Diving into the Fundamentals of Cryptocurrency as a Form of Digital Payment

©2024 Nacha. All rights reserved.

Diving into the Fundamentals of Cryptocurrency as a Form of Digital Payment

Introduction

The digital payment environment is complex and ever evolving. We likely hear terms such as digital assets, digital currency, blockchain, and distributed ledgers and struggle to make sense of all the noise. This briefing focuses on cryptocurrency—a type of digital asset—and addresses definitions, processing and roles of the participants.

Digital assets are anything associated with a value existing in a digitized environment. A physical counterpart to this digital asset may be partnered, but that is not true in all cases—some only exist electronically. These assets may be purchased through crypto transactions and then accessed in their virtual location on a distributed ledger. Asset ownership can be transferred from one party to another with records added to the ledger. Cryptocurrency is one such form of a digital asset and the focus of this briefing.

As referenced in the infographic "A Closer Look at Digital Assets," cryptocurrency is defined as "digital currency that can be used as a medium of exchange through an online experience, such as via a blockchain." This definition establishes our baseline understanding when using this term and sets the stage for our further exploration of cryptocurrency.

To get to a discussion on cryptocurrency, let's start by considering digital payments. Digital payments are defined as any financial transaction involving the usage of an electronic channel or taking place within a digital environment. Digital payments include the following payments rails and use cases:

Payment Rails	
ACH	Batch process credit and debit entries.
Card Transactions	Credit-push transactions initiated across the card rails.
Instant Payments	Near-real-time credit-push transactions.
Wire Transfers	Gross-settlement credit push transactions.
Use Cases	
Contactless Transactions	Payments occurring without physical connection. Commonly associated with mobile devices and digital wallets and may incorporate near-field communication technology.
Online Gaming / Metaverse	Transactions that occur within a gaming experience. May incorporate virtual or augmented reality technology.
Online Transfers	Movement of funds/value using online or mobile access points. Commonly involves A2A and P2P scenarios.
Peer-to-Peer Networks	Money movement occurring between two people via an exchange.

Cryptocurrency
Transactions processed in digital platforms are commonly placed on distributed ledgers. May fluctuate in value or be backed by fiat currency.

Digital Environments

Digital environment refers to virtual spaces or platforms where online interactions, including digital payments, occur. These environments are enabled through electronic devices such as computers, smartphones and VR/AR headsets that immerse users into a digital space.

Social media platforms, such as Facebook, Instagram and LinkedIn, are examples of digital environments that many of us use today. In addition, the Metaverse, which enables experiences like Fortnite and Metahero for gamers, is an immersive digital environment experience facilitated through virtual and augmented reality technology like Apple Vision Pro and Quest 3.

Other forms of digital environments include e-commerce platforms, collaboration centers (such as intranets and Microsoft Teams) and even education platforms. A common theme across these platforms is that they all contain elements related to communication, data sharing, storing and management, interactions and even transactional processes.

Examples of Digital Environments

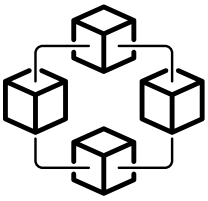
Social Media

Metaverse

Other

Technologies at Play

While there is a lot of hype about the technologies used to support digital currencies, tools like blockchains, distributed ledgers, and cryptography are not new.



Blockchains

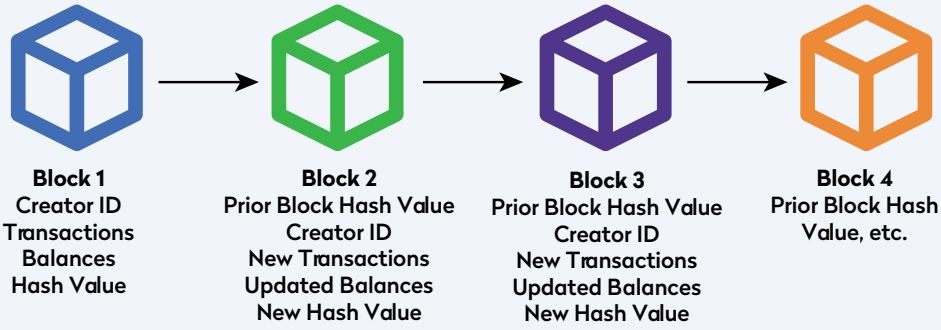
Blockchains are databases that store information in a series of blocks. New blocks are added sequentially, and each new block contains a link back to the previous one, usually through the hash value created when the block is encrypted. This linking helps those who view the blockchain keep the blocks in the proper order.

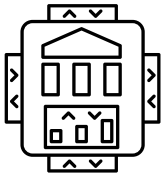
Blockchains are typically used to store data that changes over time. Each block shows the version of the data at the time the block was added. By looking back through a blockchain, a user can see the entire history of the data and trace changes all the way back to the beginning of the chain.

Nodes, or a series of computers, are used to monitor and maintain the integrity of a blockchain. This monitoring process includes consensus which ensures that unauthorized alterations have not been made. This concept is referred to as verified source of truth.

For digital currencies, the blockchain stores transactions and balances for currency owners. It acts like a combined posting journal and general ledger, with each new block listing transactions that have settled since the previous block and updated balances for all entities that own the currency.

Figure 1 – Blocks in a Blockchain



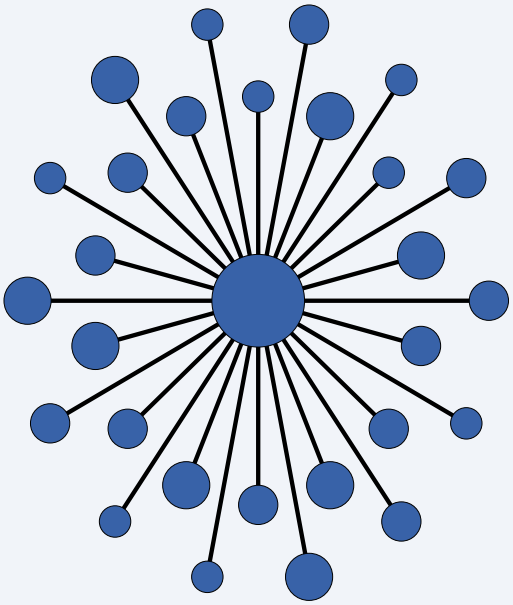


Distributed Ledgers

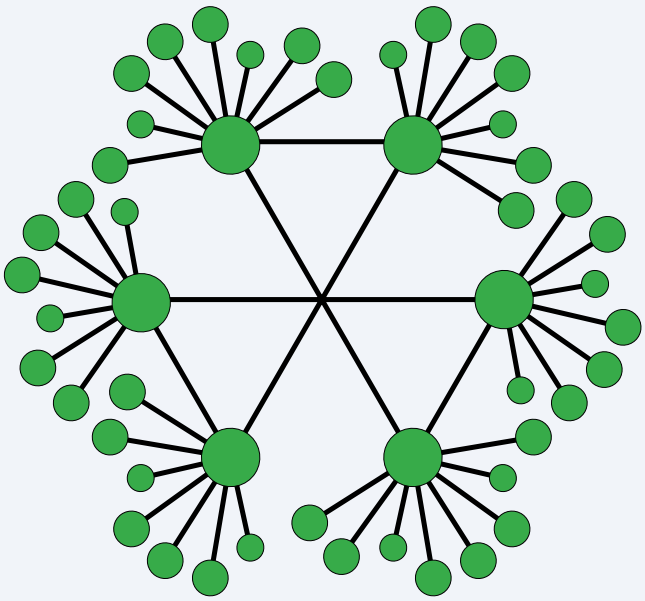
Distributed ledgers are systems used to allow parties to record transactions in multiple places at the same time. *(See Figure 2 below.)* Unlike traditional databases, distributed ledgers have no central data store or administration functionality. The shared blockchain at the center of a digital currency is one example, but not all distributed ledgers are blockchains. Most financial services applications store data in a single database with strong protective measures to keep the information private and secure.

Distributed ledgers are an effective tool for decentralized applications like digital currencies, which operate without organizational ownership or centralized control. Rather than operating under the authority of a centralized settlement agency, digital currencies settle transactions by consensus. In digital currency networks, each node has its own copy of the ledger (usually in the form of a blockchain) so it can verify that new blocks begin with the true history of transactions and balances. This syncing of shared data prevents tampering and helps keep the ledger accurate.

Figure 2 – Centralized and Decentralized Databases



Centralized Database
Single Owner
Single Instance
Restricted Access



Decentralized Copy of Data
Shared Access Validation
by Consensus

Sharing a full copy of the ledger with all network participants would seem to create privacy concerns, but digital currency ledgers don't store "customer" information—they only store account identifiers, usually called public keys. Public keys are longer than, but similar to, financial institution account numbers. By not storing personal data in the ledger, digital currency transactions are reasonably private for users, even though every node on the currency's network has a full copy of the ledger.

A currency owner's access to—and ability to spend—digital currency funds is through a private key. Private keys are lengthy alphanumeric strings that act as the sole identification of the user to the digital currency network. If public keys are similar to financial institution account numbers, private keys are like personal identification numbers (PINs) or passwords. Without your private key, you can't access your digital currency funds. Hence, the classic crypto phrase, "Not your key, not your coins."

Cryptography

Cryptography is a common tool for banking applications. Online credentials, mobile passwords, and ATM PINs are all encrypted by cryptographic programs before they are stored in a database. When these values are encrypted, the algorithm creates a hash value—a long string of letters and numbers that bears no resemblance to the original data—and stores the hash instead of the sensitive data. The same number will always generate the same hash, but two different numbers can never generate the same hash. To authenticate users at an ATM, the system takes the user's PIN input, runs it through the encryption process, and compares the resulting hash value to the hash value stored in its database. If they match, the system knows the user entered the correct PIN.

In addition to encrypting blockchain data, some digital currency systems use cryptographic hashing for another purpose. Decentralized currency networks must run through consensus of the participants instead of relying on centralized controls and computer platforms like those used to settle other types of payments.

Some digital currencies (Bitcoin, for example) depend on "miners"—private entities that voluntarily contribute computing power from their own systems to drive the network and process transactions, usually in return for a reward: A newly minted amount of the currency itself. But how can a consensus-based solution with no central control fairly select a miner to create the next block? Some systems rely on a proof of work model that requires new blocks to meet hard-to-achieve criteria in their encryption hash value. Miners must encrypt blocks over and over until they chance upon an encryption hash value that meets the requirements. This cryptography-based approach helps ensure that the most active participants are also the most rewarded.[1]

Cryptocurrency

Derived from the Greek word "kryptos," meaning hidden, cryptography literally translates to "hidden writing." It can be used to obscure any form of digital communication, including text, images, video or audio.[1]

1. IBM Block Chain

Exploring the Crypto Payment Participants

Consumers	Individuals involved in the payment either purchase or sell digital assets. Consumers create the demand for the goods and services and drive the movement of funds from mainstream financial services into digital currency mechanisms.
Cryptocurrency broker-dealers (often called exchanges)	An individual or company that facilitates the buying and selling of cryptocurrencies and usually involves a fee for services. Many such broker-dealers are fully automated software programs that operate without direct human control. This approach aligns with the digital currency focus on decentralized systems.
Financial Institutions (FIs)	FIs may play an indirect role when it comes to digital currency as the payment transaction is occurring outside of the FI. The FI serves as the gateway for those funds to move in and out of the digital currency network, but the transactions do not happen at the FI. An exception to this is if the digital currency exchange is a closed network operated by the FI. For funds to enter the mainstream financial services market they will typically be converted from digital currency into USD by a broker-dealer to be deposited electronically at the holder's FI.
Providers / Technology Companies	Companies that support aspects of the digital currency process. These companies support the digital currency ecosystem and enable other participants to facilitate payments in/out and across the digital currency environments. Examples of providers include: exchange providers, wallets, processors, asset management, borrowers and lenders, gateways, crypto ATMs, technology developers and mobile payment services (service providers that enable the management of digital currencies through crypto apps).
Businesses	Companies that are involved in the payment either purchase or sell digital assets.
Receivers	Receives the benefit from a digital currency payment.
Senders	Pays for goods, services, or money transfers related using a digital currency payment.
Operators	Similar to a card acquirer, oversees the operation of a given payment method. These parties enable the ability to accept digital payments and are involved in the exchange process.
Regulators	Agency that assumes governing control of a payment mechanism which may include establishing Regulation, laws, and examination over the given area.

Types of Digital Currency

Digital Currency refers to an asset that is managed, stored and exchanged electronically such as via through internet access. There is typically no physical component to this type of currency. Digital Currency comes in different forms and may fluctuate in value or be controlled such as by fiat-backing.

Cryptocurrency
Leveraging cryptographic technology, cryptocurrency is decentralized, and its value may be transferred across private networks. The valuation of cryptocurrencies can fluctuate and are driven by factors such as demand and availability.

Virtual Currency
A form of virtual money that can be used within an online experience or via a virtual economy. Virtual currencies may be controlled by a developer and the environment in which they operate. An example of virtual currency is closed-loop exchange mediums used within gaming environments where the currency is created and controlled by the game provider.

Stable Coins
A form of digital currency with value tied to, and backed by, fiat currencies or other commodities. While the other characteristics of these coins are similar to other digital currencies, the volatility of value is reduced with a stablecoin. Stablecoins are generally less decentralized than pure cryptocurrencies because some entity must acquire and manage the fiat currency or other asset from which the stablecoin gets its value.

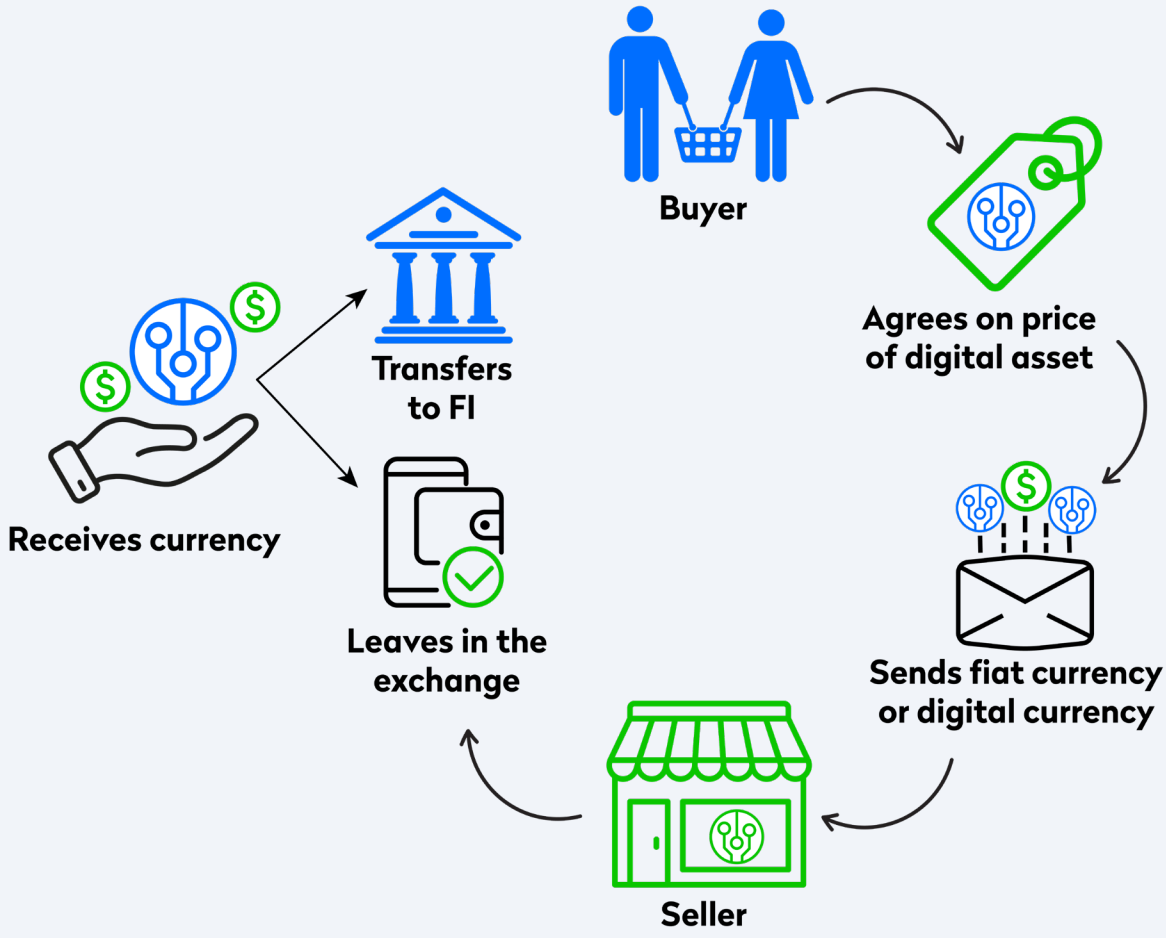
Central Bank Digital Currency (CBDC)
A form of digital currency that is issued and controlled through a central bank. CBDCs serve as a digital version of fiat currency and like Stablecoins are not subject to the same degree of valuation fluctuation. A unique characteristic of a CBDC is that connections to the network established through the central bank may or may not involve the private banking sector. Because CBDCs are controlled by central banks, they differ from most other forms of digital currency by operating in a centralized—rather than decentralized—way, allowing CBDCs to potentially function using traditional financial technologies rather than a blockchain.

Anatomy of Common Transactions

Where does the money and value go?
Buyer agrees on the price of a digital asset (current trading price, NFT auction, etc.) and either sends fiat currency or other digital assets for payment.

Seller receives value and may choose to transfer funds to their financial institution or leave in the exchange.

Figure 3 – Common Transactions Flow



Forward payment exchange:
Primary financial services market funds may be used to fund the purchase of a digital currency payment. In such transactions, funds will first move from a traditional financial service provider into a digital currency. This process is accomplished via crypto ATMs and other online mechanisms that fund the digital currency.

Parties who acquire an amount of the digital currency may use it to purchase goods and services. These transactions are logged and archived. In the case of blockchain environments, a block will be added to the blockchain logging the transaction details.

The value of the digital currency and associated digital assets will remain in the local environment until the value is moved back into fiat currency.

Exceptions:
A benefit, and potential risk, of digital currency transactions is that there is little friction involved in the payment process. For this reason, there is not a true exception process. Digital currency transactions only post if the transaction can be completed.

The valuation process is a challenge with many forms of digital currency transactions. This means that the value of the currency or asset at the time a contract is entered into may be different once the transaction has been completed.

Return processes:
Digital currency transactions are irreversible; funds cannot be pulled back once a transaction has completed.

To return funds from a digital currency transaction, a new opposite transaction would need to be initiated.

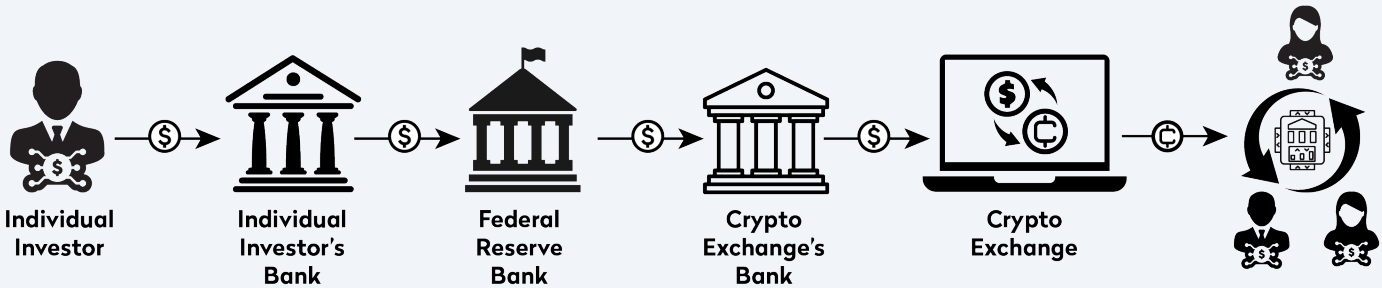
It is possible that the parties in control of the digital currency platform may have the ability to troubleshoot issues once a transaction has completed. However, this process will vary from provider to provider.

Information needed to facilitate payments:
With many digital currency transactions, the identities of the payment parties may not be known to each other. This means that parties to a digital currency transaction may stay anonymous.

For most digital currency transactions, the payor will need to know the recipient's digital currency address, also known as wallet address. This is the identifier for the location to send the value or asset. The amount, any fees, and payment details will also need to be included.

A benefit of digital currency transactions is that they can be data-rich where robust information related to the transaction can be provided. Digital currency transactions also support the ability to enable smart contracts that trigger automated actions for asset movement and titling, shipping of product, etc. related to the receipt and booking of a payment.

Figure 4 – Digital Currency Transaction Flow



Valuation of digital currencies:
Digital currency valuation will vary depending on the characteristics of the currency.

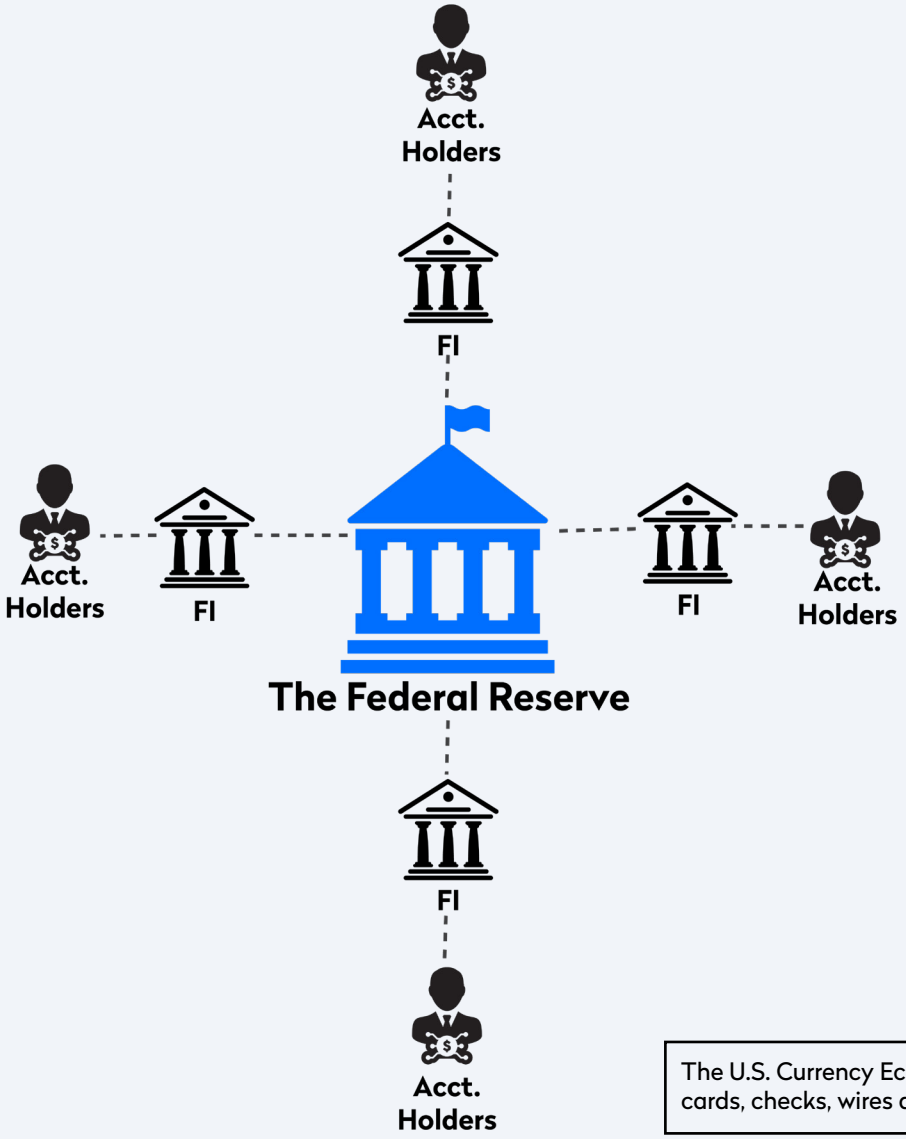
Currency that is not backed by fiat currency or another commodity results in the valuation process subject to the market. Factors such as supply and demand, utility, availability, speculation, competition, and liquidity are all considered and create a large degree of fluctuation. For example, bitcoins are mined and the number of bitcoins available can directly impact the given value.

For stablecoins and CBDC, the value of the currency is driven by the value of the fiat currency or associated commodity that controls and stabilizes the value of the digital currency.

U.S. Currency Ecosystem vs. Cryptocurrency Ecosystems

The U.S. Currency ecosystem is built around Federal Reserve settlement for all non-cash transactions, with financial institutions acting as a touchpoint for consumers and businesses that want to move money. While there are additional variables associated with various payment rails, Figure 5 below demonstrates a simplistic view of how mainstream transactions work today.

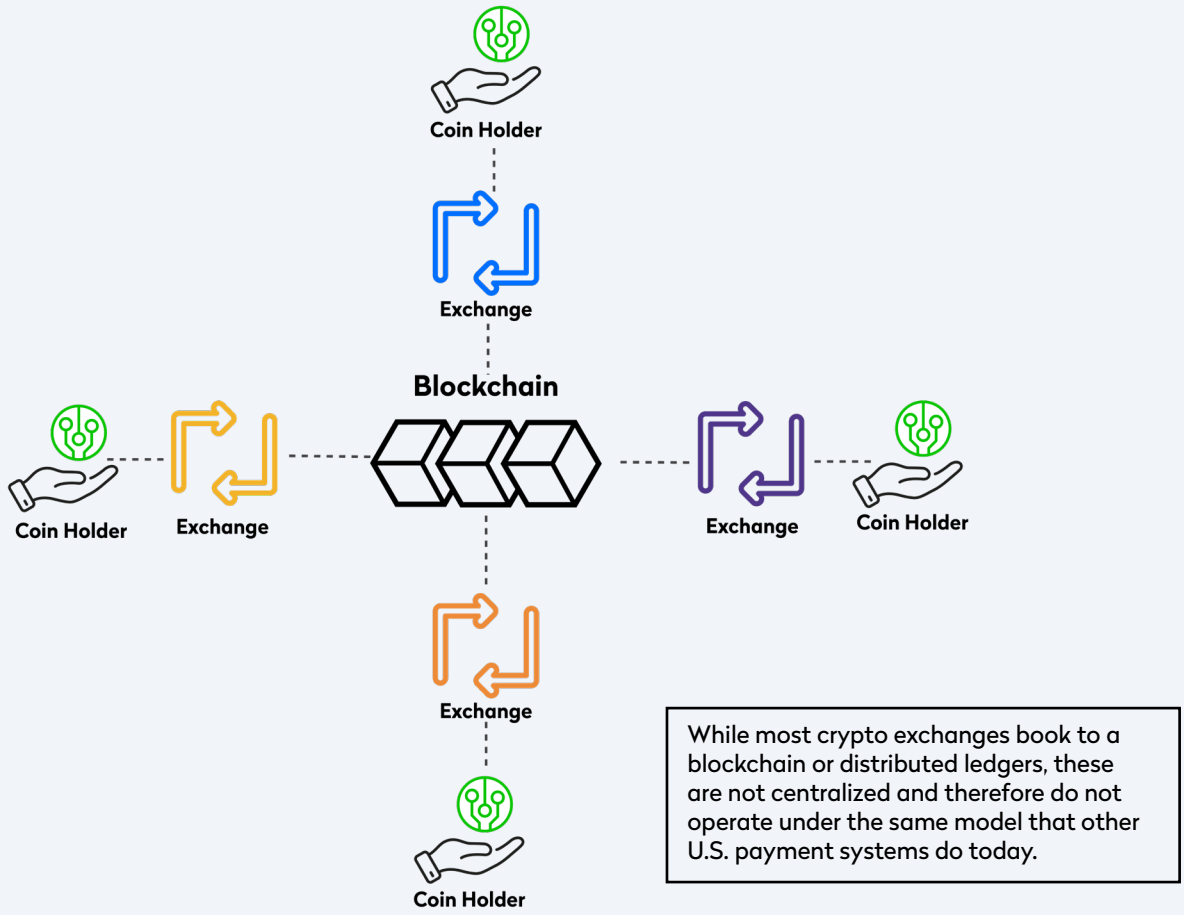
Figure 5 – U.S. Currency Ecosystem



The U.S. Currency Ecosystem includes ACH, cards, checks, wires and instant payments.

While digital currencies were designed to eliminate "trusted entities" like financial institutions, exchanges have assumed a similar role in the crypto ecosystem, acting as touchpoints for coin holders who wish to move funds. Figure 6 demonstrates the complexity of cryptocurrency ecosystems in that there is not a centralized settlement and each environment is likely to operate interdependently.

Figure 6 – Cryptocurrency Ecosystems



While the process can vary in some conditions (e.g., when the coin holder making the payment is a direct node in the decentralized network, an exchange may not be required to submit transactions to the blockchain), the graphic below represents the normal flow of funds in a digital currency transaction.

Step 1: The coin holder submits a transaction request to their exchange.

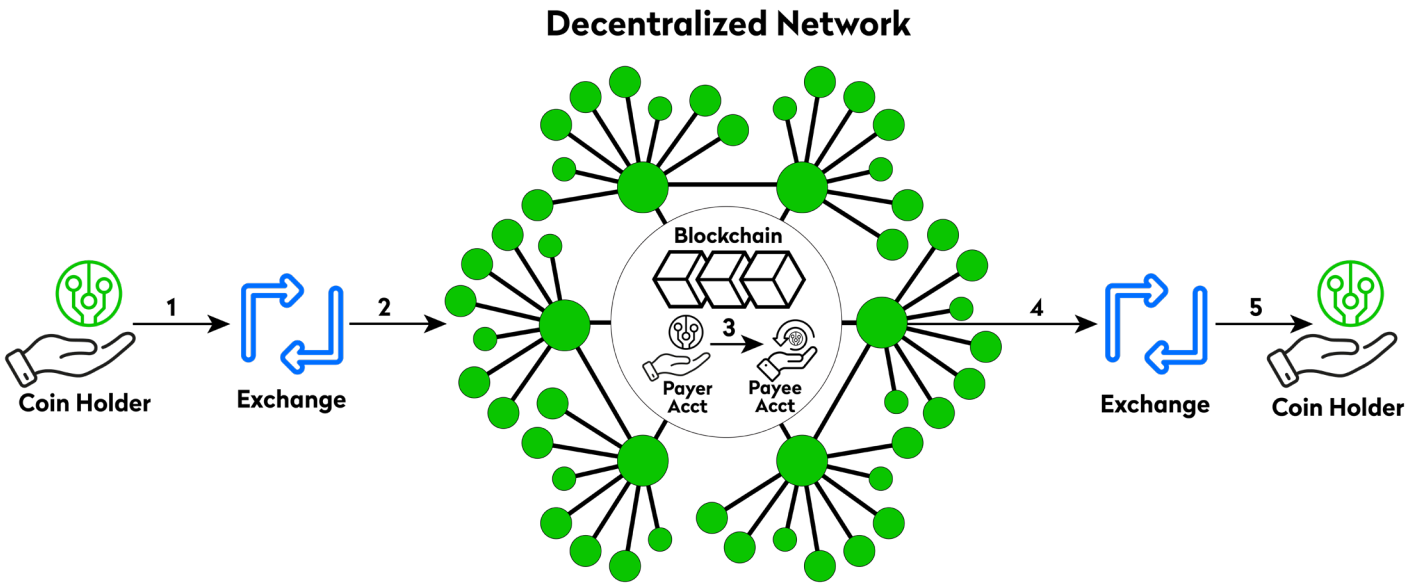
Step 2: The exchange submits the request to the blockchain via the decentralized network.

Step 3: The blockchain includes the transaction in its next block, moving funds from the payer's account balance to the payee's account balance.

Step 4: The payee's exchange sees the funds appear in the payee's account balance on the blockchain.

Step 5: The exchange may optionally notify the payee that funds have been received.

Figure 7 – The Flow of Funds in Digital Currency Transactions



Closing Thoughts

Cryptocurrency enables many different use cases and possibilities. However, proper governance structure around financial institution usage is needed to help avoid the potential for an institution to come under regulatory scrutiny. As the industry has already seen lack of oversight can cause significant challenges.

Financial institutions will likely rely on their existing know-your-customer (KYC) practices that include reviewing transactions between crypto-exchanges and bank accounts. However, once funds are converted within the exchange and transacted, if there isn't a framework developed, there is a question of if the institution will know who the participants are and gain insight into what is happening outside of mainstream financial services payments. It is a question of the exchange's responsibility versus the financial institution's, including rights and obligations.

Another consideration for financial institutions is regarding consumer rights and protections. Unlike ACH and EFTs where ACH debits (and credits in cases of fraud) are governed under Reg E, the rules for crypto and digital asset exchanges is yet to be determined. What we know today is that transactions passing from mainstream financial services to cryptocurrency environments will likely be subject to consumer protections.

With much uncertainty at play, financial institutions may not be ready to make final decisions surrounding cryptocurrency development and usage. This uncertainty is where the Nacha Payment Innovation Alliance is here to help. Keep an eye out on future briefings and other information where we will continue the conversation by diving into topics related to security, fraud and regulatory challenges.

Navigating Digital Payments Project Team

This paper was developed by the Navigating Digital Payments Project Team of Nacha's Payments Innovation Alliance.

Payments Innovation Alliance

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Navigating Digital Payments Project Team to explore the digital and physical world implications of money and asset movement. Visit Navigating Digital Payments Project Team to learn more.

©2024 Nacha. All rights reserved.