Digital Assets Internal Guide

An organizational structure document. To coordinate large numbers of workload more efficiently and avoid chaos. Detailed program development guide for the brave successor.

Authored and maintained by Norma Escobar

Table of Contents

Work Specialization

Verification of transactions

- Ensure all transactions have been settled on the blockchain.
- Match data record provided by client focusing on the date, transaction hash, amount, asset type and destination address.
- Determine the status of the transaction as verified or null.

Sent/Received dashboard

- Organize data clumps in an accountant-friendly manner.
- Label transactions as incoming or outgoing.

Daily prices and historical data

- Get the closing price of major assets in any time frame.

Transaction Rollback

- Determine the balance of any wallet address at year-end (or any date).
- Perform any tasks related to ownership ceremonies, such as ownership ceremony rollbacks.

Unrealized gains/losses

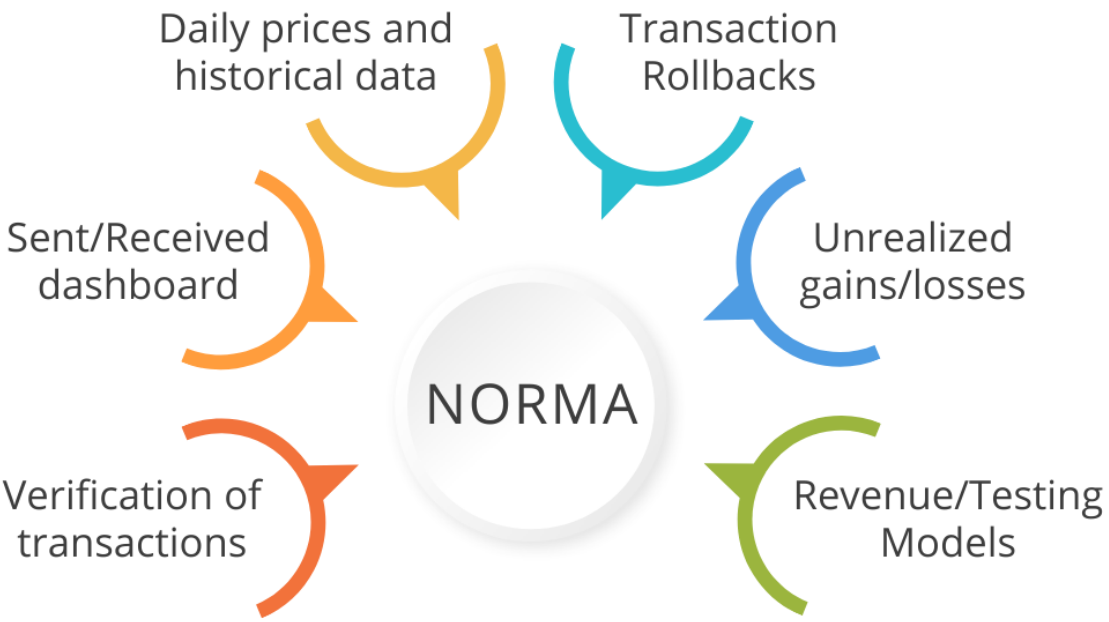
- Provide the closest P/L estimate *per transaction* for every major asset, and inevitably, get the closest estimate of the wallet address P/L.

Revenue/Testing models

- Test revenue correctness by creating calculators.
- Test mining revenue by creating maximum output models dependent on network hash rate, hardware and block rewards.

Excel, AutoHotkey and Power Automate

- Provide assistance with any tool in the MS Office Suite, but more related to automating workloads and other repetitive tasks, such as web scraping.

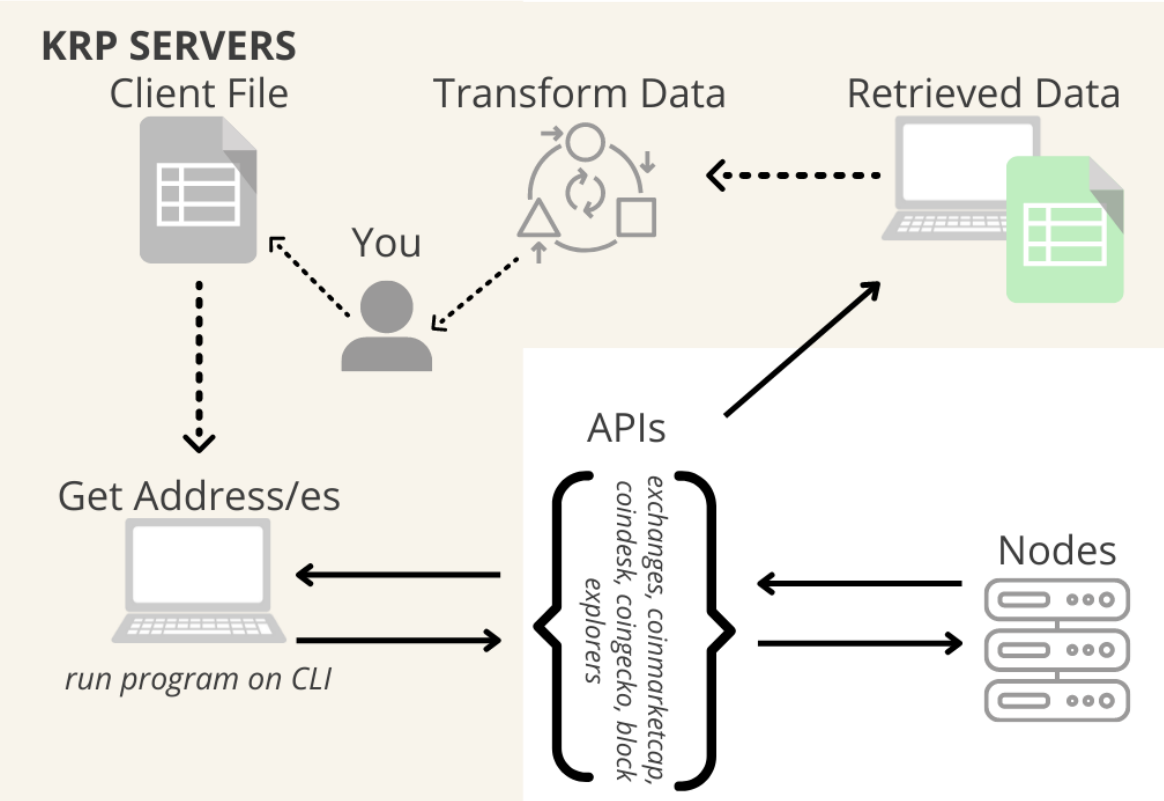


Documentation

Ultimately, all duties and responsibilities regarding digital assets *(for on-chain work)* can be encapsulated under 3 major categories:

1. Software Development
2. Client Files
3. Assurance Controls

Software Development



- Development, from scratch, of a reliable internal program that can fetch values from nodes directly via APIs, is necessary for smooth data extraction to work on client data.
- Perform routine code reviews to ensure the program is running bug-free and at its best functionality.
- Add/remove functions according to the needs of the firm.
- Keep up to date with the latest upgrades and technologies in the space.
- Meet with other software companies to find the best fit for each scenario.
- Note: the program is compliant with our existing security protocols, meaning no client file ever leaves our KRP servers.

Client Files

- Verification of transactions
- Sent/Received dashboards
- Daily prices and historical data
- Transaction rollback
- Unrealized gains or losses
- Revenue/testing models

Assurance Controls

- Act as the first point of contact for any technical questions related to the digital assets industry.
- Act as a second layer of confirmation for
    - Wallet balances
    - Proof of funds
    - Verification of funds
    - Tokens labelled as scams
    - APY
- Perform routine controls on our code base to add or remove features YOU desire.
- Ensure that all programs developed internally are up to the industry standard and expectations.
- Whitepapers analysis.

Formalization

The following contains a guide to organizing client data for verification of transactions on the blockchain, a list of the resources used during the verification process and an appendix. This guide should be considered the standard for on-chain work.

1. Organizing client data
2. Block Explorers
3. Mining
4. Introduction to openbtc for excel
5. Common misunderstandings
6. Appendix

Organizing client data

Most of the time our clients will give us a chunk of data in a CSV file. While the data looks intimidating, there are only a few columns that will grant us sufficient information to verify the transactions on the blockchain.

Date	**Transaction Hash**	**Transaction Value**	**Asset**	**Destination Address**

After the 2.0. version update of openbtc for excel, we no longer rely solely on the data provided by our clients. We are able to extract those values from a single input: wallet address/es.

Moving forward, all I will require from you is the list of address/es.

Block Explorers

Each network has its own set of tools used for blockchain exploration. Since cryptocurrencies are open-source projects, most of the tools out there are free and used by accountants and developers all over the world.

Asset/s or Networks	Block Explorer
Bitcoin	https://oxt.me/
Bitcoin, Ethereum, Bitcoin Cash	https://www.blockchain.com/explorer
Bitcoin, Smart Contract Platforms	https://explorer.bitquery.io/
Ethereum, ERC-20, ERC-721, ERC-1155	https://etherscan.io/
Polygon	https://polygonscan.com/
Litecoin	https://litecoinblockexplorer.net/
Ripple	https://xrpscan.com/
Stellar	https://stellarchain.io/
Cosmos	https://atomscan.com/
Binance Smart Chain	https://bscscan.com/
Monero	https://localmonero.co/blocks
Avalanche	https://explorer.avax.network/

It is preferred to use the native block explorers for each asset. Sometimes the same address can be used for different networks, and using the native block explorer reduces that risk.

Mining

The strategy to test revenue is almost identical for all proof-of-work networks. There are three components that will determine the profitability of operations:

1. Hardware capacity
2. Client's network hash rate share
3. Operational expenses (such as electricity and mining fees).

Hardware Capacity

Since mining is a highly monopolized field, most likely the mining equipment is being made by the same companies. All we are concerned with is determining 3 specific characteristics of any mining equipment:

01. Hash rate Capacity
02. Power Consumption
03. Mining Algorithm

The hardware specifications are easy to gather. On your web browser type "*equipment model in question + specs*".

Client's network hash rate share

The formula to calculate our client's percentage of the total network hash rate that their miner represents is the following:

Client's hash rate share = equipment hash rate/ daily network hash rate

Now, we have to determine the total daily block reward. So for example, a Bitcoin block is mined every 10 minutes or so.

*Daily block reward = Mining reward * blocks per day*

Finally, we have to determine the amounts of coins we will get according to our mining capacity:

*Client's daily coins = total daily block reward * client's hash rate share*

Mining Algorithm

The mining algorithm will determine the asset being mined. For example, if our client mines using NVIDIA GPUs, we automatically know they are not mining for Bitcoin. Maybe back in the early years, when Bitcoin mining wasn't as competitive, however, now it would be virtually impossible to compete against ASIC miners.

Introduction to Open Bitcoin for Excel

Formerly known as auditcoin.

Open Bitcoin for Excel *("openbtc" for short)* is an open-source Python program that provides detailed wallet information about prices, transactions, and blockchain confirmations more directly into excel. It was born from a lack of existing libraries.

Openbtc is compatible with all major assets including, but not limited to, Bitcoin, Ethereum, Polkadot, Stellar, Monero, Litecoin, Cardano and Ripple.

Understand that there is a world of existing software products designed for cryptocurrency accounting. However, openbtc is the only program created specifically for our needs. That is, handling volumes of 1,000,000 plus transactions, sent/received view mode, individual verification of each transaction, decoupling of smart contracts and historical data that seamlessly integrate with excel.

The development of the program started in February 2022 and it continues to be updated and maintained by Norma Escobar.

Common Misunderstandings

The name “cryptocurrencies” is very misleading because not all cryptos were created to act as currencies. As a matter a fact, most cryptocurrencies out there were created for other purposes unrelated to money payments and currency. Bitcoin’s whitepaper explicitly states that it was created under the idea of becoming a global payment network.

Ethereum, for example, was created to become a super-powerful decentralized computer that gives life to decentralized applications (also known as DApps). Ether is the currency needed to pay for computing power and the more people use the Ethereum Virtual Machine, the more demand there is for Ether, hence the growth in price.

Understanding this is crucial in order to recognize wallet activity trends and behaviour patterns. For example, if our client holds a significant amount of ATOM and does not sell it, does this mean they haven’t profited? Absolutely not. ATOM, like many other coins, is a proof of stake. Meaning that by simply staking the coins, a client can generate anywhere between 5-20% yield.

The yield is significantly higher for clients participating in liquidity farms, whose sole purpose is to generate profits by the tokens received as part of their reward for having a stake in the pool. At first, it can be intimidating to recognize patterns, but it does get easier the more you learn about the different cryptocurrency projects out there.

A good understanding of our client’s business model, and the crypto project they are invested in, will give you a great notion as to how exactly they make money. This is very helpful to determine how revenue can be tested. I wish there was a single strategy that could give us a conclusive revenue test, however, due to the nature of cryptocurrencies and the projects behind them, each client will most likely require a different auditing strategy.

Appendix

API - Application Programming Interface. In the context of APIs, the word Application refers to any software with a distinct function. Interface can be thought of as a contract of service between two applications. This contract defines how the two communicate with each other using requests and responses.

APY - Annual Percentage Yield, is the rate you can earn on an account over a year and it includes compound interest.

ASIC miners - An application-specific integrated circuit (ASIC) miner is a computerized device or hardware that uses ASICs for the sole purpose of mining bitcoin or another cryptocurrency.

Asset - in this context, it is a coin or a token.

AutoHotkey - a free and open-source custom scripting language for Microsoft Windows, initially aimed at providing easy keyboard shortcuts or hotkeys, fast macro-creation and software automation that allows users of most levels of computer skill to automate repetitive tasks in any Windows application.

Bitcoin - a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network. Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.

Block explorer - an online tool that enables you to search for real-time and historical information about a blockchain, including data related to blocks, transactions, addresses, and more.

Block rewards - the number of coins you get if you successfully mine a block of the currency.

Blockchain - a distributed ledger technology in which a record of transactions made in bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network.

Blockchain exploration - the act of exploring the blockchain for patterns and confirmations.

Calculators - in this context, to create models based on specific inputs to calculate the veracity of existing outputs.

Closing price - the last recorded price of an asset, regardless of whether the cryptocurrency market is open 24/7.

Code reviews - a software quality assurance activity in which one or several people check a program mainly by viewing and reading parts of its source code. At least one of the persons must not be the code's author.

Cryptocurrencies - a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

Destination address - the address receiving the coins or tokens transferred.

Documentation - grouping specialists based on their job descriptions, talents, locations, or other connections is the act of documentation.

Ethereum - a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Its native currency is Ether.

Formalization - defines how uniformly standardized company procedures, rules, and job descriptions are. It may control how managers and employees interact, as well as workplace culture and operating procedures.

Functions - a block of organized, reusable code that is used to perform a single, related action.

Hardware - the machines, wiring, and other physical components of a computer or other electronic system.

Hash rate capacity - a measure of how many calculations can be performed per second and can be measured in billions, trillions, quadrillions, and quintillions. For example, a hash rate of 1TH/s means one trillion calculations can be performed every second.

Incoming - in this context, a transaction received by the client.

KRP servers - internal computers that contain all the data used in the firm.

Liquidity farms - also known as liquidity pool that powers a marketplace where anyone can lend or borrow tokens. The usage of these marketplace incurs fees from the users, and the fees are used to pay liquidity providers for staking their own tokens in the pool.

Major assets - Bitcoin, Ether, AVAX, Matic, Cosmos, Lumens, Monero, Litecoin, ADA, XRP, SOL, DOT.

Mining - The competitive process that verifies and adds new transactions to the blockchain for a cryptocurrency that uses the proof-of-work (PoW) method.

mining algorithm - the algorithms in charge of making possible cryptocurrency mining. Normally these algorithms are cryptographic hash functions very complex and they can adjust the mining difficulty.

mining revenue - revenue derived from mining activities.

Monero - the largest private coin by market capitalization that uses proof-of-work to maintain network security. Monero's privacy algorithms make it impossible to trace addresses or funds.

Native block explorer - a tool created by the development team of a specific asset used to perform blockchain explorations related to that specific asset.

Network - in this context, also interchangeable with blockchain.

Network hash rate - the total computational power being used by a proof-of-work cryptocurrency network to process transactions. A high hash rate is an indicator of a network's security because it shows a large number of miners are verifying transactions.

Node - a computer that connects to a cryptocurrency network. The node or computer supports the network. It supports it through validation and relaying transactions. At the same time, it also gets a copy of the full blockchain.

Null - in this context, a transaction that has zero confirmations on the blockchain.

NVIDIA GPU - Graphics processing unit, a specialized processor originally designed to accelerate graphics rendering or mining. In this case, NVIDIA is one of the largest GPU providers in the world.

On-chain - any activity happening on the blockchain.

Open Bitcoin for Excel - An open-source python program that provides detailed wallet information about prices, transactions, and blockchain confirmations more directly into excel. It was born from a lack of existing libraries.

Open-source - denoting software for which the original source code is made freely available and may be redistributed and modified.
Outgoing - in this context, a transaction sent by the client.

Ownership ceremonies - a meeting in which the client provides proof of funds by transferring at least 85% of a wallet's assets into another.

P/L - referred to as profit or loss on investment.

Power Automate - a service that helps you create automated workflows between your favourite apps and services to synchronize files, get notifications, collect data, and more.

Power consumption - in this context, the amount of energy used per miner expressed in kWh.

Proof-of-stake - the consensus mechanism in which all network validators agree to "stake" or lock their funds in order to verify transactions and maintain network security. Seen a greener alternative than proof-of-work.

Proof-of-work - is a form of cryptographic proof in which one party proves to others that a certain amount of a specific computational effort has been expended. This is the only consensus protocol in the world that respects the laws of conservation of energy.

Python - a high-level general-purpose programming language.

smart contract platforms - a network or blockchain that supports smart contracts.

smart contracts - a computer program or a transaction protocol which is intended to automatically execute, control or document legally relevant events and actions according to the terms of a contract or an agreement.

Staking - a process that involves committing your crypto assets to support a blockchain network and confirm transactions.

transaction hash - a unique string of characters that is given to every transaction that is verified and added to the blockchain.

transaction value - in this context, the amount of the asset transacted. Not to be confused with its USD/CAD value.

Verified - in this context, a transaction that has been confirmed on the blockchain.

Wallet - a device, physical medium, program or service which stores the public and/or private keys for cryptocurrency transactions. Remember, a wallet does NOT hold funds, but rather contains the address/es that contains funds.

Wallet address - a string of letters and numbers from which cryptocurrencies or NFTs can be sent to and from.

Web scraping - data scraping used for extracting data from websites.

Whitepaper - a report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

Work specialization - how duties are distributed among employees in accordance with job descriptions. It is used to divide projects into more manageable work activities and provide each employee with manageable duties. Low efficiency and burnout are the most frequent effects of improper specialization.