A Brief Primer on Cryptocurrencies and Keys: How Evolving Payment Trends Influence the Management of Cryptocurrencies in Business

By Eric E. Cohen, CPA

Eric is a prolific author, engaged in virtually every effort to standardize accounting and audit data, a national expert on a wide variety of standards efforts, and co-founder of XBRL.

He is a contributing editor to *ThinkTWENTY20*.

As more and more organizations are accepting cryptocurrencies[1] for payment, or investing in cryptocurrencies as part of their treasury function, the issues of both how to acquire and how to manage these assets become more important for financial professionals to understand.

While most organizations are still trying to adapt to the long-standing but challenging world of login names and passwords for security and access, cryptocurrencies exacerbate the issue with new mechanisms and a new vocabulary, largely surrounding the use of private and public keys. In this article, we will examine cryptocurrency management, focusing on this new vocabulary and techniques related to the new issues of key management. For financial professionals with responsibilities for oversight over an enterprise's assets, the article may help with issues related to risks, controls and management. For auditors, it may provide useful background for understanding the new corporate environment and for the development of relevant audit procedures.

A Brief History of Payments and Authentication

Over the last 40 years, the methods businesses use to send and receive payments, as well as how they manage their investments, has changed markedly. As the PC revolution began 40 years ago, through the ages of the Internet and now into blockchain, we have gone from mail and phone to online services, to the new world of cryptocurrencies and to investments with decentralized finance (DeFi).

While most organizations are still trying to adapt to the long-standing but challenging world of login names and passwords for security and access, cryptocurrencies exacerbate the issue with new mechanisms and a new vocabulary.

Forty years ago (1981), as the PC (personal computer) era began, those computers did not yet do much talking to each other. While the IBM PC and the Compaq portable, and their clones and competitors, starting showing up in offices and for the mobile warrior, neither local area networks nor telephonic connections were common. The digital connection between trading partners, and between businesses and their financial institutions, had not begun in earnest.

The typical small business would primarily be dealing with three methods of payments: for business-to business activities, primarily cash and cheques/checks, the latter more prevalent for payment on account; for consumer-to-business activities, cash and credit cards were more the norm. There was no commercial Internet 40 years ago and only very limited online banking or brokerages. Cash, credit cards and cheques mechanisms each had their own risks; as someone who himself installed point-of-sale systems for clients, I had access to credit card information much like that we hear about in today's security breaches, but only because of direct access to the seller's computers, where the information was collected in batches and sent only on a periodic basis to the credit card processor.

Thirty years ago (1991), the (World Wide) Web era began. Although the interim period had heralded the rise of Electronic Data Interchange (EDI) and specialized online services, it was the new connected age where widespread use of online systems and, with it concern about controlled access to those online systems, began to rise. With that growth came the proliferation of login names and passwords, and we sit here – 30 years later – with few excellent answers to those legacy challenges. People have difficulty remembering login names and passwords; security experts recommend changing those passwords regularly as well as making them more complex, making it even more challenging to remember … or even type efficiently and accurately. Password managers, software and online systems that offer up the login information on demand, help but have their own problems.

Although two-factor authentication (TFA) devices – combining "who you are" (such as fingerprints or eye scanning) or "what you have" (such as a separate piece of equipment) to "what you know" (your login and password) – were widely available 20 years ago (in 2003 RSA SecurID,[2] as a "what you have" device, held 70% of the market as a hardware device to make logging into systems more secure), it has only been the recent highly publicized privacy breeches that have led more information environments to strongly encourage or require TFA. For example, I can access my email or systems for a University with which I am associated only with the use of one of my smart devices as an authenticator, using Microsoft Authenticator[3] for TFA. Cryptocurrency exchanges, such as Coinbase, highly recommend TFA; Coinbase supports Yubico's Yubikey.[4]

Twenty years ago, ACHs (automated clearing houses) started taking off, and business-to-business payments through an electronic funds transfer network took the paper (and the paper trail) out of payment transfers. ACH transfers do require sharing banking information with the payer, which may not be ideal. With that knowledge, however, ACH payments were fast and easy.

As ACHs were taking off, the Extensible Markup Language (XML) also began its ascent. Where HTML was characterized as “the web of information,” XML ushered in “the web of data.” In XML’s early maturation, the idea that we would be able to hook together our business systems, including payment processes, using XML Web Services[5] for a Service Oriented Architecture (SOA) held great potential. While you rarely hear about SOA anymore, Application Programming Interfaces (API)[6] and Representational State Transfer (REST) seem to have won the battle[7] for development mindset.

Ten years ago, electronic payment methods began to proliferate. Essentially tied to credit cards, the digital “wallets” (not to be confused with cryptocurrency wallets, as we will discuss) started showing up, joined with the inclusion of NFC (near field communication) technology in mobile phones: Visa,[8] Google,[9] Apple and many others[10] began offering mobile, or digital, wallets. The idea of a wallet as a place you kept your credit cards, and not necessarily your money, wasn’t so confusing then.

Thirty years ago, the new connected age – where widespread use of online systems and, with it, concern about controlled access to those online systems – began to rise.

Coincidentally, at the same time, the crypto era began. That crypto era was also marked by a different kind of digital wallets, but these manage something completely different than the Google and Apple wallets. These cryptocurrency wallets store information related to the private keys necessary to control the new assets.

More recently, related to payments and investments, decentralized finance has become the big deal – where terms like *staking*, *delegation*, *pooling* and other ways of earning “interest” or appreciation on cryptocurrencies without losing control of the cryptocurrencies has brought additional potential benefit to holding onto cryptocurrencies along with the hoped-for appreciation of the cryptocurrency itself.

Although Bitcoin, Ethereum and others of their ilk are still a mystery to many, the number of people “investing” in cryptocurrency is rising. A recent poll had it as 13% over the last year in the US[11]; in Canada, the numbers may be around half of that.[12] The crypto adoption numbers don't differentiate between how the cryptocurrencies are handled, and that's where the new vocabulary comes into play. The term wallet is thrown around even in this space to mean a true cryptoasset wallet managing keys, an account with a custodian where you see your holdings but do not have direct control, and other ways it may be different.

So, with that brief background on how payments have changed over 40 years, let's focus more specifically on our new world of things like Bitcoin and Ethereum, collectibles known as non-fungible tokens (NFTs) and other assets tracked on blockchains and the variations thereof.

A Brief Overview of How Cryptocurrencies Are Tracked by Keys

The original Bitcoin[13] whitepaper[14] introduced some terms not part of the average financial professional's vocabulary: in particular, *private key* and *public key* are introduced in the whitepaper as the "keys" (no pun intended) to the Bitcoin blockchain's design. (The Bitcoin blockchain[15] is the append-only database that tracks Bitcoin, using cryptographic means and methods to secure it.) Public Key Infrastructure (PKI) is not unique to cryptoassets and blockchain, although the application is. Those who have studied security may be aware of how a matching pair of codes, the private key and the public key, are used as part of encryption – sending secret messages, if you will. The private key is a unique code, meant to be kept private and used to authorize payment in the cryptocurrency world by digitally signing the information, while the public key … well, the public key is where it starts to get a little tricky. While generally, the public key is designed to be … well … public, the Bitcoin whitepaper recommends keeping the public key private as well[16].

The whitepaper does not speak to a Bitcoin *address* per se. The address is what we give out today to receive Bitcoin "into" our wallet or exchange instead of the public key. The whitepaper introduces the transactions only as "a chain of digital signatures." In fact, the Bitcoin whitepaper doesn't reference a wallet at all. The original Bitcoin client, however, had the ability to create wallets, the storehouse of the keys; that client was known as Bitcoin-Qt.[17] (Qt[18] refers to the software toolkit used to build the graphical user interface.) The whitepaper does, however, speak to the necessity of not only keeping the private key private, but also the benefit of keeping the <u>public</u> key private. To do so, in advance of Bitcoin's implementation, the developer community added the concept of a Bitcoin address.[19] A Bitcoin address is unambiguously derived from the public key, but it is almost impossible to calculate the public key from the address. Bitcoin addresses are usually 34 characters and currently start with the numbers 1 or 3 (legacy addresses) or bc1 (SegWit addresses). Some cryptocurrencies and tokens, such as Stellar, do not have the same "address as abstraction" and use the public key itself as the address.[20] Stellar does use the term address in a different way, which they call a “federated address”; this is an alias (a simpler phrase you can give out instead of the more complex public key) that you can provide as an easy shorthand.[21]

Although Bitcoin, Ethereum and others of their ilk are still a mystery to many, the number of people “investing” in cryptocurrency is rising.

Creating a private key usually begins with a “seed” to help generate random numbers; most financial professionals are somewhat comfortable with the concept of random numbers, especially used in audit sampling. When the seed is not random, it becomes simple to guess private keys of addresses with balances in them, as the key is derived from the seed by a consistent algorithm. For example, I can use a tool like BitAddress.org to help me generate a private key and a related address. Using the “Brain Wallet” option, I can type in a seed phrase to generate a private key, and then use a lookup tool such as Blockchain.com to see whether the related address has any Bitcoin in it. Typing the seed phrase “Satoshi Nakamoto” results in an address of 1JryTePceSiWVpoNBU8SbwiT7J4ghzijzW, and I can tell[22] that address has had transactions run through it in the past. An attacker can quickly run through seed phrases that might appeal to the Bitcoin crowd, automatically identify the private key and related Bitcoin addresses, identify if any have a balance. They then have all of the tools necessary to empty the balance.

Bringing this back to the concept of a wallet: a cryptocurrency wallet manages keys; it can create them, keep inventory of them, look up the related addresses and display balances of holdings, etc. But as a key is just a code, I can create a key without a wallet (as I did in the above example); I can export the keys from one wallet and import them into another wallet (concurrently). There are no balances or amounts unique to the wallet, which is likened to a window to the holdings on the blockchain; it just has the keys, which blockchains they apply to, and potentially some additional information necessary to identify specific tokens on the chain to which they relate.

Tracking Crypto “Beyond” the Keys

So, an organization tracking cryptocurrency holdings by using private keys (individually) or a key management tool like a wallet is one option for managing cryptocurrencies, and financial professionals have a new challenge of figuring out how to control this information. But self-managed (non-custodial) wallets are not the only way cryptocurrencies are managed.

Where the Bitcoin whitepaper spoke to peer-to-peer payments without the need for a single central intermediary, the advantages of having such an intermediary have countered the benefits of self-management of the cryptocurrencies. For those who wish to acquire cryptocurrencies without finding a peer who already holds it, or performing the *mining* activities to earn them, exchanges and other custodians have arisen. Organizations with names like the aforementioned Coinbase, Binance, Kraken and Gemini have arisen to facilitate the purchase and sale of cryptocurrencies.

These exchanges are used by many people to purchase, control and sell their cryptocurrencies. Often, people will say their account on these services is their wallet. But as Kraken notes, “Kraken is an exchange, not a wallet service. We provide clients the ability to deposit funds to our corporate wallet for safekeeping while the funds are being exchanged or used for trading or staking, but we do not provide a personal wallet service.”[23]

Unlike the wallets described above, the account holder does not have control of the funds through possession of the keys; they cannot look at the respective blockchains to see their holdings, as they are aggregated by the exchange; you have to look at your account with the exchange instead. You can, however, deposit selected cryptocurrencies into these accounts, and you can withdraw (transfer) cryptocurrencies from these services to true “personal” wallets or to send to others.

Probably one example of the real confusion in this space is with Coinbase (the exchange) and Coinbase Wallet (a true, non-custodial wallet, where the user holds the keys to the cryptocurrencies). Coinbase calls amounts held on its exchange (you have no access to the keys) a “hosted wallet.”[24] It then goes on to say the separate Coinbase Wallet is a “non-custodial” wallet. And to make things more confusing, the non-custodial wallet page[25] speaks about “stor[ing] all of your crypto and NFTs in one place” – when, in fact, the crypto and NFT are *not* stored in the application, only the keys that control them.

The AICPA’s guide *Accounting for and auditing of digital assets* has much to say about purchasing or receiving cryptocurrencies and how to recognize them for account.

But there is yet another way people are “purchasing” cryptocurrencies – through services like Robinhood or PayPal. They also may call it a cryptocurrency wallet,[26] but these accounts are quite different from the first two options. At the present time, these services do *not* permit deposits of cryptocurrencies or withdrawals of cryptocurrencies[27] at all – just buying with fiat, holding, and selling for fiat.

What Does This Mean for Enterprise Cryptocurrency Management?

The AICPA’s guide *Accounting for and auditing of digital assets*[28] has much to say about purchasing or receiving cryptocurrencies and how to recognize them for accounting purposes. They describe the situation of *recognition of digital assets when an entity uses a third-party hosted wallet service* as a special and somewhat complicated situation. From a security point of view, however, it is relatively simple: you have an account with a third party and the ability to communicate with that third party.

Third parties also come into play on the receiving side in the first place. Many businesses that have decided to “accept” cryptocurrencies for payment (for appearance’s sake) avoid the technical issues of controlling cryptocurrency as payments by using a third-party service that acts as an intermediary and hides the complexities through immediately turning any cryptocurrency into fiat currencies. For organizations that choose to actually receive and hold the cryptocurrencies for any amount of time, there are more issues to consider.

As mentioned, services like Robinhood or PayPal (under the conditions as this article is being written) do not permit cryptocurrency deposits, and so are not relevant to the management discussion for payments. For investments, these services offer reduced acquisition and liquidation costs (as crypto is not actually being procured), but have certain other concerns outside of the scope of this article.

The exchanges (such as Coinbase, the exchange) or other platforms (such as Coinbase Pro, a trading platform used for exchanging and selling cryptocurrencies, but perhaps less well suited for initial acquisition) can provide a cryptographic address for receiving cryptocurrencies from third parties, for example, for payments. As custodial accounts where the user does not control the keys, corporate control is more similar to traditional banking and investment accounts.

So, the greatest issue in these "simple" options for new consideration is that of non-custodial wallets, where access to the wallet(s) – or directly to the private keys generated by or managed by the wallets – means control of the assets under control by the wallets' private keys. On top of that, the keys can be exported and then imported into another wallet.

Most wallets are initiated with a random seed, from which many private key/public key pairs are created. That seed, a very big code, which is very difficult to memorize, can be represented with easier to represent words, so memorizing 12 or 24 words serves as a mnemonic for the long phrase. The mnemonic seed phrase, known as a BIP39 seed, if known by an employee, can easily be used to duplicate the content of a wallet.

In the COSO thought leadership paper, *Blockchain and Internal Controls: A COSO Perspective,*[29] guidance about "implementing appropriate segregation of duties between the ability to authorize blockchain transactions … and the ability to record transactions within the entity's general ledger," in particular "using multisignature or key sharding techniques" is offered as guidance. The paper notes, however, that, "Enterprise key management software is only beginning to emerge, as are key management guidelines" and references a National Institute of Standards and Technology (US NIST) project on Key Management guidelines.[30]

The Challenges of a Rapidly Changing Web of Value

We have seen payments and investments change markedly over the last 40 years. In the past 10 years, Bitcoin has been the catalyst for a new and rapidly changing *web of value*, where the challenges to financial professionals to understand and control the new cryptocurrency class of digital assets in a rapidly evolving world filled with terms that previously belonged to the IT (information technology) department, not the accounting department. Financial professionals should be working with management and IT to prepare a solid foundation for managing accounting, finance and treasury in the upcoming days.

[1] This article will use the term *cryptocurrencies* generically for digital assets such as coins, tokens, central bank digital currencies (CBDC) and those assets sometimes called digital assets or currencies, virtual currencies, cryptocurrencies or similar terms.

[2] https://www.rsa.com/content/dam/en/data-sheet/rsa-securid-hardware-tokens.pdf.

[3] https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-auth-app-overview See also Google Authenticator at https://www.google.com/landing/2step/.

[4] https://help.coinbase.com/en/coinbase/getting-started/getting-started-with-coinbase/2-factor-authentication-2fa-faq.

[5] https://www.w3.org/2002/ws/.

[6] https://blog.api.rakuten.net/evolution-of-apis/.

[7] https://www.w3.org/2005/Talks/1115-hh-k-ecows/#(7).

[8] https://www.wired.com/2011/05/visa-digital-wallet-nfc/.

[9] https://techcrunch.com/2011/05/26/google-wallet-offers/.

[10] https://blog.717cu.com/resources/education/financial-education-blog/the-history-of-digital-wallets.

[11] https://www.norc.org/NewsEventsPublications/PressReleases/Pages/more-than-one-in-ten-americans-surveyed-invest-in-cryptocurrencies.aspx.

[12] https://reviewlution.ca/resources/cryptocurrency-canada-statistics/.

[13] Although this article will be primarily using the term *Bitcoin* throughout, the basics are true for most other cryptoassets.

[14] https://bitcoin.org/bitcoin.pdf.

[15] From ISO 22739:2020: blockchain is a "distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links."

Note 1 to entry: Blockchains are designed to be tamper resistant and to create final, definitive and immutable (3.40) ledger records (3.44).

[16] From the Bitcoin whitepaper: "… privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous."

[17] https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/.

[18] https://www.qt.io/home.

[19] https://en.bitcoin.it/wiki/Invoice_address.

[20] See https://developers.stellar.org/docs/tutorials/create-account/ where they note "The public key is always safe to share."

[21] https://developers.stellar.org/docs/glossary/federation/.

[22] Seehttps://www.blockchain.com/btc/address/1JryTePceSiWVpoNBU8SbwiT7J4ghzijzW.

[23] https://support.kraken.com/hc/en-us/articles/115006441267-Differences-between-a-crypto-exchange-and-a-crypto-wallet-service.

[24] https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet.

[25] https://wallet.coinbase.com/.

[26] https://www.paypal.com/us/smarthelp/topic/MY_WALLET_PER.

[27] https://www.paypal.com/us/webapps/mpp/ua/cryptocurrencies-tnc.

[28] https://www.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/accounting-for-and-auditing-of-digital-assets.pdf.

[29] https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf.

[30] https://csrc.nist.gov/projects/key-management/key-management-guidelines.