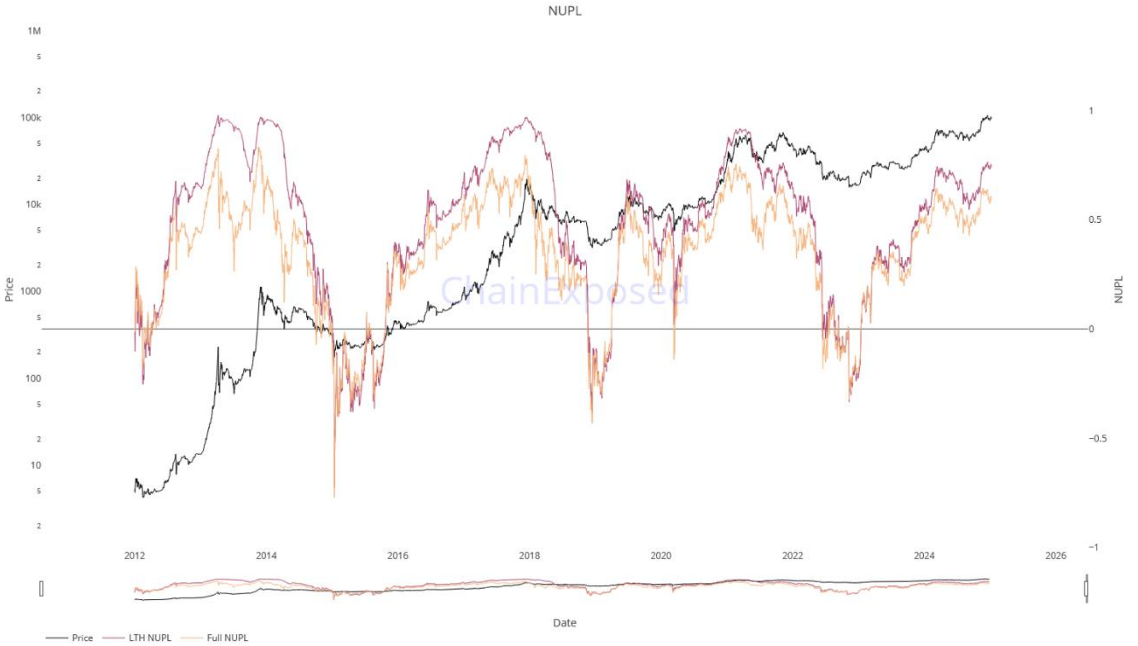


FIGURE 8. Long-term Holders Net Unrealized Profit/Loss (LTH NUPL) Indicator (ChainExposed, 2025).

FIGURE 9. Spent Output Profit Ratio (SOPR) Indicator (ChainExposed, 2025).

4.1 Market Value and Realized Value

The calculation of the RUPI begins with understanding two key concepts: Market Value and Realized Value. Market Value is calculated by multiplying the current price of an asset by the volume at entry. On the other hand, Realized Value comes from the average price at which the asset was last transferred, times the total circulating supply of coins. This comparison helps evaluate the unrealized profit or loss, providing an estimate of the paper gains or losses for Bitcoin investors (Schultze-Kraft, 2019).

4.2 Market Value and Realized Value Ratio

The MVRV Ratio is a crucial metric calculated by dividing the Market Value by the Realized Value. This ratio serves to indicate whether an asset is overvalued or undervalued in relation to its historical cost basis. The MVRV Ratio is further normalized to ensure comparability, scaling it to a range from 1-6, which helps in analyzing market trends over a specified period (Figure 8).

During periods of significant market euphoria, such as 2013, 2017, and 2021-2024, the MVRV ratio spikes dramatically. These spikes indicate that the market value of Bitcoin is significantly higher than its realized value, suggesting high unrealized profits for holders. This often coincides with peak market sentiment and potential market tops.

High MVRV ratios, especially at extreme levels like those seen in 2013 and 2017, signal times to consider taking profits as the market may be overheating.

Conversely, when the MVRV ratio dips below 1, as seen around 2015, 2018-2019, and potentially in future cycles, it indicates that the market value has fallen below the realized value. This suggests that holders are collectively underwater, often correlating with market bottoms or periods of capitulation. The chart suggests that periods when the MVRV ratio is below 1 could be seen as buying opportunities since the market value is lower than the collective cost basis of all coins. This was notably the case during the 2015 and 2018-2019 bear markets. (ChainExposed, 2025.)

FIGURE 10. Market Value Realized Value (MVRV) Indicator (ChainExposed, 2025).

5 WALLET TRACKING SYSTEM

This chapter aims to bridge the gap between raw blockchain data and practical utility by introducing a real-time wallet tracking system via a Solana-based Telegram bot. This demonstration will be conducted following a tutorial provided by the Helius team, showcasing how onchain analytics can be directly applied to enhance investment decisions, monitor transactions, and detect market trends in real-time.

5.1 Solana

Solana was selected for this demonstration due to its unique attributes that align with the requirements of a real-time wallet tracker.

One key attribute is lightning fast. Solana's architecture supports more than 4,407 transactions per second, which is essential for real-time applications where any delay in data processing can mean missed opportunities or outdated information. This high capacity allows the bot to manage numerous queries and updates simultaneously without any network congestion.

Another compelling reason is low transaction costs. In contrast to other blockchains where transaction fees can become excessively high, particularly during peak usage, Solana offers very affordable costs. This is crucial for a wallet tracking application that requires frequent blockchain queries, making sure that the operational costs do not erode the financial advantages provided by the insights.

Lastly, scalability is a fundamental aspect of Solana's design. It is built to expand seamlessly, accommodating an increase in user numbers or query complexity without compromising performance. (Solana, 2025.)

5.2 JavaScript

JavaScript is a high-level programming language primarily used for web development to create interactive and dynamic elements within websites. It is known for its ability to manipulate and update the content of web pages in real-time without needing to reload the entire page, enabling features like form validation, responsive design, and interactive animations (MDN, 2024).

JavaScript was the language of choice for implementing a bot to track onchain activities because it offers a robust ecosystem with Node.js for server-side operations, fitting well with the asynchronous nature of blockchain interactions (Sergey, 2022).

5.3. Implementation

5.3.1 Setting up a Telegram Bot

The process was initiated by starting a conversation with BotFather. I searched for BotFather in the Telegram search bar and clicked it to start the chat. Once in the conversation, a new bot was created by typing and sending the command '/newbot'. BotFather then guided me through naming the bot and assigning it a username. After completing these steps, an access token was provided by BotFather, which was noted down for later use in the setup shown in figure 11. (Venter, 2024.)

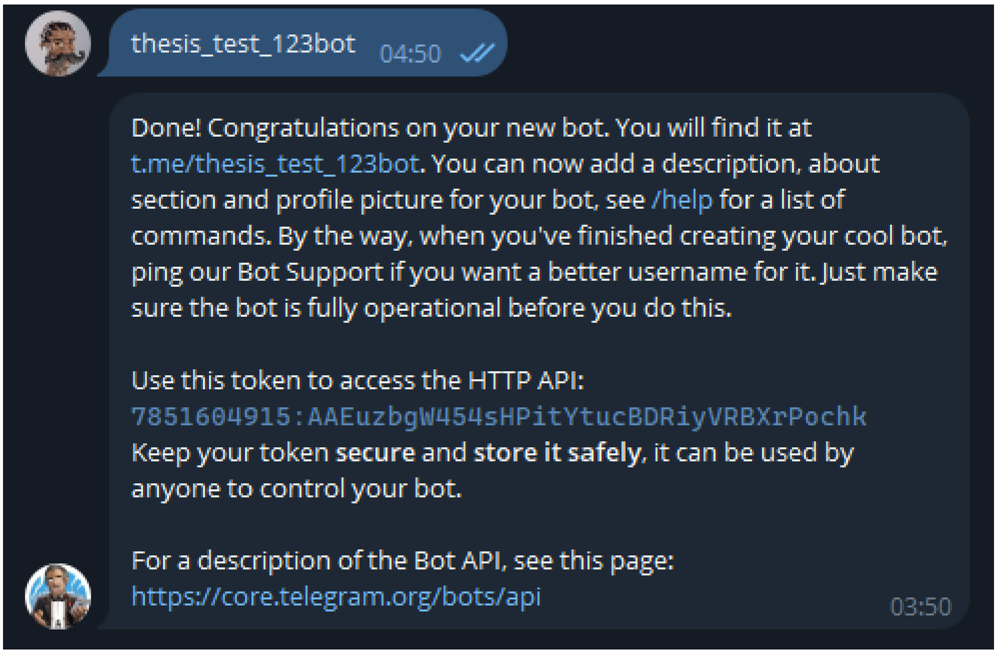


FIGURE 11. Telegram Bot Token Creation (Telegram, 2025).

5.3.2 Setting up the Webhook Provider

Cloudflare Workers were utilized to deploy code that runs continuously, ready to respond to updates from the webhook. A webhook is essentially an HTTP callback: an HTTP POST that occurs when something happens. Instead of continuously polling a server for updates, a webhook allows a service to notify your application whenever an event occurs. This is useful for real-time applications where immediate action upon an event is needed (Svix, 2025).

In this implementation, Helius was used as the webhook provider for monitoring Solana blockchain activities. A new webhook is created through the Helius dashboard, specifying a Trigger Event, typically transactions involving a particular Solana account, and a Callback URL, which leads to the deployed Cloudflare Worker (Figure 12). When an event occurs, an HTTP POST is sent to this URL with details of the event.

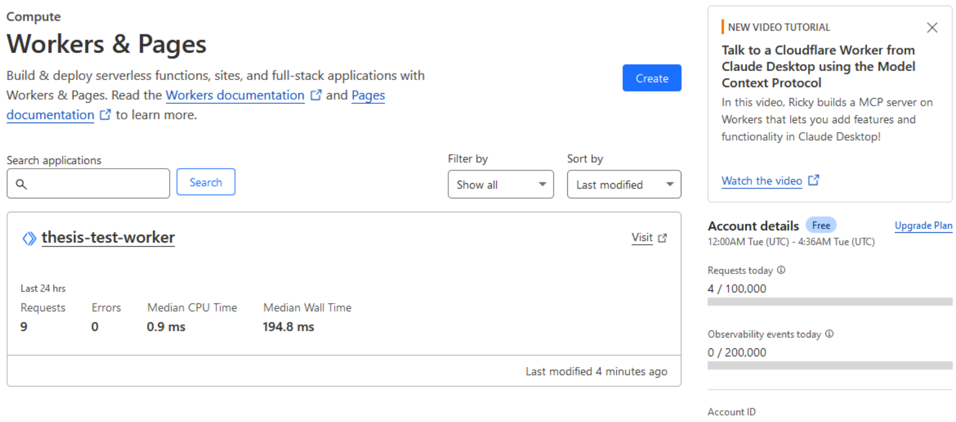


FIGURE 12. Workers and Pages Dashboard (Cloudflare, 2025).

5.3.3 Cloudflare Worker as the Webhook Listener

The code is deployed to Cloudflare Workers shown in figure 13, where it listens for webhook calls from Helius. The script handles incoming POST requests, parses the payload to interpret the event details, and may perform actions based on these details, such as updating databases, sending notifications, or processing data further. This ensures that applications can react promptly to blockchain events.

Sensitive data like API keys or tokens are managed as environment variables in Cloudflare Workers. This approach is adopted to keep credentials secure, avoiding their exposure within the codebase.

```
worker.js 3
worker.js > handleRequest

const TELEGRAM_BOT_TOKEN = BOT_TOKEN;
const TELEGRAM_CHAT_ID = CHAT_ID;
const HELIUS_API_KEY=API_KEY;
const HELIUS_RPC_URL = `https://mainnet.helius-rpc.com/?api-key=${HELIUS_API_KEY}`;

addEventListener('fetch', event => {
  event.respondWith(handleRequest(event.request))
})

async function handleRequest(request) {
  if (request.method === 'POST') {
    const requestBody = await request.json();
    console.log('Received POST request with body:', requestBody);
      const Transferdescription = requestBody[0].description;
      const Transfertimestamp = new Date(requestBody[0].timestamp * 1000).toLocaleString(); // C
      const Transfersignature = `https://xray.helius.xyz/tx/${requestBody[0].signature}`
      // Construct the message
      const messageToSendTransfer =
      `----NEW UPDATE---\n`+
      `Description:\n${Transferdescription}\n` +
      `Signature:\n${Transfersignature}\n` +
      `Timestamp:\n${Transfertimestamp}`;
      await sendToTelegramTransfer(messageToSendTransfer); // Send to Telegram



    return new Response('Logged POST request body.', {status: 200});
  } else {
    return new Response('Method not allowed.', {status: 405});
  }
}

// This function is used to send NFT Updates to the bot
async function sendToTelegramNFT(message, imageUrl) {
  const telegramUrl = `https://api.telegram.org/bot${TELEGRAM_BOT_TOKEN}/sendPhoto`;
  const response = await fetch(telegramUrl, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json',
```

FIGURE 13. Cloudflare Worker Code (Venter, 2024).

5.3.4 Security

Security was a concern throughout the implementation process. The access token received from BotFather was stored in a secure file, utilizing Cloudflare's environment variables to prevent direct access from the codebase.

Additionally, in the webhook configuration, as shown in figure 14, the webhook URL was set to accept requests only from Helius, enhancing security by limiting the sources of incoming POST requests. The option to add an Authentication Header was left empty as it wasn't necessary with the current setup, but it provides an additional layer of security if custom authentication were needed.

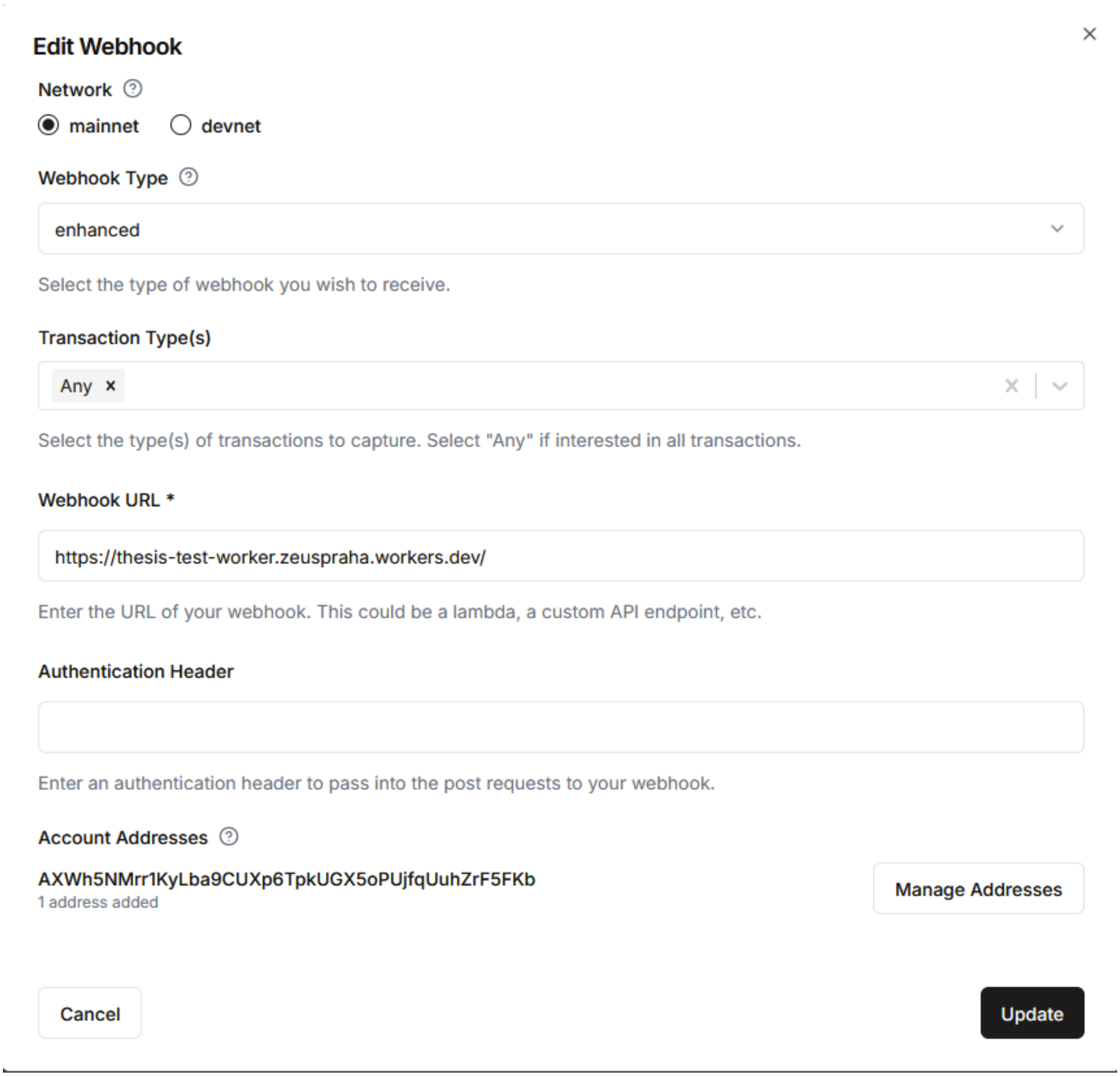


FIGURE 14.Helius Webhook Settings (Helius, 2025).

5.3.5 Results

The system is configured to track all transactions involving the wallet address AXWh5NMrr1KyLba9CUXp6TpkUGX5oPUjfqUuhZrF5FKb. This includes both incoming and outgoing transactions, ensuring that any movement of funds to or from this wallet is immediately captured. The transactions monitored are not limited to simple transfers but could potentially include interactions with smart contracts, token minting, or NFT transactions, given the capabilities of the Solana blockchain.

In terms of efficiency and real-time nature, the notifications demonstrate a high level of responsiveness. As depicted in the image, the notification was sent at

1:02:22 PM on 1/2/2025, which indicates that the system processes and alerts on transactions almost instantaneously. This real-time functionality is crucial for applications requiring immediate awareness of blockchain activities, like trading bots, security monitoring, or real-time analytics. (Figure 15.)

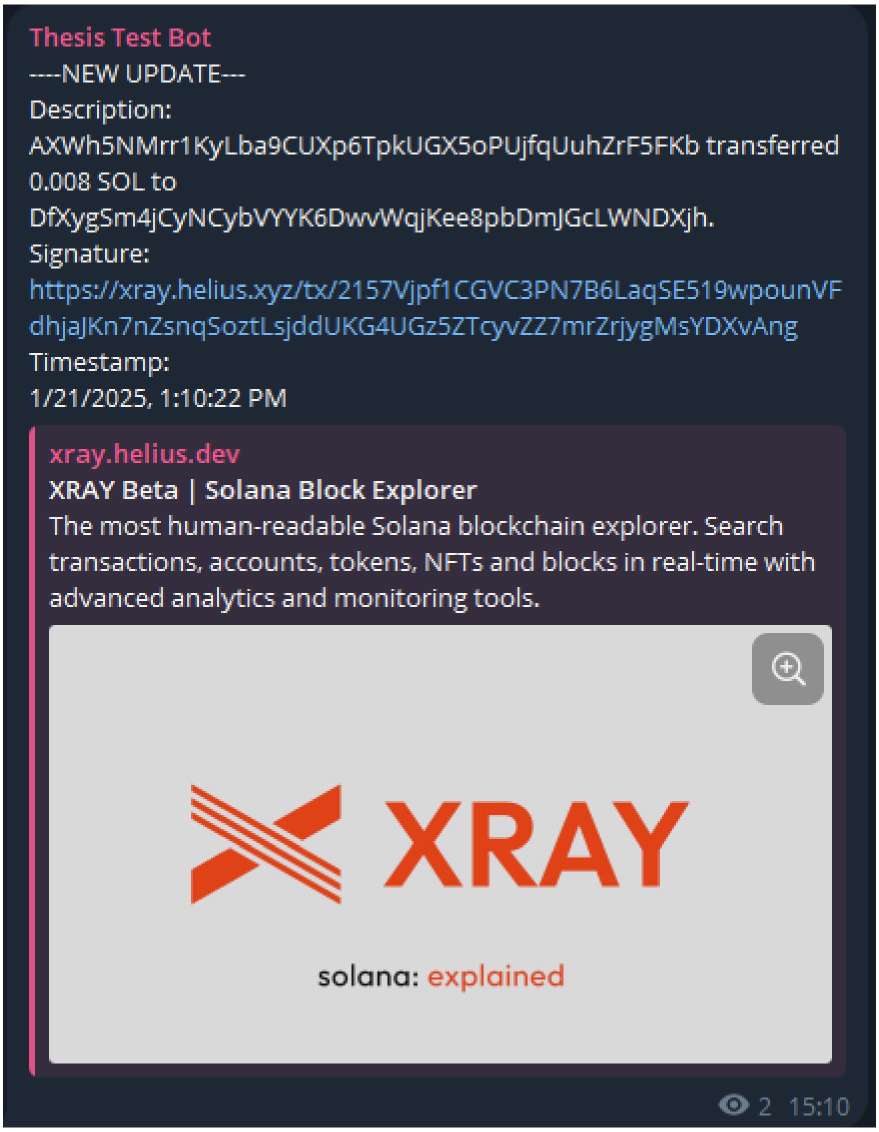


FIGURE 15. Transaction Notification to Telegram

6 CONCLUSION

The exploration of onchain analytics in this thesis has helped to clarify a transformative approach to understanding and valuing cryptocurrencies, leveraging the transparent and immutable nature of blockchain. By exploring Bitcoin's historical data and applying onchain metrics such as transaction volume, wallet holdings, and the Market Value to Realized Value (MVRV) ratio, this research has demonstrated how these tools can offer deeper insights into network health and market dynamics compared to traditional financial analysis. Furthermore, the development and implementation of a real time wallet tracking system have showcased the practical utility of onchain analytics, bridging raw blockchain data with actionable tools for investors.

Reflecting on the results of this research, it is evident that onchain analysis provides a robust framework for interpreting cryptocurrency markets. The analysis of Bitcoin's MVRV ratio, for instance, revealed its ability to signal potential market tops and bottoms—high values in 2013 and 2017 indicated euphoria and overvaluation, while dips below 1 in 2015 and 2018-2019 pointed to undervaluation and capitulation. Similarly, metrics like Net Unrealized Profit/Loss (NUPL) and Long-Term Holder Spent Output Profit Ratio (LTH-SOPR) enriched this perspective by highlighting investor sentiment and long-term holder behaviour, offering a more nuanced view of market cycles. These findings suggest that onchain analytics not only enhances our understanding of price movements but also empowers investors to make data-driven decisions in a volatile environment.

The Telegram bot implementation further underscored the real-time potential of onchain analytics. By tracking wallet activities with near-instantaneous notifications. This system proved its efficiency and responsiveness. This hands-on experiment highlighted how onchain data, once abstract, can be transformed into a tangible asset for everyday investors, enabling them to monitor significant transactions and detect trends.

Personally, I find the most compelling outcome of this research to be its democratizing potential. Onchain analytics levels the playing field by providing transparent, verifiable data that anyone with the right tools can access and interpret. Unlike traditional markets, where insider knowledge often dictates success, the openness of blockchain data—exemplified by tracking large holders like Jeffrey Wilcke or entities like BlackRock—offers retail investors unprecedented visibility into market movers. However, this transparency comes with challenges, such as the pseudonymous nature of addresses and the need for sophisticated tools to decode complex data, which my bot seeks to address in a small but practical way.

In conclusion, this research affirms that onchain analytics is not merely a supplementary tool but a foundational framework for cryptocurrency analysis. By combining historical insights with real-time applications, it offers a comprehensive lens through which to view digital assets. My results underscore its value in predicting market trends and enhancing decision-making, while the Telegram bot exemplifies its practical reach. As blockchain technology matures, I am confident that onchain analytics will play a pivotal role in shaping a more transparent, informed, and equitable financial ecosystem.

REFERENCES

Arkham Intelligence (2024). Blackrock's Holdings. URL: https://intel.arkm.com/explorer/entity/blackrock. Accessed: 2.12.2024

Arkham Intelligence (2024). Jeffrey Wilcke's Transaction History. URL: https://intel.arkm.com/explorer/entity/jeffrey-wilcke. Accessed: 2.12.2024

Bitcoin Project (2009). Block Chain. URL: https://developer.bitcoin.org/devguide/block_chain.html. Accessed: 15.11.2024

Butterfill, J. (2024). Volume 207: Digital Asset Fund Flows Weekly Report. CoinShares. URL: https://blog.coinshares.com/volume-207-digital-asset-fund-flows-weekly-report-72042acb489f. Accessed: 6.12.2024

ChainExposed (2025). URL: https://chainexposed.com/. Accessed: 08.01.2025

ChainExposed (2025). Long-term Holders Net Unrealized Profit/Loss (LTH NUPL) Indicator. URL: https://chainexposed.com/NUPL.html. Accessed: 08.01.2025

ChainExposed (2025). Market Value and Realized Value (MVRV) Indicator. URL: https://chainexposed.com/MVRV.html. Accessed: 08.01.2025

ChainExposed (2025). Spent Out Profit Ratio (SOPR) Indicator. URL: https://chainexposed.com/SOPR.html. Accessed: 08.01.2025

Cloudflare (2025). Workers and Pages Dashboard. URL: https://dash.cloudflare.com. Accessed: 15.01.2025

Coinbase Global Inc (2012). What are crypto whales. URL: https://www.coinbase.com/learn/crypto-basics/what-are-crypto-whales. Accessed: 4.12.2024

Coinbase Global Inc (2012). What is proof of work or proof of stake. URL: https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake. Accessed: 13.11.2024

Coinmarketcap (2024). Market capitalization of Bitcoin as of November 12, 2024. URL: https://coinmarketcap.com. Accessed: 12.11.2024

Cryptopedia (2023). Blockchain consensus mechanisms beyond PoW and PoS. Gemini. URL: https://www.gemini.com/cryptopedia/blockchain-consensus-mechanism-types-of-algorithm. Accessed: 17.11.2024

CryptoQuant (2024). 3 Key Indicators. URL: https://userguide.cryptoquant.com/quickstart/5-minute-data-guide/3-key-indicators. Accessed: 08.01.2025

CryptoQuant (2024). CryptoQuant User Guide: 3 Key Indicators. URL: https://userguide.cryptoquant.com/quickstart/5-minute-data-guide/3-key-indicators. Accessed: 14.12.2024

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the Economic Institutions of Capitalism. Journal of Institutional Economics. Accessed: 12.11.2024

Digiconomist (2021). Bitcoin energy consumption index. URL: https://digiconomist.net/bitcoin-energy-consumption. Accessed: 15.11.2024

Ethereum (2015). Proof-of-Stake (POS). URL: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Accessed: 16.11.2024

Glassnode (2024). URL: https://glassnode.com/. Accessed: 9.12.2024

Gomez, A. (2024). The role of crypto wallets in managing your digital assets. LinkedIn. URL: https://www.linkedin.com/pulse/role-crypto-wallets-managing-your-digital-assets-andre-gomez-gawmf. Accessed: 19.11.2024

Helius (2025). Helius Webhook Settings. URL: https://dashboard.helius.dev. Accessed: 19.01.2025

Investopedia (2024). Four Scandalous Insider Trading Incidents. URL: https://www.investopedia.com/articles/stocks/09/insider-trading.asp. Accessed: 22.11.2024

Investopedia (2024). Stealth Address (Cryptocurrency): Meaning and Concerns. URL: https://www.investopedia.com/terms/s/stealth-address-cryptocurrency.asp. Accessed: 2.12.2024

Kejriwal, S. (2024). Arkham Intelligence review 2024: Revolutionizing crypto analytics. Coinbureau. URL: https://coinbureau.com/review/arkham-intelligence-review/. Accessed: 9.12.2024

Makori, J. (2023). What is onchain analysis and 3 tools to visualize onchain Data. Coingecko. URL: What is Onchain Analysis, and How Do You Use It? | CoinGecko. Accessed: 22.11.2024

McCaffrey, J. (2019). Blockchain Fundamentals: Diving into Transaction Hash Chains. Microsoft. URL: https://learn.microsoft.com/en-us/archive/msdn-magazine/2018/august/blockchain-blockchain-fundamentals-diving-into-transaction-hash-chains. Accessed: 25.11.2024

MDN Web Docs (2024). What is Javascript. URL: https://developer.mozilla.org/en-US/docs/Learn_web_development/Core/Scripting/What_is_JavaScript. Accessed: 10.01.2025

Miłosierny, M. (2023). Finance Bridge: Edition #5. Glassnode. URL: https://insights.glassnode.com/finance-bridge-edition-5/. Accessed: 14.12.2024

Nakamoto, S. (2008). Bitcoin: a Peer-to-Peer Electronic Cash System. URL: https://bitcoin.org/bitcoin.pdf. Accessed: 12.11.2024

Nansen (2024). What Is Onchain Analysis, And Why Is It Useful For Crypto Traders, URL: https://www.nansen.ai/guides/what-is-on-chain-analysis-and-why-is-it-useful-for-crypto-traders. Accessed: 2.12.2024

Personal Screenshot (2025). Telegram. Telegram Bot Token Creation. Accessed: 14.01.2025

Personal Screenshot (2025). Telegram. Transaction Notification to Telegram. Accessed: 21.01.2025

Phillips, D. (2021). Lost Bitcoin: 3.7 million Bitcoin are probably gone forever. Decrypt. URL: https://decrypt.co/37171/lost-bitcoin-3-7-million-bitcoin-are-probably-gone-forever. Accessed: 19.11.2024

River Financial Inc (2024). What is Bitcoin mining. URL: https://river.com/learn/what-is-bitcoin-mining/. Accessed: 23.11.2024

Schultze-Kraft, R. (2019). Dissecting Bitcoin's Unrealised On–Chain Profit/Loss. Glassnode. URL: https://medium.com/glassnode-insights/dissecting-bitcoins-unrealised-on-chain-profit-loss-73e735020c8d. Accessed: 17.12.2024

Sergey, O. (2022). 9 Best Programming Languages for Blockchain Development. Blaize. URL: https://blaize.tech/blog/5-best-programming-languages-for-blockchain-development/. Accessed: 10.01.2025

Solana (2025). Solana's homepage. URL: https://solana.com/. Accessed: 03.01.2025 Solscan (2024). Top 10 holders of Jupiter token. Solana Blockchain. URL: https://solscan.io/token/JUPyiwrYJFskUPiHa7hkeR8VUtAeFoSYbKedZNsDvCN#holders. Accessed: 4.12.2024

Song, J., Li, W., & Wei, D. (2023). Blockchain Data Analysis from the Perspective of Complex Networks: Overview. Tsinghua Science & Technology. Accessed: 13.11.2024

Statistics Finland (2021). Decrease in heating consumption covered the effect of remote work on energy consumption in households in 2020. URL: https://stat.fi/til/asen/2020/asen_2020_2021-12-16_tie_001_en.html. Accessed: 15.11.2024

Stevens, R. (2023). What is Dune Analytics and how does it work. Coindesk. URL: https://www.coindesk.com/learn/what-is-dune-analytics-and-how-does-it-work. Accessed: 9.12.2024

Svix (2025). Webhook vs Callback: What's the difference. URL: https://www.svix.com/resources/faq/webhook-vs-callback/. Accessed: 10.02.2025

Szabo, N. (2018). Smart Contracts: Building Blocks for Digital Markets. URL: https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf. Accessed: 20.11.2024

Valente, M. (2019). What is proof of authority. Coinhouse. URL: https://www.coinhouse.com/insights/what-is-proof-of-authority. Accessed 16.11.2024

Venter, O. (2024). Helius. Solana Dev 101: How to set up a Telegram bot to track onchain events. URL: https://www.helius.dev/blog/solana-telegram-bot. Accessed: 14.01.2025

Wright, E. (2024). What are inflows and outflows on crypto exchanges. Cointelegraph. URL: https://cointelegraph.com/explained/what-are-inflows-and-outflows-on-crypto-exchanges. Accessed: 6.12.2024