

Blockchain, Crypto, and Household Financial Security

An Introductory Guide for Policymakers and the Social Sector



April 2023

**FINANCIAL
SECURITY**
PROGRAM
aspen institute

Purpose of this Guide

In 2022, cryptocurrency went mainstream.

Millions of people -- including disproportionate numbers of Black consumers -- purchased cryptocurrencies for the first time. The scale and swiftness of this development in so many Americans' financial lives prompted us at the Aspen Financial Security Program to set out to learn more and to begin to seek answers to key questions that might ultimately shape our point of view on what is required to ensure that the cryptocurrency and blockchain ecosystem is both safe and structurally inclusive. Ultimately, we seek to answer a fundamental question:

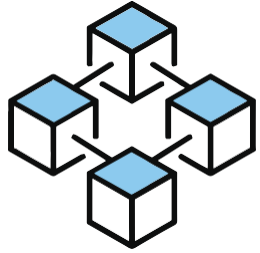
What do crypto and the blockchain mean for the financial security of people in America?

Our own learning journey continues as the crypto and blockchain space continue to evolve at lightning speed. In partnership with Humanity Forward, we offer this guide as a learning “short-cut” for other social sector leaders who may benefit from:

1. An overview of the basics of this new ecosystem
2. Key use cases that illustrate how the blockchain might shape households' financial lives
3. A set of key questions and considerations for how we shape and regulate this ecosystem in service of financial security

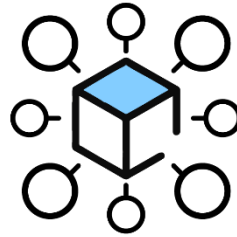
What's in this Guide and How to Use It

This short guide is organized into 3 sections to support policymakers and social sector leaders to develop their understanding of how blockchain, cryptocurrency (“crypto”), and distributed ledgers could impact household financial security, as follows:



1. Blockchain Basics

Learn about the infrastructure that powers the blockchain and how people access the blockchain ecosystem via crypto wallets and exchanges to buy/sell assets like crypto, tokens, and NFTs.



2. Decentralized Finance ("DeFi") Financial Products

How a new suite of financial products are emerging on the blockchain, designed without the need for an intermediary or issuing bank.



3. Blockchain as Regulatory Technology (Regtech)

How blockchain may deliver gains in operational efficiency and security for companies and impacts household financial security.

Each section of this guide explains key concepts, provides examples, and lists key questions that policymakers may face in shaping the development of the blockchain ecosystem toward one that drives stronger, more inclusive financial outcomes for all families in America.



David Derryck
Entrepreneur-In-Residence at the
Aspen Institute Financial Security Program

[Aspen Profile](#) | [Connect on LinkedIn](#)



Mack Wallace
Fellow and Senior Policy Advisor for
Inclusive Financial Systems at the Aspen Institute

[Aspen Profile](#) | [Connect on LinkedIn](#)

About the Aspen Institute Financial Security Program

The Aspen Institute Financial Security Program's (Aspen FSP) mission is to illuminate and solve the most critical financial challenges facing American households and to make financial security for all a top national priority. We aim for nothing less than a more inclusive economy with reduced wealth inequality and shared prosperity. We believe that transformational change requires innovation, trust, leadership, and entrepreneurial thinking. FSP galvanizes a diverse set of leaders across the public, private, and nonprofit sectors to solve the most critical financial challenges. We do this through deep, deliberate private and public dialogues and by elevating evidence-based research and solutions that will strengthen the financial health and security of financially vulnerable Americans.

To learn more, visit AspenFSP.org, join our mailing list at <http://bit.ly/fspnewsletter>, and follow [@AspenFSP](https://twitter.com/AspenFSP) on Twitter.

Acknowledgements

The Aspen Institute Financial Security Program would like to thank David Derryck and Mack Wallace for authoring this guide, as well as Karen Andres, Sohrab Kohli, Tim Shaw, Ida Rademacher, Kate Griffin, Noha Shaikh, and Faye Steele for their insights and contributions.

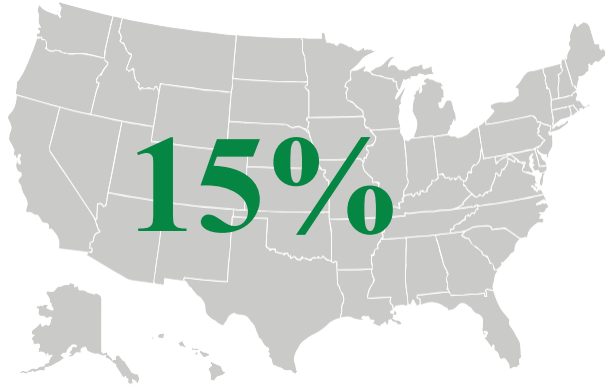
The Aspen Institute Financial Security Program would like to thank Humanity Forward for their support of this project.

Background: The Rise of Crypto and the Blockchain



Crypto and blockchain technology are growing in popularity in the United States

By the Numbers



Harris Poll: **15% of U.S. adults** own some form of cryptocurrency, with **23% of African Americans** having an ownership stake.¹



\$1 trillion

\$1 trillion is the market capitalization of the cryptocurrency market.²



295 Million Users

As of January 2022, the number of cryptocurrency users worldwide is approximately 295 million.³

Decision makers focused on Americans' financial security need to understand what blockchain is – and what it might mean in the future

The first blockchain, Bitcoin, debuted in 2008. What started as a single application has, over the last 15 years, developed into a global phenomenon.

But what is it? What does this technology mean for financial services? How about household finances?

Blockchain represents a new type of system – one with its own ecosystem, its own players, and its own linkages to the financial system, real economy, and people's lives. It represents more than just a 'digital asset' – it offers technological capabilities that allow for a new framework for ownership and record keeping of all types of assets – tangible, intangible, or digital.

Crypto, short for cryptocurrencies, became the first popularized use case of blockchain. Crypto is a 'digital asset' native to a blockchain and, along with tokens and NFTs, is one of several different types of assets whose ownership can be recorded and tracked on a blockchain.

Applications and smart contracts built using the blockchain are already powering the next generation of financial services and products, and new use cases beyond finance such as commerce, sustainability, and transportation.



Blockchain applications could impact all three pillars of Americans' financial security

FINANCIAL SECURITY



NEW CASH FLOW

Potential for new cash flow and wage-generating economic activities enabled in the blockchain economy.

Potential for faster (i.e., real-time) access to earned wages via blockchain smart contracts.



TOKENIZED ASSETS

All types of tangible and intangible assets can be tokenized and thereby monetized - introducing new potential benefits and risks.

Digital assets like cryptocurrencies represent a new store of value to save and invest in.



DELIVERY OF BENEFITS

Blockchain infrastructure could change the tools that people use to access or manage their financial lives, including the delivery of employer and government benefits.

In addition to the purchase of cryptocurrency, blockchain technology is starting to be used 'in the background', in ways that could impact Americans' financial security.

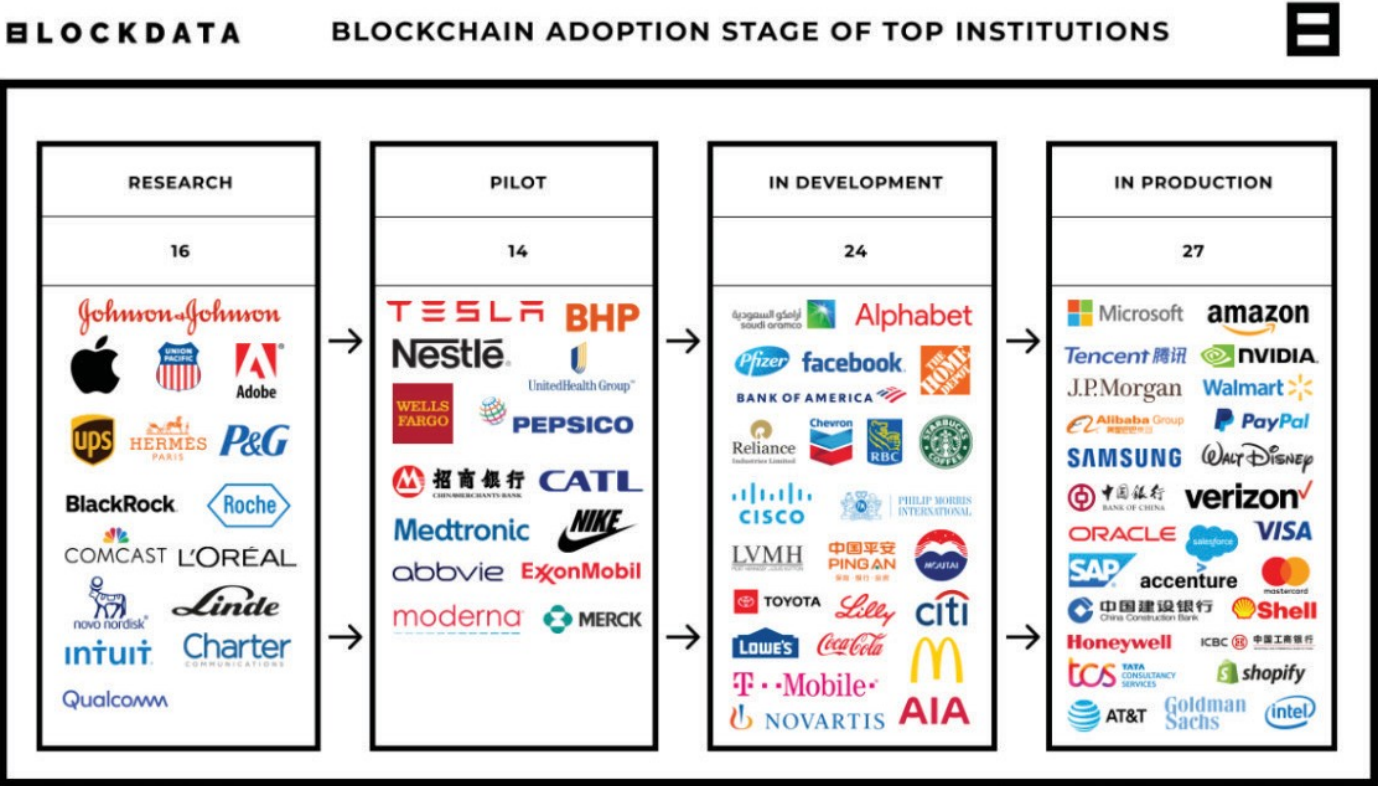
As consumers and employees, people in the United States increasingly interact with blockchains through their purchases and employers. Behind the scenes, U.S. businesses are experimenting with blockchain to help improve:

- 1. Operational Efficiency** → Driving down costs in supply chains and in the production of a range of goods and services leading to lower prices, automation of labor, or both
- 2. Cybersecurity** → Protecting people from financial losses caused by fraud and data security breaches
- 3. Legal Contracts** → Establishing undisputed asset ownership and dividing ownership of physical assets



Many people may be surprised to know they already interact with companies using blockchain technology within their operations

Eighty-one of the top 100 publicly traded companies are using blockchain technology.⁴



BLOCKDATA IS A CB INSIGHTS COMPANY

WWW.BLOCKDATA.TECH | INFO@BLOCKDATA.TECH



SECTION ONE

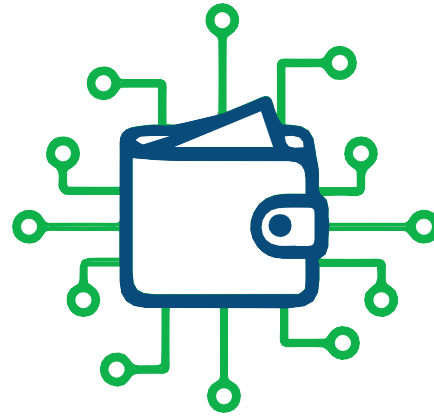
Blockchain Basics: People, Blockchain Technology, and Their Money



Breaking Down the Blockchain Ecosystem into 3 Key Pieces



I. The Infrastructure that Powers the Blockchain



II. The Crypto Wallet and the Exchange: How People Access the Blockchain Ecosystem



III. How People May Use the Blockchain Ecosystem Today & In the Future

We'll go step-by-step into each of these pieces and explore definitions, concepts, and implications for Americans' financial security.

1. The Infrastructure that Powers the Blockchain

Key Blockchain Infrastructure Concepts

- The purpose of a blockchain network is to record and track the movement of tokens, which represent tangible, intangible, or digital assets, and whose ownership is recorded on individual “blocks.”
- **Blockchain** is a shared, immutable ledger that consists of a growing list of records, called “blocks,” that are securely linked together using cryptography (“crypto”).
- Each blockchain is composed of a series of individual ‘blocks,’ which together are referred to as the “ledger.”
- A **distributed ledger** is a specific type of blockchain that uses peer-to-peer (P2P) networks to create and operate a shared blockchain that is geographically distributed and decentralized across many participants.
- **Cryptocurrencies, tokens, and NFTs** are all types of tangible and intangible assets whose ownership is recorded and tracked on the blockchain.
- Most public blockchains get funded through an “Initial Coin Offering” (ICO) which functions similar to a stock market “Initial Public Offering” (IPO).





The purpose of a blockchain network is to record and track the movement of tokens, which represent assets

Blockchains issue “tokens” to track various assets. Blockchains can track all types of asset ownership, including:

1. Tangible assets, such as cash, a house, or manufactured goods
2. Intangible assets, such as intellectual property, patents, or copyrights
3. “Digital assets” which are native to the blockchain itself, such as cryptocurrency

Cryptocurrencies are issued directly from the blockchain. Through cryptography, tampering or revision of individual blocks in the blockchain is detected and prevented.



Each blockchain is composed of a series of individual ‘blocks,’ which together are referred to as the ‘ledger’

Look closely, and you’ll see that a blockchain is composed of a series of individual “blocks.” Together, these blocks add up and are referred to as the “ledger.” Each individual block contains three key elements:

1. A cryptographic “hash” (a unique digital fingerprint)
2. A time stamp
3. The encoded transaction data describing the details of the transaction

Over time, these blocks build into a ledger which track the changes in ownership of whichever asset the blockchain was designed to record.



A distributed ledger is a specific type of blockchain that uses peer-to-peer (P2P) networks to create and operate a shared blockchain that is geographically distributed and decentralized across many participants

Key Points:

- Any participant can review the ledger and no entity controls the ledger.
- Within this decentralized network, participating computers, referred to as “nodes,” collectively store and share files.
- P2P networks are what enable the transfer of assets without the need of an intermediary of a central server.
- Decentralized ledgers are more resilient (e.g., than a centralized database) because they do not have a central point of failure.
- Increasingly, these distributed ledgers are also being recognized as legal entities.⁵

The Infrastructure that Powers the Blockchain

1 Money (IOUs) or any digital assets that hold value such as contracts, media, IP, agreements or software applications



2 Transaction, execution of a contract, execution of an app or consumption of media



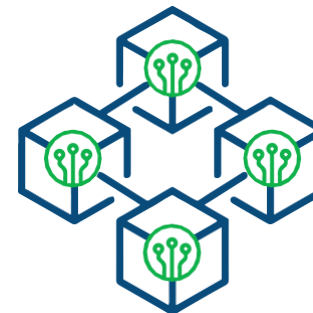
3 The block is broadcast to every party in the network



4 Those in the network approve the transaction is valid



5 The block then can be added to the chain, which provides an indelible and transparent record of transactions



6 Transaction gets executed and the digital asset holding value officially transfers



Cryptocurrencies, tokens, and NFTs are the most common types of assets recorded and tracked on the blockchain



Cryptocurrencies

- Native asset of, and issued directly from, a specific blockchain. For example, Bitcoin is the native currency for the Bitcoin Blockchain. Similarly, Ethereum is the native currency for the Ethereum blockchain.
- Behave like money, meaning they can be used as a medium of exchange or as stored value.

Tokens

- Applications built on top of blockchains and can represent any type of asset.
- Tokens are programmable via software protocols and “smart contracts” (i.e., programs that run when predetermined conditions are met).
- Tokens are transparent – meaning the protocols and transactions are viewable to all – and permissionless, meaning there is no central authority that grants approval or restricts their usage.

NFTs

- Short for non-fungible token, an NFT is a specific type of token.
- NFTs establish indisputable digital proof of ownership of an underlying asset.
- No two NFTs are exactly alike and each can only be officially owned by a single person. As such, NFTs can counter fraud and forgery and can be used as a certification.

NFT sales amounted to \$18.5B in 2021 (a 570x increase over 2020); monthly sales hit a high of \$4.5B in January before declining in line with the overall crypto correction in spring 2022.⁶

Most public blockchains get funded through an ‘Initial Coin Offering’ (ICO)



- Like an IPO, a set number of tokens on the blockchain are minted and available.
- After the ICO, the public blockchain continues to expand through “miners” who provide computing power to the blockchain in exchange for tokens.
- Companies then take these proceeds and fund “projects” that are submitted by developers and voted upon by a governance committee or community members, depending on the blockchain’s governance structure.

Examples of popular ICOs



E O S

Raised over \$4.2B from its ICO



Tezos

Raised \$232M from its ICO

Key Blockchain Infrastructure Risks

Key Risks

- **Consumer Protection:** blockchain networks support a range of consumer use cases, some envisioned and others yet to be, that cross the jurisdiction of various regulatory authorities. Ambiguity or inconsistent oversight can result in consumer exposure to new types of risk and fraud.
- **Money Laundering & Sanctions Evasion:** the global and decentralized nature of blockchain networks differs from current payment, banking, and other financial networks where there are no network operator(s) to oversee.
- **Energy Consumption:** some types of blockchain networks are more energy intensive (e.g., proof of work) while others are less energy intensive (e.g., proof of stake)
- **Lack of Legal Recognition:** blockchains can track all types of assets but can be limited in value if there is not also formal, legal recognition of the ownership of the physical or intangible asset.



Key Blockchain Infrastructure Questions for Policymakers

Key Questions

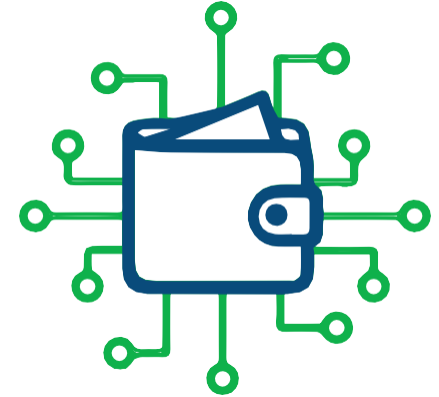
- How should regulatory jurisdiction be governed for blockchains, given that blockchains represent a range of different types of tangible, intangible, or digital assets – and are cross-border networks?
- How should disclosures of risk apply to blockchains, given the broad access to blockchains available to consumers (via crypto ownership, NFT ownership, and other projects) that they are unlikely to fully understand?
- How should sanctions policies (e.g., anti-money laundering and anti-terrorism financing) evolve to restrict or blacklist decentralized protocols?
- What are the climate and energy implications for operating different types of blockchains (e.g. proof of work vs. proof of stake)?
- What ownership, licensing, and intellectual rights should be legally conferred upon NFTs?
- How should NFTs be treated by securities law as a means of asset ownership?



2. The Crypto Wallet and The Exchange: Accessing the Blockchain

Key Crypto Wallet & Crypto Exchange Concepts

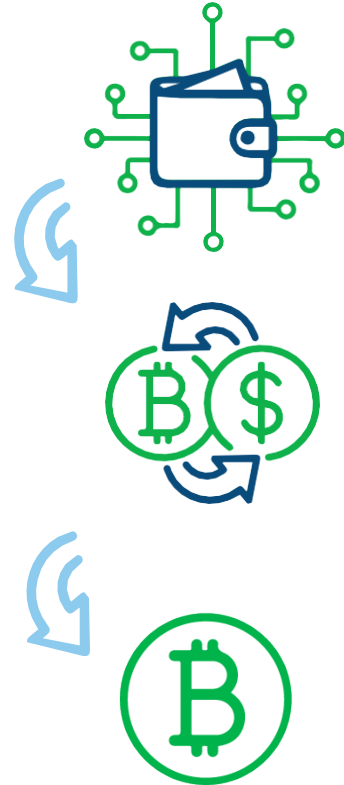
- Crypto wallets allow regular people to participate and use the blockchain to make transactions, often using exchanges as the facilitating intermediary.
- The purpose of the crypto wallet is to store the “keys” which prove ownership to token(s) or cryptocurrency within the blockchain.
- There are two types of crypto wallets: custodial and non-custodial.
- An exchange is the intermediary that helps people buy and sell tokens and cryptocurrencies.
- Exchanges often provide custodial wallets like stock brokerages do; however, assets held in crypto wallets by crypto exchanges are commingled with the exchange’s assets and do not offer investor protections like a bank or brokerage account.



This is How People Can Engage with the Blockchain Ecosystem



DeFi applications (dApps) provide blockchain-enabled financial products, including stablecoins, lending and borrowing, and payments.



The **crypto wallet** is a person's gateway to the ecosystem, holding assets much like a physical wallet.

Exchanges act as an intermediary, facilitating buy/sell of various assets, holding the assets in custodial crypto wallets, and allowing cash in/cash out of the ecosystem on behalf of people and institutional investors.

Cryptocurrency

Tokenized Physical Assets

NFTs
(Tokenized Digital Assets)

Blockchains are used to track and record ownership of various tangible, intangible, and digital assets.



The purpose of the crypto wallet is to store the ‘keys’ which prove ownership to token(s) or cryptocurrency within the blockchain

A crypto wallet does not directly store the actual token or cryptocurrency; instead, crypto wallets store the keys needed to prove ownership and make transactions.

Every crypto wallet stores three important pieces of information:

I. Your private key	The private key is a randomly generated 256-bit integer used to digitally sign your transaction.
II. The public key	The public key is randomly generated using a second type of cryptography to verify your digital signature.
III. The blockchain address	The blockchain address is unique and is used to identify the owner. It is comparable to an account number corresponding to block(s) on the blockchain. Different blockchains have different address lengths, but all addresses are alphanumeric.

Wallets need both the private key and public key in order to complete and record a transaction. It is only after the private key is validated that a transaction gets recorded to the blockchain.

In instances where the user does not have a crypto wallet and the person loses their keys, the person permanently loses access to their assets.



There are two types of crypto wallets: custodial and non-custodial

	Custodial Wallets	Non-custodial Wallets
Control	Relies on Third-Parties and Exchange A company keeps and maintains control of your tokens and/or crypto on your behalf.	Owned & Controlled by User User is entirely responsible for their private keys. If they lose their private keys, they lose access to their wallet.
Customer Value	Convenience Best for users that value ease of use.	Security Best for users that value security and full control of their own wallet and its assets.
Popularity	Most Popular People are most familiar with this method from traditional financial services.	Limited Popularity Requires technical know-how of software-based wallets or hardware wallets.
Used For	Cryptocurrencies, NFTs, and established blockchain use cases	Cryptocurrencies, NFTs, and DeFi applications For trading and participating in DeFi applications, a non-custodial account is almost always required.



Crypto wallets vary in the specific kinds of assets they can hold

While all crypto wallets allow you to store tokens and cryptocurrencies, each crypto wallet varies in the specific kinds of assets they can hold.

A physical wallet accepts any kind of currency. Meanwhile, a crypto wallet can only accept specific types of cryptocurrencies or tokens based on the network the wallet is associated with. There are ongoing efforts to enable more interoperability.



Metamask is the leading wallet for Ethereum and Ethereum-based tokens. They had over 10M monthly average users in August 2021.

An exchange is the intermediary that helps people buy and sell tokens and cryptocurrencies



Exchanges represent a **principal entry point** through which cash and fiat currency can be converted to and from the blockchain ecosystem, and across blockchains.








Each exchange differs in the assets supported, transaction types, fees, payment methods for money in or money out, and in their security to protect from breaches or stealing of people's assets.

Global crypto exchanges typically comply with Know Your Customer/Anti-Money Laundering (KYC/AML) rules, providing a level of market trust.



Exchanges operate 24/7 and the largest, Binance, has volumes in excess of \$11B in a single day⁷



# ▲	Exchange	Trading volume(24h)	Weekly Visits ⓘ	# Markets	# Coins	Fiat Supported
1	 Binance 	\$11,891,484,829 ▼ 17.94%	15,046,498	1689	386	AED, ARS, AUD and +43 more ⓘ
2	 Coinbase Exchange	\$1,258,091,940 ▼ 19.14%	959,236	598	232	USD, EUR, GBP
3	 Kraken	\$1,044,991,199 ▼ 1.58%	774	990,352	714	217 USD, EUR, GBP and +4 more ⓘ
4	 Binance.US	\$209,181,339 ▼ 28.78%	433,833	313	147	USD
5	 KuCoin 	\$451,311,162 ▼ 22.86%	1,916,603	1391	769	USD, AED, ARS and +45 more ⓘ

Data from December 2022



Exchanges commingle assets held in customer wallets with their own. If the exchange fails, a customer is not protected and can lose all their assets

- Exchanges often provide a custodial wallet to customers. These wallets provide a means of holding the token or cryptocurrency purchased or sold.
- Opening an account with an exchange is akin to an online brokerage platform (e.g., for stocks, mutual funds, and ETFs).
- A crypto exchange operates similarly to the Nasdaq or NYSE. Instead of investment products, these exchanges provide the tools to buy and sell tokens and cryptocurrencies. Exchanges can facilitate frequent trading or buy-and-hold strategies.

However, unlike traditional stock exchanges or brokerages, crypto exchanges are **not members of SIPC** (the Securities Investor Protection Corporation) and a person's wallet assets are commingled with the exchange's assets. **As a result, a person could lose all their assets as unsecured creditors if the exchange should fail or get hacked.**

Exchanges in the News



Prominent crypto exchange FTX failed and declared bankruptcy in November 2022. Customers with wallets at FTX stand to lose billions given that their assets were uninsured. The failure of FTX resulted in a chain reaction that also brought down BlockFi, Celsius, and Genesis.

Crypto Exchange Key Risks & Policy Questions

Key Risks

- Consumer Protection: a person can lose all their assets held in their crypto wallet as an unsecured credit if an exchange should fail or get hacked.
- Investor Protection: investors on crypto exchanges are not insured against failures or loss.

Key Questions

- What consumer protections should be provided to people who hold assets in custodial or non-custodial wallets?
- What level of legal responsibility should exchanges have to their customers?
- How important is wallet interoperability between blockchains as a policy objective?



3. How People Use the Blockchain Ecosystem Today & In the Future

Key Concepts

- Blockchain and crypto could directly impact Americans' financial security, both through changes in cash flow and asset ownership.
- This impact is expected to grow in the years ahead as more applications are created and adoption spreads.



By 2030, is real-time payroll the norm?

Potential Future Use Case

Meet Anna

A middle-aged retail worker in suburban Texas

Today, like many, Anna is paid every two weeks. However, she sometimes needs money sooner to meet her financial obligations. To do that, Anna uses Early Wage Access providers to get an “advance” on her paycheck. Depending on the EWA provider and her employer, Anna may be charged a fee and is limited in the amount that she can access.

In the future, companies may have eliminated the need for EWA providers because they utilize real-time payment protocols. In the future, Anna could receive her paycheck as she earns it in real-time (minute by minute, hour by hour, day by day). At the end of every shift, Anna might receive a notification that her pay has been deposited into her account. The funds would be immediately deposited in stablecoins via the blockchain and she would then be able to access them using her debit card immediately. By using a real-time payment protocol via blockchain she might be able to improve control over her cashflow and weather smaller shocks more easily.



The photos used in the Potential Future Use Case slides are stock photographs and do not depict actual people or their financial situations.

By 2030, will blockchain protect and monetize intellectual property for creators and freelancers?

Potential Future Use Case

Meet Sam

A young graphic designer living in urban California

Today, creators like Sam, who include musicians, journalists, and designers, use different platforms to sell their work. Sam's work has a watermark and licensing restrictions for how that work can be used personally and commercially. However, once purchased, Sam cannot easily track usage or licensing adherence. In fact, Sam has seen his work on platforms and websites that he is not affiliated with. Yet the cost of addressing the situation is too expensive for him.

In the future, the blockchain might enable Sam to secure and monetize his creations in the form of an NFT. When a person licenses Sam's work, a transaction is recorded to the blockchain indicating who licensed it as well as the digital address of where the work is being used. With an NFT, Sam's work would effectively be digitally copyrighted. In addition, Sam could set up the NFT to pay him royalties automatically via a smart contract associated with his NFTs every time his works are downloaded and used on platforms, including photo stock image libraries.

The photos used in the Potential Future Use Case slides are stock photographs and do not depict actual people or their financial situations.



By 2030, will the blockchain ecosystem promote community development and create new pathways to home ownership?

Potential Future Use Case

Meet Lane

In her early 30's and looking to purchase her first home

Lane rents a unit in a triplex. She has been saving to buy a house but a traditional starter home remains outside her financial means.

In the future, real estate might be tokenized by converting the value of the real estate into a token stored on a blockchain, enabling digital ownership and transfer. These divisible tokens would each present a fractional share of ownership stake in that real estate. The owner, who lives in a unit and rents one to Lane and one to another person, tokenizes the property. The owner would sell Lane tokens representing the unit she currently occupies and retain the tokens for the remaining unit in order to maintain financial flexibility. Lane would have purchased her starter home and the homeowner would have monetized a part of their real estate asset.



The photos used in the Potential Future Use Case slides are stock photographs and do not depict actual people or their financial situations.

SECTION TWO

"DeFi": The New Suite of Blockchain- Enabled Financial Products





Decentralized Finance, or ‘DeFi’, Describes the Full Range of Financial Services that use Blockchain

DeFi financial products include saving, borrowing, lending, paying, investing, and insuring and rely on the blockchain rather than a bank or other centralized authority to provide the financial product.

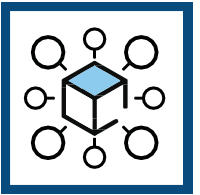
Potential Value of DeFi

- Lower cost, higher yields → without intermediaries, cost savings in the form of higher yields or lower rates could be passed on directly to people.
- Smart contracts → are readily executable.

State of Play

- There are more than 3,000 dApps across 20 categories.⁸
- The market value of DeFi dApps is greater than \$100B.⁹

DeFi provides access to traditional financial services and enables new ones



Key Concepts

- DeFi represents a new suite of blockchain-enabled financial services that build upon traditional financial products, introducing new concepts such as staking and yield-farming.
- DeFi financial products are often referred to as “dApps” or decentralized applications built as “smart contracts.”
- At their simplest, dApps offer financial services like savings accounts. At their most complex, dApps offer more exotic financial products like options and derivatives
- Once a user uses a wallet to move fiat currency into the blockchain ecosystem, DeFi becomes accessible.



DeFi products are being built to satisfy household financial needs

The modern financial system is generally composed of 5 types of consumer finance products. DeFi seeks to replicate current functionality and build upon each of them:





Financial Product Type	How it Works with DeFi
Short-term savings	Transfer funds into stablecoins.
Long-term savings	Lend digital assets (crypto currencies, tokens, or NFTs) via yield-farming, or yield-staking. Purchase index funds, earning returns on underlying DeFi assets.
Credit	Borrow using digital assets as collateral.
Payments	Instantaneous settlement of funds.
Insurance	Instantaneous settlement and execution via smart contracts.

Stablecoins are used to facilitate usage of all 5 types of financial products



Stablecoins facilitate the usage of DeFi financial products

- A stablecoin is a type of currency whose value is pegged to an underlying asset. That asset can be a fiat currency, a commodity or other cryptocurrency.
- When a stablecoin is pegged to a single cryptocurrency or basket of cryptocurrencies, the stablecoin is often overcollateralized—meaning the value of the cryptocurrency is typically higher than the value of the stablecoin due to current volatility in cryptocurrency valuations.
- In contrast, when the stablecoin is pegged to a fiat currency like USD, the stablecoin maintains close to a 1:1 ratio. Stablecoins have found their strongest first use case in facilitating lending and borrowing in crypto, as stablecoins provide people stability in the underlying asset and smart contract for people to transact.¹⁰

Name	Market Cap ⓘ
 Tether USDT	\$68,437,764,707
 USD Coin USDC	\$45,002,947,709
 Binance USD BUSD	\$21,620,875,129
 Dai DAI	\$6,477,872,984

Data as of October 2022



DeFi enables instant collateral-based lending

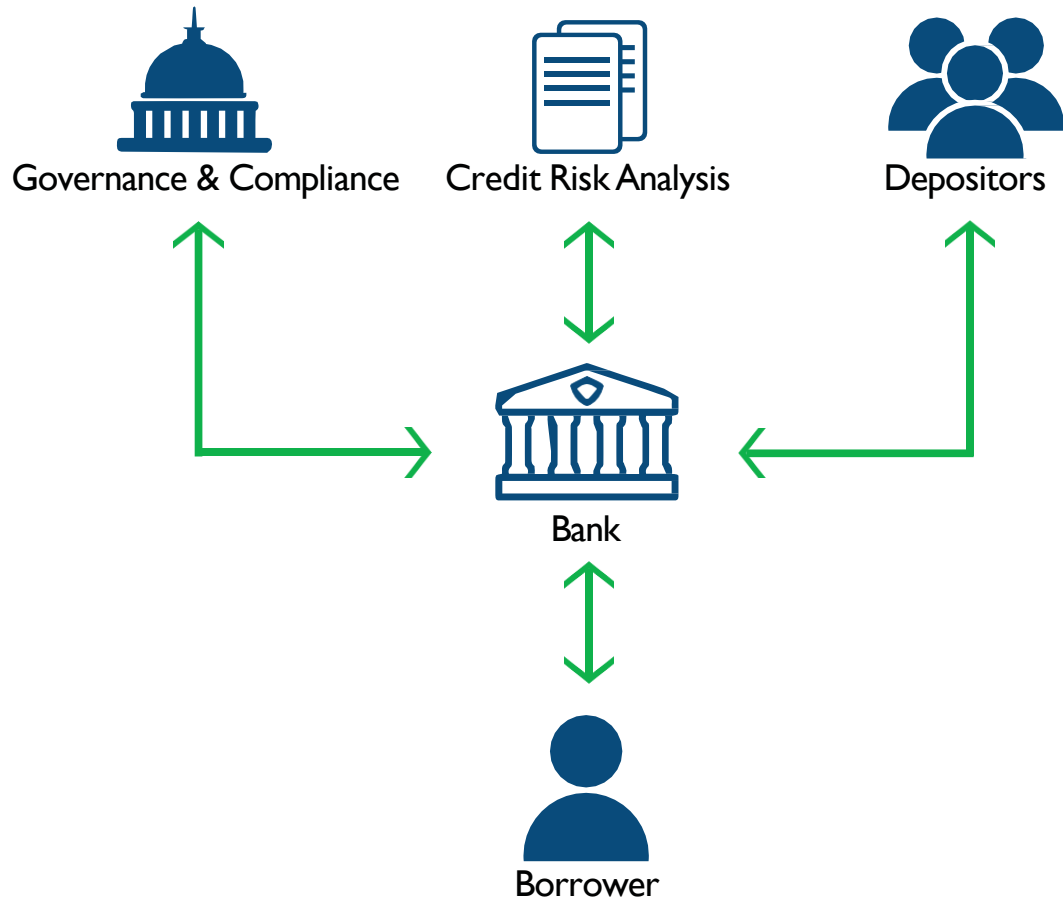
- A person can borrow funds, utilizing their cryptocurrency as collateral for a loan. Unlike traditional financial services, these dApps are permissionless, meaning an individual does not need a bank account or good credit.
- A second differentiating factor between DeFi and traditional financial services is the time frame: borrowers and lenders may have contracts that last as little as minutes.
- The source of the borrowed funds comes from either people or companies pledging their cryptocurrency to lending pools and earning interest on funds that are borrowed. This is also referred to as “yield farming” and is explained on slide 42. Borrowers pay interest on funds borrowed, much like a traditional loan.
- People who take on a DeFi loan can be exposed to new types of risk. For example, a user is exposed to counterparty-risk for lending directly to another user. There is also the risk of overindebtedness by either the borrower or lender if the value of the collateral falls. To mitigate the risk of default, most all DeFi loans today are overcollateralized or use stablecoins as collateral.

Examples of Popular Platforms

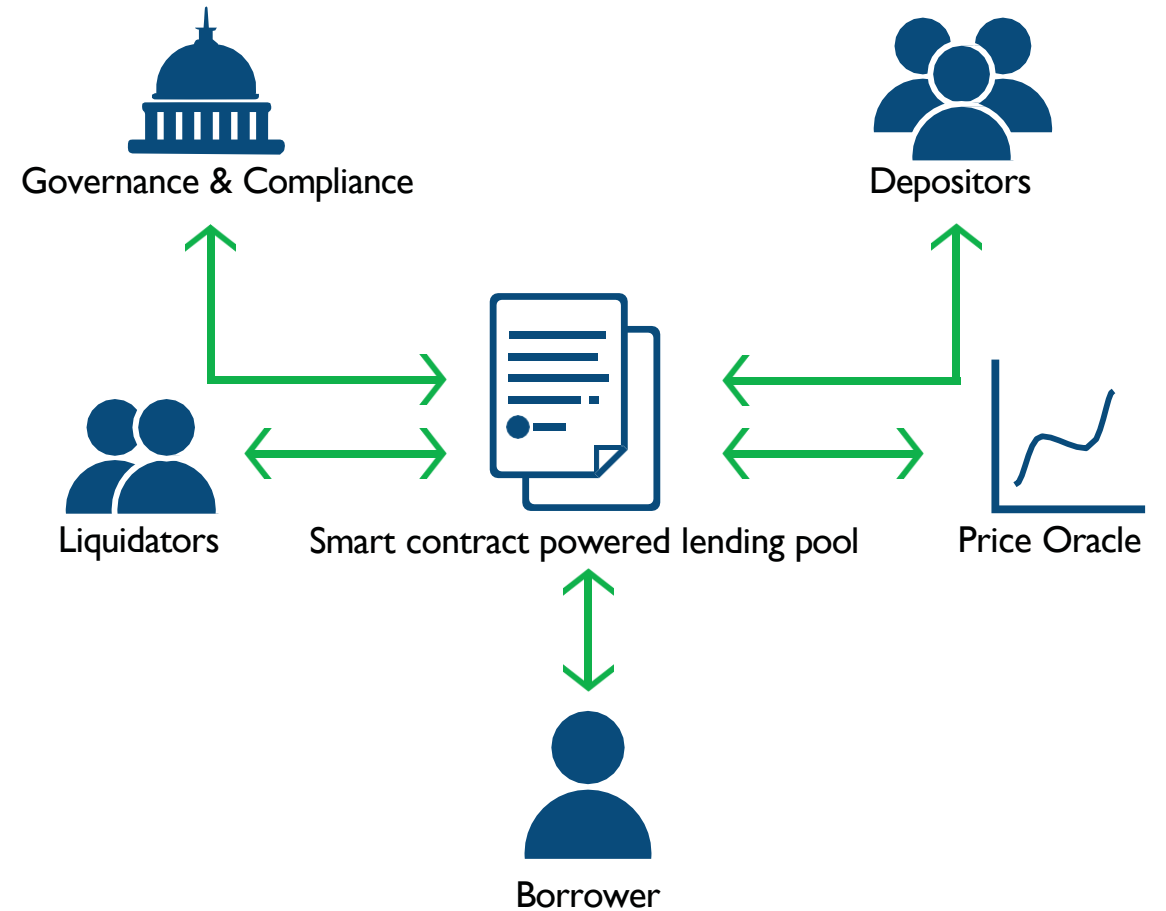
(by MakerDAO)

How is DeFi Lending Different from Traditional Lending?

Traditional Lending



DeFi Lending



A price oracle is a pre-determined source of price data that is used as a reference to help establish a price for DeFi transactions that do not occur directly on the blockchain and for where there may not be an exact market price.



Traditional Loan vs DeFi Loan

Traditional Finance Loan	DeFi Collateralized Loan
<p>A Borrower applies for a loan for fiat currency from a traditional financial institution.</p>	<p>Borrower requests a loan for one or more digital assets, typically a USD stablecoin, from the asset pool of a DeFi platform governed by a smart contract.</p>
<p>The financial institution reviews the Borrower’s identity, assets and liabilities, credit scores, zip codes, and other personal information in order to approve or deny the application.</p>	<p>The smart contract “tells” the Borrower the required collateral in the form of digital assets (cryptocurrency, NFT) needed for the loan amount. Currently, the collateral is often worth more than the loan being requested.</p>
<p>Approval/Denial decisioning is typically measured in days and if approved, the financial institution makes a loan of fiat currency to the applicant with repayment terms and is assigned any necessary collateral in the form of a lien or security interest.</p>	<p>If the collateral-to-loan ratio is met approval is measured in seconds. The smart contract holds the collateralized assets and makes a loan in the form of one or more digital assets -- but usually a stablecoin.</p>
<p>If Borrower defaults on the loan, the financial institution can exercise its lien or security interest rights, engage in debt collection, report late payments to credit agencies, or file a lawsuit.</p>	<p>If the collateral-to-loan ratio drops below a specified amount, the smart contract liquidates collateral to pay off debt.</p>



Traditional Loan vs DeFi Loan

DeFi's intended goals:

- DeFi can eliminate or significantly reduce transaction fees charged by banks and other financial institutions
- DeFi is permissionless—anyone with internet access can use it and its products without securing approval from a central authority (traditional financial institutions)
- Digital assets can be transferred in a matter of seconds

There is potential for DeFi lending to provide access to useful, affordable financial products and services to more people. Current traditional financial services do not adequately meet the needs of many citizens, especially those with low or volatile incomes. DeFi offers the potential for a new method to provide secure financial products using permissionless networks. While this potential may exist, DeFi is not there yet.

In its current form, DeFi's benefits are also some of its barriers to financial inclusion. For instance, due to the volatility of digital assets (primarily cryptocurrencies) most loans are overcollateralized by 120%-150% to account for the value in fluctuating collateral. While this is beneficial to the lender from a risk perspective, it requires the borrower to have more assets. However, if we begin to tokenize real world assets, the pool of collateralizable assets may increase and we could see collateralized prices become more muted.



DeFi payment protocols enable recurring payment streams, instant settlement, and micro-amounts

Payments were the first use case for cryptocurrencies and continue as a key means to transfer value between two or more parties. In the fiat currency ecosystem, cash is permissionless and anonymous. Once cash becomes a check or money transfer, it must be settled through a central authority. Bitcoin was designed as an open finance ecosystem to allow for P2P transfer.

DeFi payment dApps build on this intention by allowing the transfer of value to be permissionless and trustless across the blockchain ecosystem without need for an exchange (i.e., truly decentralized). New payment dApps seek to allow recurring payments streams on a predetermined time increment (second, minute, hour, etc.) or milestones, at any amount.

Examples of DeFi payment platforms



Celer



Two ways people can earn passive income and save on the blockchain

1. How staking provides a short- and long-term savings opportunity

- People can pledge and lock up their crypto to help validate transactions and add new blocks to the ledger of blockchains designed as “proof-of-stake.”
- People are rewarded with more crypto tokens from the blockchain, typically earning a percentage of the platform’s fees.
- The lock-up period and the fixed rate of interest are known in advance. Similar to a CD, a person tends to earn more the longer they commit their crypto.

2. How yield farming provides savings opportunity for active investors

- People can earn income by providing their crypto to DeFi dApps, typically to lending pools that provide DeFi loans and earn interest from borrowers.
- Funds remain highly liquid with few dApps requiring a lock-up period. Users can instantly move in and out of DeFi protocols in search of the highest yield for their money.
- Interest rate yields are dynamic, variable, and constantly changing so a user must monitor their rate of return. The total return is unpredictable and not known in advance.



People can also purchase investment products like DeFi index funds and more complex swaps

DeFi companies are also replicating traditional investment products, including:

- **Index funds:** tracking the overall value of the crypto or NFT markets
- **Derivatives:** perpetual crypto futures, or a futures contract with no expiration date, have gained in popularity as crypto traders seek to track the underlying value of a cryptocurrency

By 2030, will the DeFi ecosystem will be used to tokenize real-world possessions for crypto-based loans?

Potential Future Use Case Meet Sarah

She works part-time for Uber, DoorDash, and TaskRabbit in urban Florida

Today, like millions of workers, Sarah is employed as a gig worker, employed across several tech platforms on a contract basis. While she enjoys the flexibility, her monthly income is highly variable. Her unpredictable income makes it hard to get approved for a traditional loan.

In the future, Sara might tokenize her major possessions, including her car, home appliances, and prized jewelry, onto the blockchain. She could use these tokens as collateral to secure a DeFi short- term personal loan. She might use these DeFi products whenever she needs 1-3 weeks' worth of income to bridge gaps in her cash flow to meet her rent, utility, or other financial obligations. In the future, DeFi loan products could be readily accessible via a mobile app and would potentially have lower interest rates and fees as compared to payday, pawn, or title loans.



The photos used in the Potential Future Use Case slides are stock photographs and do not depict actual people or their financial situations.

DeFi Key Risks & Policy Questions

Key Risks

- **Failures & Bankruptcies:** a failure in one area can cause contagion to other parts of the ecosystem through counter-party relationships not fully seen or understood.
- **Consumer Protection:** a product failure can result in a person losing their assets. Further, a person may lack sufficient understanding of a DeFi product's terms, risks or benefits given these are new types of financial products, creating opportunities for bad actors or predatory practices. The ability to collateralize new types of real-world assets for lending amplifies these risks.

Key Questions

- What risk do failures of DeFi dApps pose to the safety and soundness of the overall financial system, now or in the future?
- What do failures of DeFi dApps mean for consumers?
- How should the consumer protection framework be updated to account for DeFi products? In particular, what are the risk implications of allowing people to tokenize and collateralize more of their assets to obtain credit?
- What types of disclosures and rules would enable stronger investor and consumer protections?
- How should consumers be protected or educated about permissionless activities?



SECTION THREE

Blockchain as RegTech and Cybersecurity Tool



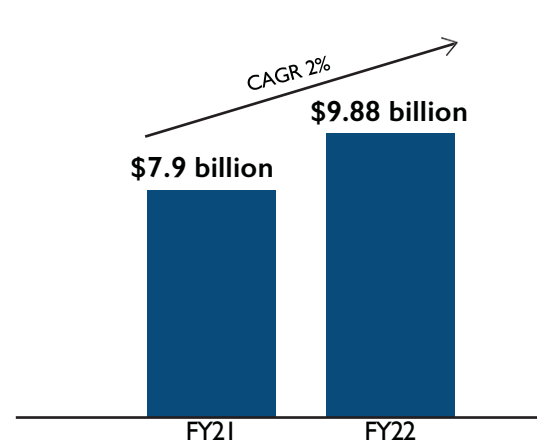


Regtech, or Regulatory Technology, is a Fast-Growing Force in Financial Services

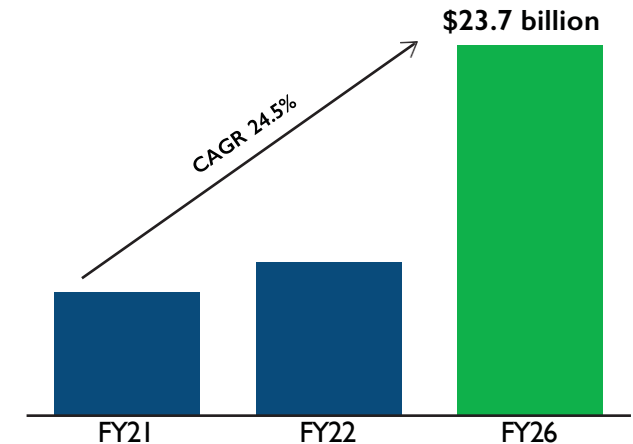
RegTech is the management of regulatory processes using smart technology by companies.



Global financial institutions spent \$213.9 billion on AML compliance in 2021.¹²



The global regtech market is expected to grow from \$7.9 billion in 2021 to \$9.88 billion in 2022 at a compound annual growth rate (CAGR) of 25.1%.¹³



The market is expected to grow to \$23.76 billion in 2026 at a CAGR of 24.5%.¹⁴

Blockchain-enabled regtech solutions can drive down cost and provide permissionless digital verification solutions



Key Concepts

- Blockchain as a regtech solution can facilitate more cost-efficient AML and KYC, with substantial opportunity for savings.
- Blockchain solutions can assist in more efficient and transparent record keeping.
- Blockchain solutions can mitigate fraud and assist in transaction monitoring.

Blockchain as a regtech solution can facilitate more cost-efficient AML and KYC



The immutable ledger for cryptocurrency and token ownership and transactions provides for incontrovertible transaction tracking and ownership tracking. At the same time, the historical record of the ledger supports record keeping and blacklist screening at scale.

Blockchain also holds promise to make true the goal of empowering users to provide verifiable, self-permissioned data, bypassing third-party data gatekeepers or systems. Each time a KYC transaction occurs at a participating institution, the most up-to-date information is entered into the shared distributed ledger, allowing different institutions to rely on the same checks and information up to a certain level.

However, the anonymity of many public blockchains can hinder KYC efforts, a key challenge in the deployment of the technology for this use case.

Trulioo offers identity verification for people in over 40 countries.



Blockchain as a regtech solution can also aid in record keeping requirements and can play a role in monitoring transactions to prevent fraud



As part of their compliance activities, companies must maintain records that they have appropriately screened new clients. Blockchain-based regtech companies could provide a solution that tracks individuals that have had a compliance screening, makes that ledger available to other platforms, and updates as new blocks are added to the chain. This would effectively allow multiple institutions to rely on the same source, thus reducing cost and increasing speed.

As the volume of transactions increases across different blockchains and DeFi applications it will be incumbent on those platform operators to provide safe and sound platforms. Regtech companies are using machine learning and artificial intelligence to observe transaction data and develop algorithms that would detect suspicious and/or red flag activities.

Chainalysis uses blockchain to combat money laundering, fraud, and compliance violations in the cryptocurrency sector.



Trustev delivers fraud prevention solutions online by scanning transactions in real time to determine their legitimacy.



Regtech Key Risks & Policy Questions

Key Risks

- AML/KYC: the immutable ledger can establish incontrovertible transaction and ownership tracking. However, the anonymity of public blockchains can also hinder KYC efforts.
- Identity: blockchain could enable additional private methods or forms of identification that may or may not reconcile with current methods.

Key Questions

- How does Regtech change the current implementation of AML/KYC compliance efforts utilizing blockchain technology?
- How does Regtech address issues of individual data sovereignty?
- How does Regtech address the development and implementation of new algorithms?
- How do regulators become users of Regtech themselves and keep current with developments in Regtech?



By 2030, could regtech and the blockchain be used to help people access public benefits?

Potential Future Use Case

Meet Judy

A single mom in her 50s who qualifies for nutrition assistance

Regtech holds the promise of being able to streamline access to benefits. Today, under traditional rules, every person is required to identify themselves for each new account and/or service provided (e.g., for WIC and SNAP). This places undue burden on the recipient.

In the future, the government might use the blockchain and regtech to streamline the enrollment process. In the future, Judy would:

- Establish her identity on the blockchain through her wallet and completing KYC/AML requirements. Judy's KYC/AML requirements would only be updated if there was a material change in her status.
- When Judy applies for her nutrition assistance she grants access to the presiding agency for them to confirm that her identity and credentials are current and valid.
- The agency checks the blockchain ledger, sees that her credentials are current and valid, and moves to the next step.

Such a system would reduce the burden of gathering identity documents such as utility bills, drivers license or state ID, checking OFAC lists, etc. for Judy and reduce the cost for the service providers.

The photos used in the Potential Future Use Case slides are stock photographs and do not depict actual people or their financial situations.



ENDNOTES

- 1 Laningham, Andrew, A Growing Number of U.S. Adults Invest In Cryptocurrency - Harris Poll, The Harris Poll, March 7, 2022
- 2 Cryptocurrency Market Capitalization, Slickcharts.com. October 16, 2022
- 3 Cryptocurrency Market Size Worth \$11.71 Billion By 2030, GrandView Research, September 2022.
- 4 Schweiger, Lucas, 81 of the Top 100 Public Companies are using blockchain technology, Blockdata, October 6, 2022
- 5 Select Committee on Blockchain, Financial Technology and Digital Innovation Technology, SF0038 - Decentralized autonomous organizations, Sixty-sixth Legislature of the State of Wyoming 2021 General Session, April 21, 2021
- 6 State of the NFT Market, Forkast News, March 2022.
- 7 Top Cryptocurrency Exchanges Ranked By Volume | CoinMarketCap, CoinMarketCap, November 29, 2022
- 8 Number of Blockchain Wallet Users 2022/2023: Breakdowns, Timelines, and Predictions - Financesonline.com, Finances Online, February 2021
- 9 DApp Statistics, State of the DApps, October 16, 2022
- 10 Chung, James, DeFi Market Commentary, Consensus, April 2022 and Top Stablecoin Tokens by Market Capitalization, CoinMarketCap, October 16, 2022
- 11 How Does DeFi Lending Work?, Appinventiv, August 16, 2022
- 12 Global Spend on Financial Crime Compliance at Financial Institutions Reaches \$213.9 Billion, LexisNexis, June 9, 2021.
- 13 RegTech Global Market Report 2022, ResearchAndMarkets, June 3, 2022
- 14 ibid.

Other References

[A simple explanation of how blockchain works](#) by Paul Dughi

[What is Blockchain](#) by World Economic Forum

[Blockchain—A Short and Simple Explanation with Pictures](#) by Adil Haris

[A Beginners Guide To Understanding The Layers Of Blockchain Technology](#)

[Blockchain & The Role of P2P Network](#) by Toshendra Kumar Sharma

[Cryptocurrencies vs. Tokens: Digital Assets | Gemini](#) by Cryptopedia

[Code, Speech, and the Tornado Cash Mixer | Electronic Frontier Foundation](#)

[Crypto Exchange Competitive Analysis](#) by Chainalysis

[State of Crypto Report 2022](#) by Gemini

[Non-Fungible Token \(NFT\): Overview, Evaluation, Opportunities and Challenges](#) by Qin Wang, et al.

Learn more about these topics from the following sources

RegTech

- [Anti-Money Laundering and Blockchain Technology](#)

DeFi

- [A Complete List of Stablecoins 2022](#)
- [Stablecoins Explained](#)
- [Value Proposition of Stablecoins for Financial Inclusion](#)
- [How DeFi Lending Works](#)
- DApp Statistics
- [Explore The World of Digital Profits with DeFi Lending and Borrowing Platform Development](#)
- [Real-World Use Cases for Smart Contracts and dApps](#)

Blockchain

- [Blockchain Use Cases](#)

DeFi Ecosystem

The DeFi ecosystem is currently composed of a mix of centralized and semi-decentralized applications. Centralized dApps are custodial and utilize centralized price feeds, liquidity, and interest-rate determination for borrowing/lending. Meanwhile, semi-decentralized dApps are non-custodial with price feeds, interest rates, and liquidity coming from multiple, independent sources. While the name “DeFi” invokes fully decentralized provision of financial services, there currently are no fully decentralized dApps operating.’

Deeper Focus: What is an NFT?

NFTs are a form of smart contract minted on the blockchain and the underlying smart contract of the NFT assigns ownership and transferability of the NFT. NFTs are unique and indivisible. Once an NFT has been minted and recorded on the blockchain, each subsequent transaction is recorded on the block chain making it part of the ledger and therefore visible and verifiable. NFTs are built in a specific standard which makes them interoperable between applications and platforms that accept that standard. The Ethereum blockchain is the dominant platform for NFTs but others include Solana and Ronin (home to Axie Infinity for gaming).

NFTs represent ownership of digital assets on the blockchain in the digital world. Their characteristics—unique, indivisible, verifiable—are consistent with the attributes of physical assets in the real world. As a result, it is now feasible to use an NFT to digitize physical assets in the real world and map them to the blockchain creating a digital record that can allow for value transfer between parties via the blockchain.

Glossary

- **AML/KYC** refers to the regulatory processes of identity and transaction verification of ‘Anti-Money Laundering’ and ‘Know Your Customer’.
- **Blockchain** is a shared, immutable ledger that consists of a growing list of records, called “blocks,” that are securely linked together using cryptography (“crypto”).
- **Crypto** is a native asset of, and issued directly from, a specific blockchain.
- **Crypto exchange** is the intermediary that helps people buy and sell tokens and cryptocurrencies.
- **Crypto wallets** store the keys needed to prove ownership and make transactions on behalf of the user.
- **dApps** or decentralized applications refer to DeFi financial products built as “smart contracts.”
- **Digital assets** are native to the blockchain itself and can be any digital representation of value such as cryptocurrency, NFTs and stablecoins.
- **DeFi**, short for decentralized finance, refers to a suite of blockchain-enabled financial products, including stablecoins, lending and borrowing, and payments.
- **Distributed ledger** is a specific type of blockchain that uses peer-to-peer (P2P) networks to create and operate a shared blockchain that is geographically distributed and decentralized across many participants.
- **Initial Coin Offering (ICO)**, similar to an initial public offering (IPO), a set number of tokens on the blockchain are minted and made available at its inception.
- **NFT** or non-fungible token is a specific type of token that establishes indisputable digital proof of ownership of an underlying asset.
- **Protocol** is software code that allows information to be shared across networks automatically and securely and provides instructions on how to function.
- **RegTech**, or regulatory technology, is the management of regulatory processes using smart technology by companies.
- **Price oracle** is a pre-determined source of price data that is used as a reference to help establish a price for DeFi transactions that do not occur directly on the blockchain and for where there may not be an exact market price
- **Smart contracts** are programs that run when predetermined conditions are met).
- **Stablecoin** is a type of currency whose value is pegged to an underlying asset. That asset can be a fiat currency, a commodity or other cryptocurrency
- **Tokenized** is the process of replacing sensitive data with nonsensitive unique identifiers “tokens”.