The Industry Standardization and adoption of Cryptocurrency

As the cryptocurrency market continues to grow significantly as the leading disruptor in the world of finance, a large ecosystem of competitive cryptocurrency solutions have developed to accommodate the new digital asset class to fit within regulatory standards.
“Central bank digital currency is coming alive”

Christine Lagarde, former head of the IMF, current president of the European Central Bank. (In a 2019 interview about digital currency disruption)
The Problems

Over $219 billion dollars worth of digital assets guarded by nothing but cryptography circulates the global market today.

The worldwide consensus towards the legal classification of cryptocurrency as an asset or property has paved the way for global competition to flourish in the development of solutions that are universal and borderless. Since the inception of Bitcoin in 2009, the utility of cryptocurrency has evolved well past having only the purpose of an electronic means of exchange like originally intended. The technology unintentionally evolved to providing far more utility like smart contract application, data verification and transparency, and non-fungibility of digitized goods. Now in order for all of these innovations to take place, tracking and accurate audit reports must be able to take place through the blockchain. The secondary industry created to support the primary cryptocurrency industry is composed of 3rd party services and technologies designed to accommodate products built using blockchain. These products can be anything from coins/tokens to platforms built under a blockchain network. These projects rely on 3rd party services and technologies for various necessities such as auditing through their respective blockchain networks, calculating cryptocurrency taxes, and accounting transactions in compliance with regulatory standards.

The difficulty and risk in using 3rd party services in a rapidly developing industry is due to trust and reliability. Due to the nature of the cryptocurrency market volatility, many projects have come and gone along with their intended secondary market providers. For example in both a high volume and low volume market, cryptocurrency exchanges need reliable 3rd party partners not just to improve internal operations but also to support the lifeline of the exchange itself. One example of a 3rd party service many exchanges use is cold-storage solutions or protected custody services. Since these services do not necessarily serve the business model of the exchange, the exchange would much rather rely on 3rd party providers as this would be a lower cost than taking full responsibility internally.

Traditional spreadsheet software like Excel or Google Sheets are not optimized or even practical for cryptocurrency accounting or tracking due to the sheer volume of cryptocurrency trades that take place along with the huge variety of available digital assets in the market. Most accountants have very little to no experience in handling clients with digital assets. For this reason, not only is there the challenge of finding the best tools for cryptocurrency accounting but also finding industry professionals capable of providing help. For this reason, industry professionals like CPAs will be more able to quickly accomodate for the new asset class by using the right software and tools that provide the proper guidance. In this case study, we will highlight three main pain-points faced by over ten of our high-profile clients in the cryptocurrency landscape today.
TRACKING

How do you manage multiple data sources in a diverse digital economy?

Cryptocurrency tracking has its own set of challenges. There are different blockchains to track from that don’t communicate. For example, tracking Bitcoin and Ethereum use their own native blockchain with each their own trackable digital asset. Distributed ledger technology has its limitations, these limitations are determined by the rules set in code for how the blockchain operates. When it comes to balance tracking, all that is needed is a public wallet address for digital assets like Bitcoin, Ethereum, and Litecoin however some require more parameters to be met for sending and receiving digital assets. With all these different parameters and differentiation towards the process of transacting digital assets, creating tracking software that is universally compatible with nearly every blockchain network is nearly an impossible task. The difficulty of universal compatibility is precisely why many projects have become specialized and very niche in the cryptocurrency industry. There is reasonable risk in relying on third party information providers for the accuracy of data pulled from the blockchain. While popular blockchain scanning services exist for the community like Blockexplorer for Bitcoin and Etherscan for Ethereum, data pulled from these websites are falsely assumed to provide 100% accurate information from the blockchain while also being a potential point of failure if something were to go wrong from their end.

It is far safer and reliable to run a full node in-house for the desired blockchain data audits, reports, and for maintaining privacy. Not every cryptocurrency is a hardfork of Bitcoin. In recent years with great improvements to smart contract deployments and the standardization of the technology, more tokens are now created under smart contract friendly application-based blockchains like Ethereum and NEO. Ethereum standardized their token protocol through ERC-20 and NEO with NEP-5. With many different tokens created under these blockchain networks the complexity of tracking tokens multiplies. There is also the question of how to improve token tracking for not only mainnet tokens but testnet tokens as well. Public wallet addresses don’t function all in the same way either. Depending on the blockchain network, alphanumeric characters may be generated with different algorithms or have different character limits, and different addresses. There are further wallet address complications for example when networks go through softworks like segwit and multisig altering the functionality and overall user-experience of the blockchain in question.

There are over 5000 cryptocurrencies and 20,000 markets operating under different protocols
The challenges around cryptocurrency accounting as mentioned earlier still hold true to this very day. Although there are many different accounting solutions in the market for organizations to choose from, unfortunately due to significant regulatory differences in accounting procedures and compliance there is no accounting platform certified in every jurisdiction. Many countries have taken their own approach in classifying cryptocurrency legally, most as an asset or property. This classification directly affects the accounting method of cryptocurrency. For example, an asset or property is calculated for capital gains or losses in a tax declaration. Another significant challenge for individuals and organizations in the need of a cryptocurrency accounting solution is how sensitive data is handled by the existing new solutions in the market. If an organization is entrusting a third party accounting platform with all of their digital asset balance and transaction data, an information leak could greatly benefit a potential attacker. Entrusting 3rd party providers like block explorers cannot generate consistent audit reports since they may often not reach consensus. One block explorer may generate completely different results when pulling data from a transaction ID or wallet balance and transaction history. This could be for example a discrepancy in the number of transactions or different wallet balances.
CUSTODY & STORAGE

$1.7 billion worth of cryptocurrencies from investors last year, according to a report from CipherTrace - Cryptocurrency Intelligence

Storing cryptocurrency is a complicated procedure to everyone due to its intangible, unseen and technical nature. In fact it is so complicated that certain institutions have declined to offer cryptocurrency storage solutions. Complications around cryptocurrency custody is one of the few problems that plague the market today. The access of a cryptocurrency wallet comes down to a single entity - the private key - which creates a single point of failure. The keys can be stored in a hot storage wallet (online storage) or cold storage wallet (offline storage). During the past few years, there have been numerous hacks and thefts on private keys stored in hot storages. Storing cryptocurrencies offline is comparatively safer than hot storages and many experts have therefore recommended this mode of storage.

The cold storages move the private key into the physical realm of existence. The keys would be stored in a small thumb size device which is capable of storing various cryptocurrencies without a limitation of volume. This means the device can be subject to theft only like how gems and cash can be stolen from a place of storage. However, unlike gems and cash, the stolen storage device will not give access to the cryptocurrency but can be held for ransom by the thief. The storage devices can also be vulnerable to physical damage.

There are various implementations to such as Multisig to mitigate cryptocurrency wallet private key vulnerabilities. Multisig stands for multi-signature, which is a specific type of digital signature that makes it possible for two or more users to use a wallet as a group. Multisig technology has been extant within the world of cryptocurrencies, but the principle is one that existed long before the creation of Bitcoin. Yet the vulnerabilities exist making certain areas of the process a target for hackers.
The Solutions

Streamlining efficiencies for the cryptocurrencies and blockchain finance.

TRACKING

For decentralized finance to become a reality, financial resources and tools must be available at the P2P level and thus unrestricted to any user. Individuals and organizations can track their digital assets without ever jeopardizing their digital assets if using only a public wallet address or read-only API in the case of exchange connections. Back to the challenge of cryptocurrency tracking, which was finding the capable and reliable platform to utilize for the specific asset tracking purpose but as well as entrusting the 3rd party platform with sensitive data. At Cryptoworth, our platform along with partnered data providers with enterprise grade SLAs guarantees accurate data pulled directly through our supported blockchain networks such as Bitcoin and Ethereum in a secure way through the practice of running our own nodes. Our solutions include exchange/DEX tracking, ERC20/ERC223/NEP5/private token tracking, asset fair market value calculations through various exchange order book snapshots and using weighted daily average and several other techniques to determine the price of a cryptocurrency at any given point. Our deployment strategies provide organizations full ownership of their client data and enable privacy preservation to its maximum level.

Our platforms and its eco-system of integrations were created in a way to standardize the quality of expectations within the industry. To do this, we integrated the most popular exchanges and wallets along with full support of the largest cryptocurrencies in the market. Cryptoworth’s work on integrations are committed to serving the needs of exchanges, portfolio managers and technology providers. We help monitor assets and strengthen workflows through data visualization. Our teams empower clients by developing sophisticated user-friendly tools.

Transform your business and drive more insights

coinbase Pro
BINANCE
BITFINEX
Huobi Global
coinbase
BitMEX
coinsquare
ACCOUNTING & AUDITING

The problem comes down to managing multiple end-points in a diverse digital economy. How do you consolidate balances and transactions consisting of over 5000 digital assets and hundreds of exchanges operating under different protocols, jurisdictions, and technology?

Cryptocurrency accounting and auditing solutions are rapidly standardizing to comply with regulatory framework and strict industry standards. Accounting with cryptocurrency cannot be compared effectively with any other asset class. This is due to the complexity of variables that affect how cryptocurrency as an asset is taxed. There are occurrences in the cryptocurrency space that don’t exist in other asset classes, like hardforks. In the event of a hardfork, individuals holding a certain cryptocurrency, may receive more digital assets through an airdrop. These events are taxable events regardless of whether or not the balance holder was aware of the airdrop. These events cannot be missed when creating tax reports.

Cryptoworth’s sophisticated and CPA-reviewed accounting platform accounts for new assets generated under the synchronized wallets provided by the user. Cryptoworth is multi-digital asset compatible, this means we pull data from multiple blockchains and exchanges at all times to gather necessary data. The Cryptoworth accounting platform adheres to industry and government standards through our cost base analysis accounting principles, supporting cost-basis, FIFO and LIFO. Auditing through our platform is made possible by the complex technical infrastructure we have in place to connect many blockchain networks into an oracle-like environment maintained by Cryptoworth. Our system detects soft-forks that alter the supported blockchain networks through our managed nodes.

Any protocol changes that occur are immediately adapted into our systems to maintain a seamless consistent string of network upgrades that do not affect the standardized accounting or auditing procedures. We have the knowledge and expertise to make this essential business process smooth, cost-effective and personalized for your operations. Our clients also benefit from our software knowledge combined with our accounting solutions. We reduce the burden of cryptocurrency endpoint integrations for our customers so you can focus on growing your business. Tailored and quality bookkeeping and accounting solutions are overseen by our CPA partners, lawyers and engineers to create a seamless and accurate system.
Cryptoworth’s custody solutions take strong precautions and procedures when it comes to building infrastructure for storing and custody of cryptocurrency assets. Cryptoworth constantly evolves on cold storage and deep cold storage solutions and its landscape. Cryptoworth works with companies that provide custody services and build solutions by partnering up with other security companies. The solutions are tailor-made for each customer as we believe that each customer is unique and has their own unique requirements.

Cryptoworth combines multi-factor authentication with multipart user access schemes to design custodian infrastructure to ensure that no single person - even from the custodian company can move the assets under custody (AUC) and assets under administration (AUA). Cryptoworth builds tiered access control structures, security assessment frameworks and insurance infrastructure for the AUC. The hardware vendors for cold storages, air-gapped computers are distributed across the market to ensure diverse organization dependency which further helps to mitigate the overall risks. All custody solutions are ensured to have military-grade security and Cryptoworth helps you to get high level FIPS 140-2 rating for our solutions and infrastructure we provide.

Cryptoworth’s latest thinking involves keyless wallets that uses threshold cryptography on the elliptic curve digital signature algorithm (ECDSA) to distribute the signatorial responsibilities among multiple sets of entities. Keyless wallets rely on multi-part computing (MPC) cryptography. This approach uses multiple non-trusting parties to conduct a computation on their own unique fragment of a larger data set. In other words, instead of using a single atomic private key for transaction signing, the responsibility is divided among multiple parties. The keys for these parties are generated in their own devices using distributed key generation protocols and the key never leaves the device. That key is used to sign the transaction without revealing the secret key to the other parties involved. At Cryptoworth we see a huge potential to use keyless schemes as it eliminates the single point of failure of a private key.
About Cryptoworth

Founded in 2017, Cryptoworth is a cryptocurrency solutions and consultancy company working hard at the intersection of cryptocurrencies, blockchains, business and people to better-serve the fintech industry. Cryptoworth was created to reduce the complexity of cryptocurrency adoption, usage, and management. Cryptoworth provides the best cryptocurrency and blockchain solutions for use cases spanning from single users to large institutions. We are a team who strongly believes in the cryptocurrency-oriented future for the financial world and we look forward to expand our ventures and services in multiple areas.

Visit: https://cryptoworth.app

Toronto
1 Yonge Street, Suite 1801
Toronto, ON, M5E 1W7
Canada

Montreal
1250 Guy St Suite #600,
Montreal, QC, H3H 2L3
Canada

No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cryptoworth. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.
"With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless."

- Satoshi Nakomoto, founder of Bitcoin