GEORGETOWN UNIVERSITY
Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

DECRYPTING CRYPTO

Edited by Yaya J. Fanusie, Visiting Fellow

An explainer series on digital assets covering:

- Cryptocurrency
- Blockchain Technology
- Tokenization
- CBDCs and Stablecoins
- TradFi and DeFi
- Digital Asset Exchanges
- Smart Contracts
- Illicit Finance

Decrypting Crypto:
Cryptocurrency

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Michelle Chen and Ana Mocanu, Research Assistants

Key Insight

Cryptocurrencies have introduced a new way to transmit value on the internet, prompting traditional financial institutions to explore ways to integrate the technology into mainstream use. The regulatory environment still faces significant regulatory uncertainty in the United States, but the European Union has taken major steps to formalize its cryptocurrency markets.

Summary

Cryptocurrencies are units of digital ownership recorded on a distributed ledger system known as a **blockchain**. Unlike fiat currencies issued by national governments that need regulated financial institutions to facilitate digital transactions, cryptocurrencies run on public blockchain platforms where a transaction settlement is conducted by a network of computers open to anyone with internet access.

Cryptocurrency transactions occur directly between individual wallets and are verified by a decentralized network of validators or miners, who confirm the transactions in batches before adding them to the blockchain. This approach makes the entire transaction history of all wallets publicly visible without requiring or attaching users' personal identification to the wallets.

Key Facts

To own cryptocurrency and transact on a blockchain, one must have a private key: a unique string of numbers and characters tying specific units of data on the blockchain to a digital wallet. Similar to the function of physical wallets, digital wallets can store one's private funds as well as credentials for transacting. They fall under two general categories, custodial and self-custodial, with the former being more widely adopted by the casual user.

A custodial wallet's private keys are managed by a firm on behalf of the user. Access to cryptocurrency accounts is primarily verified through traditional passwords and biometric verification processes. Examples of such custodians include Coinbase, Binance, and Blockchain.com.

A self-custodial wallet keeps the private key with the user, giving the users full control of the wallet's contents. While this keeps funds more secure from hacks, self-custodial wallets tend to be less user-friendly than custodial wallets and require more diligence in protecting one's private key.

Some businesses do accept cryptocurrency payment methods, but it is not widespread. A study estimated that around 2,352 US businesses accept Bitcoin. One noteworthy case is U.S. Telecom provider AT&T, which began accepting payments in 2019 through cryptocurrency payment processor BitPay. In 2021, $1.2 trillion was exchanged in conventional banking cross-border payments. Cryptocurrency is borderless with users generally able to transact with anyone with a corresponding crypto wallet. This ease of access offers potential opportunities for improving financial efficiency and access.

Key Institutions

Developers, validators, and miners form the backbone of the cryptocurrency ecosystem, designing blockchain **protocols** and verifying transactions to maintain system integrity.
While cryptocurrency trading was initially limited to a niche group of technologists, it has become increasingly accessible to the general public through exchanges and regulated products. Centralized exchanges like Binance, Coinbase, and Kraken simplify trading with user-friendly interfaces, fiat on-ramps, and services like staking and lending, lowering barriers to entry for retail investors.
Simultaneously, institutional players like Grayscale, BlackRock, and Fidelity are introducing regulated products such as Spot Bitcoin and Ethereum ETFs, broadening access and seeking to integrate crypto into mainstream finance. Technology companies and payment processors like Block and Paypal have been developing end-market applications integrating crypto with day-to-day payment transactions. These activities occur within a still-evolving policy environment, where regulators are tasked with helping the cryptocurrency sector balance innovation with consumer protection, addressing risks such as money laundering and market manipulation.

Background

The roots of digital currency systems trace back to the late twentieth century, beginning with David Chaum's DigiCash in 1983. DigiCash introduced cryptographic protocols as a way to secure digital transactions and enable anonymous payments.
However, it relied on a centralized structure, which limited its potential and scalability by creating decision-making bottlenecks and limiting adaptability to market changes. Later, in 1998, Wei Dai proposed the concept of a pseudonymous electronic cash system called b-money, while Nick Szabo developed the framework for another cryptographic digital transaction system called Bit Gold. Though never fully implemented, both were among the earliest and most impactful attempts to create decentralized virtual currencies. They introduced foundational concepts such as distributed ledgers, proof-of-work, and anonymous transactions, laying the groundwork for the eventual development of Bitcoin's protocol.
Bitcoin, the first and still most popular cryptocurrency, was introduced in 2009 by the pseudonymous creator Satoshi Nakamoto. Its biggest breakthrough was establishing a system where users could trust the validity of online transactions without relying on a central authority. Unlike previous attempts at internet-based currency, Bitcoin successfully implemented a proof-of-work system where computers seek rewards by racing to solve cryptographic puzzles. This incentivizes validators to participate in the confirmation transaction process and thus maintain network integrity, solving the **double-spending problem** (use of the same token to conduct multiple transactions). Bitcoin's supply is fixed at 21 million coins, creating scarcity, and each bitcoin can be broken down into smaller units, a divisibility allowing Bitcoin to function as an exchange medium even when its value increases. Bitcoin proponents argue that this scarcity positions it as a hedge against inflation. Moreover, Bitcoin's popularity was not only due to technological innovation but also its timing, offering a decentralized alternative during a global financial crisis that provoked dissatisfaction with traditional financial systems.
Today, the cryptocurrency market has grown, encompassing thousands of coins beyond Bitcoin. New coins first emerged in the 2010s,

such as Litecoin (LTC), Ethereum (ETH), Ripple (XRP), and Dogecoin (DOGE), offering new use-cases or technical refinements, from enabling smart contracts to facilitating faster cross-border payments and supporting community-driven digital assets.

Policy and Regulation Issues

The decentralized, fast-evolving, and global nature of cryptocurrencies brings regulatory challenges. While many nations have started to develop policy frameworks for the exchange, taxation, and risk management of cryptocurrencies as a whole, lawmakers and regulators are usually a few steps behind the rapidly developing cryptocurrency industry.

In the US, cryptocurrency has been subject to anti-money laundering (AML) regulations since 2013 under the Financial Crimes Enforcement Network (FinCEN). However, debate continues over which regulatory bodies should oversee these rapidly evolving digital assets. While the CFTC regulates commodities and the SEC securities, cryptocurrencies often blur the lines of oversight.

The European Union has been more proactive in regulating the cryptocurrency industry, developing a rigorous set of guidelines pertaining to the space. In April 2023, the Markets in Crypto Asset Regulation (MiCA) was passed, establishing that all companies looking to trade or issue cryptocurrencies require licensing. Overall, the European Union has been tightening its rules on institutional players and clarifying requirements for consumer protection. Some countries, such as Bolivia, have installed a nationwide ban on the use of cryptocurrencies.

On the other end, countries like El Salvador have integrated cryptocurrency as a legal tender under the premise of encouraging foreign investment and promoting accessibility to the financial system for all citizens.

Decrypting Crypto:
Blockchain Technology

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Kelly Grace Richardson, Research Assistant

Key Insight

Blockchain technology is a revolutionary innovation for digitally transmitting data, enabling value-transfer to occur without centralized intermediaries. The decentralized software technology also supports **smart contracts** that enable transaction programmability which can be applied to manage financial and non-financial data on the internet.

Summary

A blockchain is a software protocol that produces a decentralized immutable ledger that records transactions across a wide set of computers within a network. The record of transactions is organized into blocks that are linked cryptographically so that data within the blockchain can not be changed and is available to be viewed and evaluated in real-time. Blockchains ensure that recorded transactions can not be altered and their transparency makes them useful for documenting the exchange of digital assets. Cryptocurrencies are actually units of ownership assigned to blockchain addresses, controlled by whoever has access to the address's private cryptographic key. There are various types of blockchain protocols using different mechanisms to confirm transactions and maintain the protocol's functionality and reliability. Many blockchains utilize smart contracts to automate the execution of transactions and enable sophisticated programming within the blockchain's ecosystem. Although the most popular blockchain use-case is for acquiring, holding, and sending cryptocurrencies, the technology's transparency and real-time availability of data offers improved efficiency and resiliency for managing and analyzing various types of online data. However, regulatory uncertainty around the technology–especially in the financial sector–has hindered wider adoption for both financial and non-financial applications.

Key Facts

A blockchain consists of permanent data blocks added in sequential order that are assigned a hash based on the timestamp, with each block linking the previous blocks' hash. Blockchains operate by various types of software **consensus mechanisms** to ensure that all the computers validating the network agree upon the data set and only accept one specific, authentic record of transactions. While storing and sending cryptocurrency tokens is the most popular use of blockchain technology, other use cases for the technology are still in the early exploration phase and span many industries. For example, blockchain can be used to simplify and automate the supply chain process by increasing data transparency and accuracy. Blockchain's immutable data storage process can assist with the protection of intellectual property, particularly through non-fungible tokens (NFTs) which act as digital receipts within a distributed ledger system. Currently, NFTs are primarily used by artists seeking to document and monetize their creative intellectual property in fields such as music or

art. Lastly, there is significant research and piloting in using blockchain to verify credentials.

Key Institutions

Financial institutions such as BlackRock and Goldman Sachs have ongoing efforts to educate investors and the public on blockchain technology as well as build trust in the space. Other leaders in the space include IBM, Nvidia, Block, Oracle, and Amazon, who are all investing in the technology for their business lines. Notable companies providing blockchain-related services include digital asset exchanges like Coinbase and Binance, payment providers like Ripple and Circle, blockchain infrastructure like ConsenSys, and blockchain analytics like Chainalysis and Elliptic.

Background

The concept of a cryptographically secured chain of blocks was first described in 1991 by Stuart Haber and W Scott Stornetta. The first successful deployment of public blockchain software was implemented in 2009 by a developer operating under the pseudonym Satoshi Nakamoto. This blockchain system enabled users to send and receive unit values known as **Bitcoin** in an online public ledger. In 2014, the Ethereum blockchain system introduced computer programs known as smart contracts into the blocks, enabling more sophisticated applications beyond the sending and receiving of tokens.

Policy and Regulation Issues

Blockchain technology industry faces regulatory challenges which differ from other parts of the software sector. This is especially true for the cryptocurrency use-case where much of the blockchain activity functions as a transaction in value, triggering certain financial regulatory requirements. This is complicated by the fact that, in the U.S., there is a lack of legal clarity around whether various tokens may fall under securities or commodities laws. Blockchain-related activities also raise some legal questions around personal data privacy, intellectual property, and the enforcement of smart contracts. For example, one standing question surrounds the legal validity of financial instruments issued in blockchains and whether these can be used as evidence of possession.

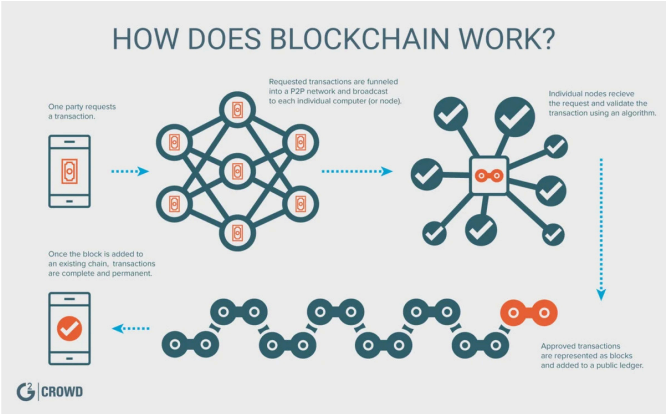

Image courtesy of Walker, Aaron. How Does Blockchain Work? 2018. G2, https://learn.g2.com/trends/blockchain-security.

Decrypting Crypto:
Tokens and Tokenization

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Julen Payne, Research Assistant

Key Insight

Tokenization brings the transparency, auditability, and programmability of blockchains and cryptocurrency tokens to traditional assets. However, there is significant legal and regulatory work needed for the tokenization of real world assets to be deployed on a mass scale.

Summary

Tokens are digital representations of rights to a unique item that may be an asset, service, or the receipt or marker of a completed action. Tokenization is the process of creating a digital representation of something that one wishes to reside on a blockchain for some function, such as to record and track transfers in ownership. Any party with internet access can create a token on a public blockchain.

Key Facts

- Because tokens operate on blockchains that typically are always accessible in real-time, auditable, and programmable, they can easily be used to indicate the transfer of value between parties.
- One of the most common types of real world asset tokenization currently being explored are investment funds. Tokenization enables investors to purchase shares of a fund through a blockchain platform whose programmability and 24/7 auditability make transactions and overall fund management more efficient.
- A very popular form of tokenization is with stablecoins, which are blockchain-based representations of fiat currencies held in a reserve. Stablecoin regulation has grown as a financial policy issue for the United States as policymakers consider how stablecoins can generate inflows into U.S. Treasuries and enable dollar-denominated payments in blockchain protocols.
- For a tokenized asset, the underlying asset itself is not legally transferred unless there is an accompanying legal framework and process in the real world (i.e., off chain). Typically, for the transaction to be legally binding, the real asset must be held in some form of neutral custody before issuing tokens to represent the value. For example, transferring ownership of an asset like a house into a special purpose vehicle legal entity would allow the holders of the real estate token to acquire the rights to the legal entity and be the legal owners of the underlying asset–the house.

Key Institutions

- Circle: U.S.-based financial technology company responsible for issuing USD Coin (USDC), the second largest stablecoin by market size.
- Tether: British Virgin Islands-based company that issues USDT, the most widely used stablecoin today.
- Ondo: Decentralized Finance (DeFi) network that issues a variety of token products backed by U.S. Treasuries primarily geared towards large institutional investors. It is backed by BlackRock's BUIDL fund.

- Securitize: The world's largest tokenization platform/provider. Provides the tokenization infrastructure for BlackRock BUIDL, Apollo Global's ACRED, and Hamilton Lane's SKOPE funds.
- Opensea: One of the world's leading NFT marketplaces.
- Ethereum Foundation: Non-profit that funds and supports the development of the Ethereum blockchain ecosystem.

Background

In 2015, the Ethereum Foundation created the ERC-20 token standard in order to establish common technical rules for smart contracts for tokens on the Ethereum blockchain. The various forms of the ERC technical standards are in reference to how tokens that represent a smart contract should behave in regards to another token. An ERC-20 is a standard in which a token is completely fungible with another that comes from the same contract (USDC, USDT). Through this standard for token issuance on a widely popular blockchain, a wave of Decentralized Finance (DeFi) applications were built with newly composable standardized tokens. In 2020, an additional standard called ERC-721 became popular that enabled a smart contract to mint/create an individual token that was completely unique, and could not be duplicated. Known as non-fungible tokens (NFTs), these tokens initially arose as digital art that could be traded on blockchains. However, the ERC-721 standard can be used for representing any sort of unique document. Over time, many other types of programmable blockchains besides Ethereum have developed, with different rules for designing and issuing both fungible and non-fungible tokens. However, the ERC standards remain the most popular for token issuance. Today, there are many projects that tokenize real world assets such as fiat currency, real estate ownership, securities, and intellectual property rights onto blockchains, although the legal and regulatory framework around many of these use-cases is nascent and unclear.

Policy and Regulation Issues

A current key policy issue surrounding tokens is whether they should fall under the regulatory framework of conventional financial assets such as securities or commodities. In the U.S., there is no regulatory clarity around how tokens should be legally classified, leading to apprehension and hesitancy by token project developers, entrepreneurs, and venture capital investors. Oftentimes token issuers are forced to block their protocols from U.S. persons for fear of being prosecuted for violating U.S. securities or commodities laws. The crypto industry has been calling for a regulatory framework to legally differentiate the types of tokens at the time of issuance, so companies can obtain the required licenses for their specific businesses. A comprehensive crypto regulatory framework in the United States would help bring clarity to project developers and regulators alike and allow for greater experimentation with tokenization, including enabling traditional financial institutions to use blockchains to execute transactions of real world assets they already manage.

Decrypting Crypto:
Central Bank Digital Currencies and Stablecoins

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Melina Ramirez, Research Assistant

Key Insight

CBDCs and stablecoins are emerging as new potential payment methods, largely inspired by the rise of cryptocurrencies and blockchain technology. Although their usage and regulatory treatment are in the early stages of development, many governments and industry players are exploring how these innovations could make financial transactions more efficient and useful for the public.

Summary

A Central Bank Digital Currency (CBDC) is a public digital form of money issued by a central bank, typically denominated in the national currency and convertible to other forms of central bank money. CBDCs can serve different purposes: retail CBDCs are accessible to the general public and can substitute cash for everyday consumer payments, while wholesale CBDCs are limited to large-scale transactions between financial institutions to enhance financial market efficiency. In contrast, a stablecoin is a crypto asset designed to maintain a stable value relative to a specified asset or a pool of assets. Stablecoins pegged to sovereign currencies are more likely to guard against price volatility and function as a form of digital money, making them more attractive for payments than regular cryptocurrencies.

Key Institutions

- Bank for International Settlements (BIS): Provides research, guidance, and coordination among central banks for the development of CBDCs, including frameworks for cross-border interoperability.
- *Circle*: U.S.-based financial technology company responsible for issuing USD Coin (USDC), the 2nd largest stablecoin by market size.
- *MakerDAO*: A **Decentralized Autonomous Organization (DAO)** that governs the DAI stablecoin.
- *European Central Bank (ECB)*: Currently researching and piloting the digital euro, contributing to the advancement of CBDCs in the Eurozone.
- *Financial Stability Board (FSB)*: Evaluates risks to global financial stability and develops international regulatory standards for, among other things, **cross-border payments**, **DeFi**, and crypto-assets activities. In particular, the FSB has published a report on global stablecoins arrangements that "seek to promote consistent and effective regulation, supervision and oversight of global stablecoin arrangements (GSCs) across jurisdictions." Regarding CBDCs, the FSB does not directly focus on them but examines their implications within the broader context of financial stability and cross-border payments.
- *G7 Working Group on Stablecoins*: Assesses the potential benefits and risks of stablecoins and CBDCs in the global economy and promotes collaborative regulatory approaches.

- *International Monetary Fund (IMF)*: Researches the policy implications of CBDCs and provides technical assistance to countries exploring their potential integration. While the IMF has extensively analyzed CBDCs, its engagement with stablecoins has been more limited, primarily focusing on their regulatory and macroeconomic implications.
- *Tether*: British Virgin Islands-based company that issues USDT, the most widely used stablecoin today.

Background

The first Central Bank Digital Currency (CBDC) was introduced in 1993 when Finland launched the Avant smart card, an electronic form of cash. The Avant operated until 2000 when it was discontinued. For well over the next decade, CBDCs were not a significant focus for central banks. However, by 2014, central bankers began discussing the technological advancements of Bitcoin, leading to formal government research in digital currency technology. A significant milestone that year was the Bank of England's report *Innovations in Payment Technologies and the Emergence of Digital Currencies*, which identified the distributed ledger as a key technological innovation in digital currencies. It emphasized the potential of **distributed ledger technology (DLT)** to fundamentally transform payment systems by enabling decentralization and pointed to its potential for broader applications in financial markets.

This growing interest in digital currencies paved the way for central banks to actively explore CBDCs. As a result, by 2021, nearly 100 CBDCs were in the research or development stages, with two fully launched: Nigeria's eNaira, unveiled in October 2021, and the Bahamas' Sand Dollar, introduced in October 2020. By the end of 2024, two additional CBDCs became operational—Jamaica's Jam-Dex and Zimbabwe's ZiG.

On the other hand, stablecoins emerged in 2014 with early examples such as BitUSD, NuBits, and Tether. While BitUSD and NuBits failed due to factors such as reliance on volatile collateral or weaknesses in their peg mechanisms, Tether (USDT) was marketed as backed by U.S. dollars, making it appear more stable and secure. As a result, this stablecoin not only remained in circulation while the others collapsed but also gained significant popularity.

The next major milestone in the stablecoin space was in 2017 with the launch of DAI by MakerDAO. What made DAI unique is that it was the first to combine elements of both traditional and **algorithmic stablecoins**. DAI is collateralized, but instead of **fiat currency**, it is backed by multiple cryptocurrencies, which aims to increase its stability. It also employs an algorithmic system of smart contracts that actively manage risk by enforcing over-collateralization and automatically triggers liquidations when thresholds are breached. These liquidations not only protect the system from under-collateralization but also contribute to long-term stability by indirectly reducing the amount of circulating DAI when necessary. DAI gained popularity as decentralized finance (DeFi) grew because it enabled lending protocols, trading platforms, and yield farming strategies by providing a stable, intermediary-free medium of exchange.

Benefits & Challenges

CBDCs:

- *Financial inclusion*: Experts argue that retail CBDCs in developing countries could significantly enhance financial inclusion by expanding access to banking and digital payment services for previously unbanked

populations. CBDC issuance could incentivize individuals to open bank accounts to access CBDC wallets, potentially bringing new deposits into the banking system. Additionally, CBDC usage could generate valuable data that helps reduce credit-risk information asymmetry, enabling banks to offer lower interest rates and more accessible loans.

- *Improved cross-border payment efficiency*: CBDCs could improve cross-border payment efficiency by addressing common frictions such as high costs, long settlement times, and complex compliance processes. Additionally, CBDCs have the potential to operate 24/7, reducing mismatches in operating hours that hinder traditional payment methods. If effectively implemented, these features could enhance interoperability between domestic and foreign payment systems, positioning CBDCs as a potentially transformative tool in global finance.

Stablecoins:

- *Fast settlement and Programmability:* Unlike traditional bank transfers, stablecoin transfers move directly from wallet to wallet without a centralized intermediary, providing near-instant settlement. They are also available 24/7 and can function within blockchain smart contracts for programmable transactions.
- *Liquidity in DeFi:* Stablecoins provide significant liquidity for decentralized exchanges (DEXes) and lending protocols. In May 2022, they accounted for about 45% of the liquidity in DEXes, with algorithmic stablecoins like DAI contributing a substantial share relative to their market capitalization. Lack of tangible asset backing: While algorithmic stablecoins are an innovative concept, major concerns remain about their functionality. Following the Terra Luna crash in 2022, markets became increasingly cautious about their stabilization mechanisms and the absence of tangible asset backing, which has proven to undermine their ability to maintain stability during periods of market stress.

Policy and Regulation Issues

CBDCs:

- Legal classification: Determining whether CBDCs should be classified as cash, deposits, or e-money is a key challenge. Each approach has implications for its integration into existing legal frameworks.
- Privacy vs. Compliance: CBDC systems face challenges in balancing user privacy with financial crime prevention. While anti-money laundering (AML) and countering the financing of terrorism (CFT) are crucial considerations in monitoring CBDC transactions, there is a fine line between regulatory oversight and the unauthorized use of private data, which could result in excessive government surveillance. Additionally, because CBDCs facilitate cross-border transactions, they involve multiple jurisdictions and regulatory frameworks, making compliance even more complex. This interconnected nature also increases the risk of data breaches and unauthorized access, as sensitive financial information may be shared across various institutions with differing security standards.
- Cross-Border Use: Jurisdictional rules are needed for international CBDC transactions, such as determining applicable laws and models for interoperability, pose significant regulatory hurdles.

Stablecoins:

- Varied Regulatory Frameworks: Globally, there are not many regulations for stablecoins yet. However, the EU's MiCA categorizes stablecoins as **electronic money tokens (EMTs)** or **asset-referenced tokens (ARTs)**, requiring reserves and authorization. In the U.S., there is little federal regulation, but at the state-level, New York is enforcing measures like 1:1 liquid reserves under the BitLicense system.
- Common Regulatory Principles: Considering the heterogeneous and insufficient regulatory frameworks, common principles are emerging. Some of the most important ones are: stablecoin issuances require explicit regulatory approval, reserves must be liquid and stable to maintain a 1:1 backing, and stablecoin payment services must align with financial regulations to ensure user protections, including redemption rights and transparency.

Decrypting Crypto:
Traditional Finance Versus Decentralized Finance

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Rohan Mistry, Research Assistant

Key Insight

Although TradFi and DeFi mostly operate in separate technological ecosystems, rising private sector interest in financial innovation and growing concerns by regulators about DeFi risks are spurring efforts to broaden the regulatory perimeter to include decentralized systems.

Summary

Traditional finance (TradFi) refers to the conventional financial systems that have long governed global economic interactions, including banking, stock markets, and investment vehicles. These systems rely on centralized entities such as banks to facilitate access to services and ensure trust in transaction settlement and regulations. In contrast, decentralized finance (DeFi) is an innovation powered by **blockchain** technology that operates without centralized intermediaries. DeFi enables financial activities like lending, borrowing, and trading through **smart contracts** and distributed ledgers. The tension between TradFi and DeFi reflects a broader clash of centralized control versus decentralized, permissionless access, each offering unique benefits and challenges.

Key Facts

Traditional finance operates through centralized systems, relying on intermediaries such as banks, stock exchanges, and investment firms to ensure trust, efficiency, and regulatory compliance. Banks safeguard funds, facilitate loans, and manage payment systems, while stock exchanges provide regulated environments for trading securities. These systems are governed by extensive regulations, including Know Your Customer (KYC) procedures and Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws, designed to validate users and keep criminal funds out of the financial system. However, the requirements of compliance do create costs and barriers to serving the widest range of potential customers. Many people are not able to easily access the breadth of financial services available in the traditional financial sector. Decentralized finance (DeFi) represents a contrasting model, operating on blockchain networks with smart contracts that automate digital asset transactions between users without intermediaries. This approach significantly reduces transaction costs and barriers to entry, enabling users to access financial services directly. Platforms like Aave and Compound facilitate lending and borrowing with interest rates determined automatically by supply and demand while decentralized exchanges such as Uniswap use **liquidity pools** and algorithms for peer-to-peer trading without centralized order books. Unlike traditional finance, where asset ownership data is centralized among a few institutions, decentralized platforms use distributed ledgers maintained by a broader community to create a more transparent and collaborative system of tracking asset ownership. Despite its inclusivity, DeFi carries risks due to its lack of centralized oversight.

The ecosystem has seen over $6.45 billion in financial losses through vulnerabilities in smart contracts and governance mechanisms, highlighting the challenges in balancing security, accessibility, and innovation.

Key Institutions

Traditional finance depends on critical institutions such as central banks, commercial and investment banks, and stock exchanges. Central banks, like the U.S. Federal Reserve and the European Central Bank, manage monetary policy, control inflation, and stabilize economies during crises. Commercial banks, including JPMorgan Chase and HSBC, offer services such as savings accounts, loans, and business financing, while investment banks focus on mergers, acquisitions, and raising capital. Stock exchanges, such as the New York Stock Exchange and Nasdaq, provide regulated marketplaces for trading securities, fostering capital formation and economic growth. Regulatory bodies like the U.S. Securities and Exchange Commission (SEC) ensure compliance, transparency, and investor protection.

In contrast, decentralized finance relies much less on centralized authorities. Platforms like Aave, Uniswap, and MakerDAO use blockchain networks such as **Ethereum** to enable lending, trading, and stablecoin issuance through distributed governance structures like decentralized autonomous organizations (DAOs). This innovation has drawn interest from traditional institutions. Central banks such as the U.S. Federal Reserve are researching blockchain technology and there is rising global interest in central bank digital currencies (CBDCs). Well-known Tradfi institutions such as JP Morgan and Visa are exploring how to use some of the technological components of DeFi to increase transaction speed and cater to new customers within their own Tradfi ecosystems.

Background

TradFi's roots date back to ancient trading and lending practices, which evolved significantly after the rise of modern banking in 17th-century Europe. Globally, by the 20th century, highly regulated institutions such as banks, investment firms, and stock exchanges dominated, becoming key to financial stability and economic growth. Central banks took responsibility for oversight and intervention during financial crises.

Bitcoin's emergence in 2009 laid the groundwork for decentralized financial transactions, but the full potential of decentralized finance came into focus with Ethereum's launch in 2015. Ethereum introduced programmable smart contracts for blockchains, enabling innovative platforms like MakerDAO and Uniswap to emerge between 2017 and 2020. These platforms allowed users to directly lend and trade digital assets, not having to access any financial institution. DeFi grew rapidly but has faced significant regulatory scrutiny and concerns about security vulnerabilities. Despite these challenges, TradFi and DeFi are increasingly interconnected, with various TradFi institutions exploring blockchain technology and many DeFi platforms adopting measures to support regulatory aims like illicit finance prevention and cybersecurity resilience.

Policy and Regulation Issues

Regulation is fundamental to traditional finance, as it safeguards stability and consumer protection. Institutions adhere to strict requirements, including maintaining capital reserves, undergoing audits, and complying with AML/CFT laws. Oversight from bodies like the SEC and global organizations such as the Financial Stability Board mitigates risks but can also slow or even disincentize innovations that could improve business

productivity and customer access.
In contrast, decentralized finance operates in a separate, software-based ecosystem, enabling rapid innovation and inclusivity but exposes users to risks like fraud, hacking, and illicit fund flows. DeFi is incredibly dependent on the precision and security of its blockchain code; minor flaws in a highly liquid digital asset platform can lead to catastrophic financial consequences. This presents an ongoing concern as cyber-attacks become increasingly sophisticated. As the technology evolves and grows in use, regulators are likely to seek frameworks and guardrails to address the many novel applications within DeFi networks.
In December 2023, the Financial Stability Board in collaboration with the International Organization of Securities Commissions (IOSCO), presented policy recommendations to address market integrity and investor protection surrounding DeFi. The recommendations cover six areas: understanding DeFi arrangements and structures, achieving common regulatory standards, identifying key risks, developing clear disclosure, enforcing applicable laws, and improving cross-border cooperation.
The future likely involves blending TradFi's compliance measures with DeFi's innovation, creating a balanced financial ecosystem that fosters trust and broad accessibility.

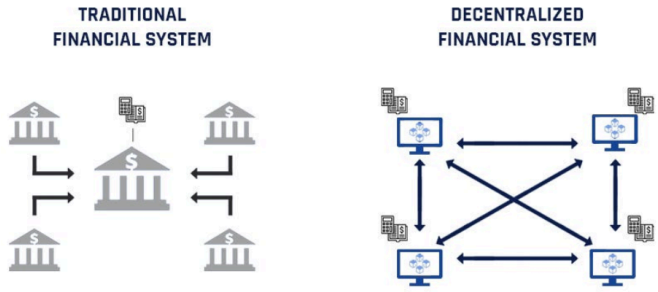

Image courtesy of Stably. (September 19, 2019). Understanding the Differences Between Decentralized Finance and Traditional Finance [Video]. Streaming Service. https://www.youtube.com/watch?v=1Nl6bTrc3gY

Decrypting Crypto:
Digital Asset Exchanges

Edited by Yaya J. Fanusie, Visiting Fellow
Written by David Lee, Research Assistant

Key Insight

Digital asset exchanges are central to the acquiring and trading of crypto assets. Anti-money laundering regulations in the U.S. are clear for most exchanges, but some regulatory uncertainty around some issues persists.

Summary

Digital Asset Exchanges are platforms that allow users to buy, sell, or swap **blockchain**-backed assets by keeping a record of ownership and facilitating the change of custody of digital assets. There are two types of Digital Asset Exchanges: **Centralized Exchanges (CEXes)**, which handle user funds and facilitate trade, and **Decentralized Exchanges (DEXes)**, which facilitate trades via contracts stored on a blockchain that is automatically executed when predetermined conditions are met. DEXes do not take custody of users' funds when facilitating trades.

Key Facts

Centralized Exchanges (CEXes) are intermediaries that act similarly to stock exchanges and hold **private keys** and funds on behalf of digital asset traders. Popular CEXes provide higher liquidity and are typically more user-friendly than Decentralized Exchanges. However, like the early bitcoin exchanges, CEXes are the target of hackers and users risk losing their investments. Notable CEXes are Binance, Bybit, and Coinbase.

Decentralized Exchanges (DEXes) are automated platforms that facilitate digital asset trade through smart contracts on blockchain networks. DEXes' users retain control of their digital assets providing a higher level of security and privacy. However, DEXes have lower liquidity and are still susceptible to vulnerabilities in smart contracts that could be exploited by hackers. Notable DEXes are Uniswap, SushiSwap, and THORChain.

Key Institutions

Financial Crimes Enforcement Network (FinCEN) supervises digital asset exchanges that are money transmitters and subject to the Bank Secrecy Act (BSA). The BSA requires such exchanges to register with FinCEN as money service businesses and implement Anti-Money Laundering (AML) and Know Your Customer (KYC) procedures. In addition, both the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) claim jurisdiction over regulating digital asset exchanges.

Background

When Bitcoin first launched in January 2009, there were only two ways to obtain it: by using computer power to verify blockchain transactions and earn bitcoins in a process called mining or arranging a peer-to-peer (P2P) trade with someone who owned bitcoins. P2P requires a high level of trust between parties to ensure that each party would fulfill the transaction. As interest in Bitcoin grew, the demand for a simpler way to obtain it grew. In March 2010, BitcoinMarket.com launched as the first Bitcoin exchange website. The

centralized exchange introduced a floating exchange rate, which provided real-time price conversion between Bitcoin and U.S. Dollars (USD) determined by supply and demand. However, due to recurring problems with fraud, PayPal blacklisted the exchange in October 2010, leading to its collapse.

Fraud and other illicit activities continued to haunt subsequent centralized exchanges, which stored the private keys for users' digital wallets on their company servers. One exchange, Mt. Gox, which once accounted for between 70% to 80% of Bitcoin trades, filed for bankruptcy in February 2014 after hackers stole 850,000 Bitcoin. Following the Mt. Gox hack, several major exchanges including Poloniex, Bitfinex, Bitstamp, Binance, Bithumb, and ShapeShift also had significant crypto funds stolen off of their centralized servers, giving popularity to the mantra, "not your keys, not your crypto."

In July 2015, the Ethereum blockchain was launched, introducing smart contracts, and decentralized applications (dApps). Smart contract programmability made it possible for Ethereum developers to create decentralized exchanges where users would control their private keys so that their funds would not be vulnerable to hacks on CEXes. Smart contracts also made it easier for people to create new cryptocurrency tokens, laying the groundwork for the Initial Coin Offering (ICO) boom. Between 2017 and 2018, more than 2,000 unique tokens were created, raising more than $10 billion.

However, scams and fraud proliferated around these ICOs, attracting scrutiny from U.S. financial regulators and law enforcement.

The U.S. has had a robust anti-money laundering (AML) regulatory framework for centralized exchanges since 2013. However, rules relating to cryptocurrency investment markets are less clear. In November 2022, FTX, the third-largest exchange at the time, collapsed after questionable management practices and insufficient reserves for withdrawals instigated a liquidity crisis. FTX's collapse caused shockwaves throughout the industry, inviting regulatory scrutiny and calls to create a clearer regulatory framework for cryptocurrency markets.

Policy and Regulation Issues

Digital Asset Exchanges face numerous policy and regulatory challenges. Key issues include:

- Money Transmitter Definition: Some legal disputes exist over whether DEXes can be considered money transmitters and how they may or may not fit under the BSA. Classifying a truly decentralized exchange platform as a money transmitter would bring regulatory challenges since it operates without an intermediary entity that can fulfill BSA obligations.
- Regulatory Classification of Digital Assets: As aforementioned, both the SEC and CFTC claim jurisdiction over digital assets as the SEC classifies digital assets as securities, while the CFTC classifies digital assets as commodities. This leads to overlapping and unclear responsibilities.

Decrypting Crypto:
Smart Contracts

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Julen Payne and Stella Millspaugh, Research Assistants

Key Insight

Smart contracts enable expansive programmability within blockchains, offering complex digital transactions and applications in decentralized platforms. There is significant work in the crypto space to improve and accelerate the use of blockchain smart contract usage, but regulatory and legal issues need to be sorted out for wider adoption.

Summary

Smart contracts are self-executing digital contracts, or agreements, on a blockchain that are automatically executed when certain conditions are met. In principle, they are the same as traditional contracts, except the terms are established and executed as code on a blockchain that cannot be altered after deployment. A key feature of smart contracts is their programmability, which allows contract creators to define complex requests and behaviors directly within the contract code. They are typically used for decentralized applications available to any blockchain user who fulfills the requirement for executing the contract. The purpose is to remove the need for a trusted third party or intermediary to enforce the terms of the contract between actors.

Key Facts & Considerations

- Blockchain smart contracts are not legally binding unless explicitly linked to a legal agreement operating in the real world. There is significant legal and policy work needed, likely including major legislation, in order to enforce blockchain smart contracts within the legal system.
- All smart contracts deployed on a permissionless blockchain can be viewed publicly by users to ensure their legitimacy, and they are not editable after being deployed.
- While any smart contract can be launched on a permissionless blockchain, users should be careful to ensure that all smart contracts they interact with are professionally audited by reputable third parties to ensure legitimacy, cybersecurity, and freedom from bugs. Although legitimate, high-quality blockchain projects conduct code audits as a best practice, there currently are no agreed-upon code auditing standards for smart contract development.

Key Institutions

- Chains: Ethereum, Solana, Binance Smart Chain, TRON, Arbitrum
- Research: Ethereum Foundation, Consensys, MIT Digital Currency Initiative, Chainlink Labs
- Companies: Chainlink, Uniswap, Aave, MakerDAO
- Auditors: Trail of Bits, OpenZeppelin, Zellic, Consensys

Background

Smart contracts were introduced as a concept by the mathematician Nick Szabo in 1994. However, the Ethereum blockchain was the

first software protocol to offer a simple yet dynamic way of creating digital contracts. The simplest and most apparent usage of smart contracts was for financial transactions, allowing two parties to exchange monetary value online without a central authority to oversee transactions. While Bitcoin was the first blockchain software protocol, its coding does not support complex digital contracts. Ethereum allowed a wider range of smart contracts to be developed and deployed on the blockchain itself, including smart contracts that create new tokens.

Key Benefits

- Instantaneous peer-to-peer execution without traditional settlement delays
- Collateralized, real-time lending without intermediaries
- Token creation and programmable issuance for various use cases
- Seamless transfer of asset ownership across blockchain networks
- Digital assets securely locked in neutral custody

Policy and Regulation Issues

Legal frameworks around smart contracts have yet to develop in full and the technology faces challenges around regulation and enforcement. Smart contracts on blockchains may not necessarily be recognized by the real-world court system, and recent government actions have raised complex legal questions that are still being litigated. For example, in recent years the United States Department of Justice has announced criminal cases that have sought to put certain non-custodial smart contract protocols under the definition of a money-transmitting business under Section 1960 of the Bank Secrecy Act (BSA). While money transmitters are generally defined as entities that transfer funds on behalf of the public or facilitate transactions in exchange for a fee, many smart contracts operate without custody of user funds or centralized control. This raises questions about how such protocols align with existing regulatory definitions and where legal responsibility should be assigned in decentralized systems. Some legal issues are being clarified, however. A U.S. federal court ruled in early 2025 that immutable smart contracts on blockchains can not be considered property because they technically can not be controlled or owned by anyone.

Real World Analogy

Aave is a decentralized cryptocurrency lending platform that allows people to take out loans from pooled crypto that others have invested for liquidity purposes. Users who lend their money to Aave earn interest on their deposits. Smart contracts in the platform guide each step of the activity. When taking out a loan, borrowers have to submit some form of collateral in the case that they cannot pay back their loan. If the value of the collateral falls below a certain threshold set by the smart contract, the collateral is automatically liquidated to repay the loan.

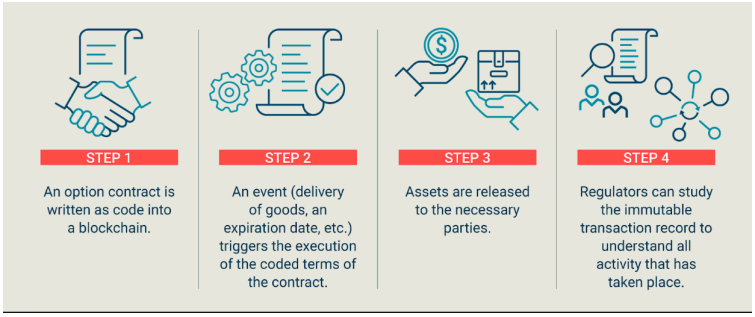

Image Courtesy of Szakiel, Patrick. How Smart Contracts Are Changing the Way We Do Business. 2022. G2, https://www.g2.com/articles/smart-contracts.

Decrypting Crypto:
Illicit Finance

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Kelly Grace Richardson, Research Assistant

Key Insight

Enforcing AML/CFT regulations in the cryptocurrency industry strengthens financial oversight by requiring KYC procedures, transaction monitoring, and sanctions compliance. However, jurisdictional inconsistencies and evolving tactics by illicit actors present ongoing challenges, requiring continuous adaptation and international collaboration by law enforcement.

Summary

The implementation of **Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)** regulations in the cryptocurrency industry has significantly reduced illicit financial activity by enforcing KYC procedures, transaction monitoring, and sanctions compliance. However, evolving tactics by illicit actors and jurisdictional inconsistencies pose challenges to regulators, requiring constant adaptation and international collaboration. Cryptocurrencies, powered by blockchain technology, allow for decentralized transactions without traditional financial intermediaries. However, their pseudonymous nature has raised concerns regarding illicit financial activities. To combat these risks, regulatory agencies like the **Financial Crimes Enforcement Network (FinCEN)** in the United States have imposed Anti-Money Laundering and Combating the Financing of Terrorism AML/CFT) requirements on cryptocurrency businesses, treating centralized exchanges as money service businesses (MSBs) subject to financial reporting obligations. These regulations require **Know Your Customer (KYC)** procedures, transaction monitoring, and reporting of suspicious activity to detect and prevent financial crimes. However, enforcement remains a complex issue due to the evolving tactics of illicit actors and the global nature of digital assets.

Key Facts

Cryptocurrency exchanges operating as money transmitters in the United States are required to implement KYC procedures, collecting personal information such as names, addresses, and government-issued identification to verify customer identities. Exchanges and other **virtual asset service providers (VASPs)** must also file **Suspicious Activity Reports (SARs)** and **Currency Transaction Reports (CTRs)** for transactions exceeding regulatory thresholds. Additionally, the **Office of Foreign Assets Control (OFAC)** enforces compliance with sanctions, requiring crypto exchanges to screen transactions against the **Specially Designated Nationals (SDN) list** to prevent illicit financial flows to sanctioned entities. The transparency of blockchain transactions has enabled the development of analytics tools that assist regulators and law enforcement in tracking suspicious activity and prosecuting illicit actors. These measures have strengthened financial oversight whilepreserving the benefits of blockchain technology.

Key Institutions

The Financial Crime Enforcement Network (FinCEN), a bureau within the U.S. Treasury

Department, enforces AML/CFT regulations, including for the cryptocurrency sector. Blockchain analytics firms like Chainalysis, Elliptic, and TRM Labs have developed tools to trace illicit transactions and support compliance efforts. Other major cryptocurrency exchanges such as Coinbase, Binance, and Kraken have implemented regulatory measures to align with AML/CFT requirements, supporting the interests of both consumers and regulators.

Background

The U.S. has been a pioneer in developing AML/CFT frameworks for the cryptocurrency industry. In 2013, FinCEN released its first guidance clarifying that cryptocurrency exchanges fall under MSB regulations, requiring compliance with financial reporting laws. This early regulatory approach helped shape global AML/CFT policies, influencing the **Financial Action Task Force (FATF)** to establish international standards for virtual asset service providers (VASPs) in 2019. These frameworks have been essential in reducing the percentage of illicit transactions occurring through U.S.-based cryptocurrency platforms compared to global averages.

Policy and Regulation Issues

The primary regulatory challenge in the cryptocurrency space around financial crime is the inconsistency across jurisdictions. Other challenges include the ever-evolving illicit finance methodologies and concerns over balancing financial transparency with user privacy. While the U.S. has led global AML/CFT policy development, regulatory clarity on whether certain digital assets are classified as securities or commodities remains in contention. The industry is also facing the creation of privacy-preserving technologies that may complicate enforcement efforts. As regulatory agencies refine their approaches, collaboration between all stakeholders will be essential in mitigating illicit finance risks while supporting the continued growth of the cryptocurrency ecosystem.

Glossary

Algorithmic Stablecoin: A type of cryptocurrency token that uses an algorithm to adjust supply and demand dynamically to maintain price stability.

Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT): A set of regulations designed to prevent financial crimes by requiring businesses to implement compliance measures.

Asset-Referenced Tokens (ARTs): Stablecoins backed by a mix of assets, such as multiple currencies, commodities, or financial instruments, to distribute risk.

Bitcoin: The first cryptocurrency, which also was the first practical application of blockchain technology, launched in 2009 by the pseudonymous software developer Satoshi Nakamoto.

Blockchain: A digital, decentralized public ledger that records transactions across a network of computers, known for its immutability, security, and transparency.

Centralized Exchanges (CEXes): Intermediary platforms that hold private keys and funds on behalf of digital asset traders.

Consensus Mechanism: A software program in which computer nodes in of a distributed ledger system agree on the correctness of a new block before it is added to the chain of records on the network.

Cross-Border Payments: Payments that involve transactions between parties in different countries.

Currency Transaction Report (CTR): A mandatory report filed for transactions exceeding a certain threshold.

Decentralized Autonomous Organization (DAO): A blockchain-based entity governed by rules encoded in smart contracts, managed collectively by its members without centralized authority. DAO decisions are made through voting mechanisms, which are usually tied to members' token ownership, and operates without centralized authority or government interference.

Decentralized Exchanges (DEXes): Software platforms that facilitate digital asset trade through smart contracts on blockchain networks.

Decentralized Finance (DeFi): Innovative approach to banking and financial services centered on peer-to-peer transactions powered by blockchain technology.

Distributed Ledger Technology (DLT): Technological infrastructure and protocols that enable simultaneous access, record validation, and immutable record updating across a network that is dispersed across numerous entities and multiple locations. A distributed ledger is a digital system that does not have a central data store or management features, in contrast to traditional databases.

Double-Spending Problem: The ability to reuse the same digital token or asset for multiple online transfers by manipulating a transaction record; a key issue preventing the success of internet-based currency before Bitcoin.

Electronic Money Tokens (EMTs): EMTs is a classification introduced under the European Union's Markets in Crypto-Assets Regulation (MiCA) and refers to stablecoins pegged to a single fiat currency, regulated as electronic money, and requiring issuers to hold liquid reserves to ensure redemption at par value. This term is specific to the EU regulatory framework and is not commonly used in the United States, where a unified regulatory classification for stablecoins has yet to be established.

Glossary

Ethereum: The second-largest cryptocurrency by market capitalization, Ethereum is a blockchain network that securely executes smart contracts without third-party involvement. Participants transact through smart contracts, with senders "signing" transactions by spending Ether, the network's native currency. Its flexible software and smart contract capabilities have enabled the development of a wide variety of applications across numerous industries.

Fiat-Backed Stablecoin: A cryptocurrency token that is fully backed by reserves of fiat currency or cash equivalents, ensuring a fixed price or value.

Financial Action Task Force (FATF): An international organization that sets global AML/CFT standards, including guidance for regulating cryptocurrency businesses and virtual assets.

Financial Crimes Enforcement Network (FinCEN): A bureau of the U.S. Department of the Treasury responsible for enforcing AML/CFT regulations and ensuring financial institutions comply with reporting obligations.

Know Your Customer (KYC): A process that requires companies to verify the identities of their customers by collecting personal information such as names, addresses, and government-issued identification.

Liquidity Pool: A crowdsourced collection of cryptocurrencies locked into a smart contract to facilitate transactions. These pools provide the funds needed to execute trades or exchanges within a network, ensuring smooth and efficient operations. Users contribute their own cryptocurrency to the pool and, in return, earn rewards or a share of trading fees as an incentive for supplying liquidity.

Mining: The use of computer processing power to solve cryptographic puzzles required to maintain and secure blockchain networks. This process is also called “proof of work” and results in the addition of a new block of records to the blockchain and rewards the miner with cryptocurrency.

Money Service Business (MSB): A category of financial institutions that are required to register with FinCEN and implement AML/CFT compliance programs.

Non-Fungible Tokens (NFTs): Unique digital assets stored on a blockchain, primarily used to verify ownership and authenticity, often used for creative works like music or art.

Office of Foreign Assets Control (OFAC): A U.S. Treasury agency that enforces economic and trade sanctions.

Privacy-Preserving Technologies: Cryptographic tools such as privacy coins and decentralized mixing services that enhance user anonymity but may also complicate regulatory enforcement.

Private Keys: An alphanumeric code used to authorize transactions and prove ownership of a blockchain asset.

Protocol: A basic set of rules that allows data to be shared between multiple computers; in crypto, the protocol establishes the blockchain system for recording and transferring digital assets on the internet.

Settlement: The completion of a financial transaction, where the asset or funds have moved from the originator’s account to the beneficiary’s account.

Smart Contracts: Digital contracts programmed on a blockchain that are automatically executed when predetermined terms/conditions are met.

Specially Designated Nationals (SDN) List: A list maintained by OFAC identifying individuals and entities subject to economic sanctions due to their involvement in illicit

activities or threats to national security.
Suspicious Activity Report (SAR): A report that companies must file with regulators when they detect transactions that may indicate illicit financial activity.
Virtual Asset Service Provider (VASP): A business that facilitates the exchange, issuance, or hold of digital assets.