Osher Lifelong Learning Institute, Summer 2025
Cryptocurrencies & The Future of Money

University of Hawaii, Manoa

Host: Joan Nix
Professor, Queens College (CUNY)
June 30, 2025

Available NEED Topics Include:

- US Economy
- Healthcare Economics
- Climate Change
- Economic Inequality
- Economic Mobility
- Trade and Globalization
- Minimum Wages
- Immigration Economics
- Housing Policy
- Federal Budgets
- Federal Debt
- Black-White Wealth Gap
- Autonomous Vehicles
- US Social Policy

Course Outline

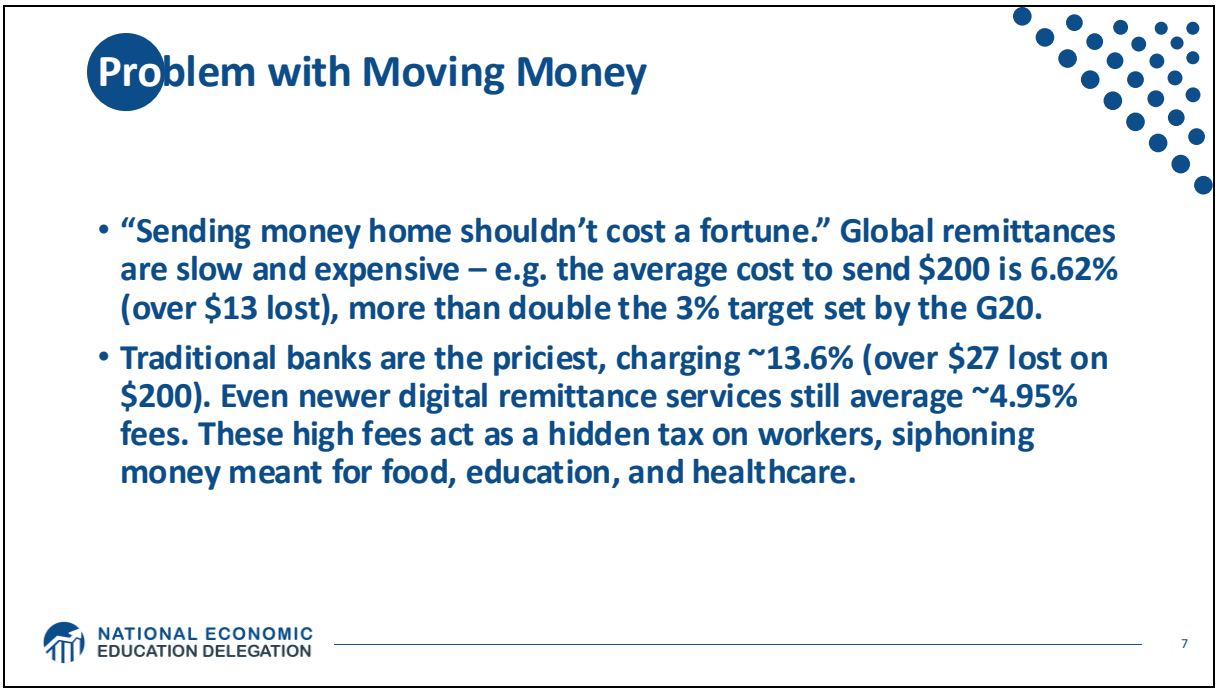
- **Contemporary Economic Policy**
  - Week 1 (6/2): Economic Update (Geoffrey Woglom, Amherst College)
  - Week 2 (6/09): Climate Change Economics (Sarah Jacobson, Williams College)
  - Week 3 (6/16): Economic Mobility (Jon Haveman, Exec Director, NEED)
  - Week 4 (6/23): Health Economics (Robert Rebelein, Vassar College)
  - **Week 5 (6/30): Cryptocurrencies (Joan Nix Queens College (CUNY))**

Submitting Questions

- **Submit questions in the chat or by raising your digital hand.**
  - I will try to handle them as they come up.
- **We will do a verbal Q&A once the material has been presented.**
- **Slides will be available from the NEED website tomorrow (https://www.needecon.org/delivered_presentations.php)**

Welcome! Over the next two hours, we're going on a journey to understand the world of cryptocurrency. Our path is designed to be logical and approachable, especially for those new to the topic. We won't delve into complex code or investment tricks; instead, we'll focus on fundamentals. First, **Why It Matters** – before defining cryptocurrency, we need to see the real-world problems it aims to solve (this is the "why" behind the technology). Next, **How It Works** – without confusing jargon. We'll use simple analogies and live demos to show the practical steps of using digital money. Then, an honest look at **Opportunities & Risks** – the incredible potential of this technology, and the serious dangers from volatility to scams. Finally, **The Bigger Picture** – we'll explore the broader crypto ecosystem beyond Bitcoin and how governments and institutions are responding. We'll end with a Q&A to address your questions. The goal today isn't to make you an expert, but to equip you with the knowledge to navigate this space safely and confidently.

Part 1 Why Crypto Matters To You



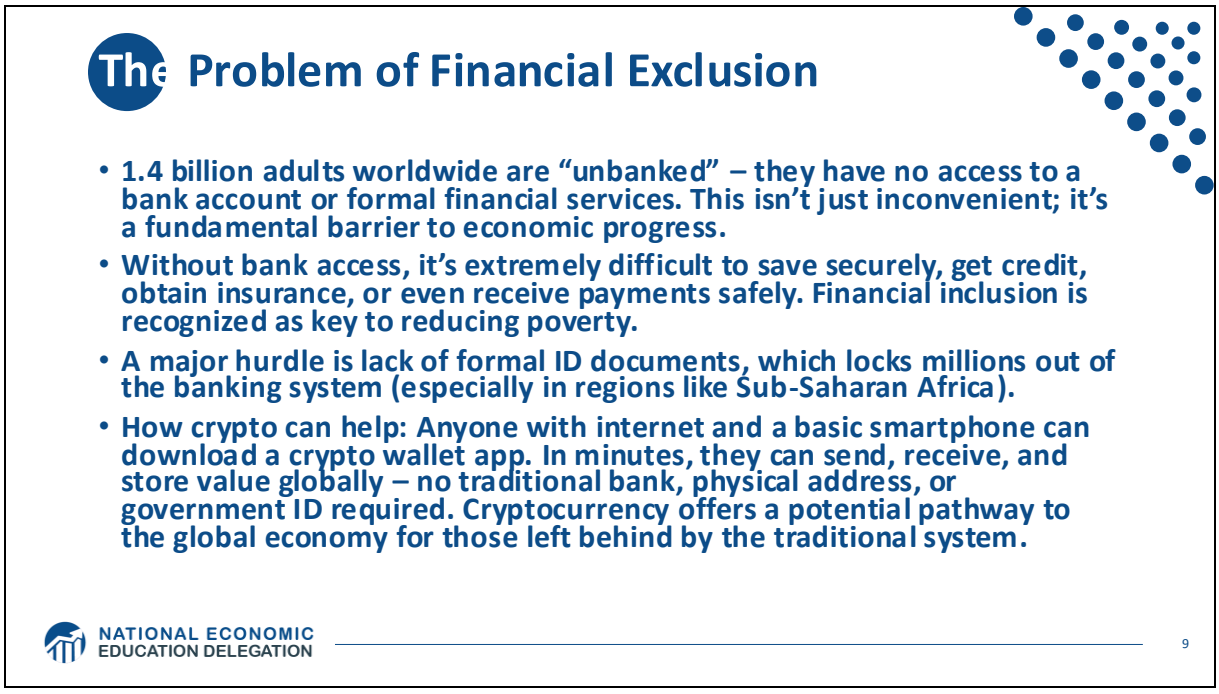
Let's start with a problem many people face: **sending money to loved ones across borders** (remittances). It's a lifeline for millions of families, yet the current system is often slow, inefficient, and costly. According to the World Bank, the **global average cost to send $200 was 6.62%** in Q3 2024. That means over $13 of that $200 never reaches the family it's intended for – more than double the G20's target of 3%. In fact, sending through a traditional bank is worst of all, with average fees around **13.64%**. Imagine losing over $27 just for sending your own money! Even modern digital services, while better, still take about 5%. These fees are essentially a **tax on the world's workers**, chipping away at funds meant for essentials like food, education, and healthcare. This painful friction in our global financial system is one of the first problems cryptocurrency advocates set out to solve.

Billion Adults Have No Access to a Bank

NATIONAL ECONOMIC EDUCATION DELEGATION

8

https://www.brinknews.com/bridging-the-digital-divide-to-widen-financial-services-in-central-asia/

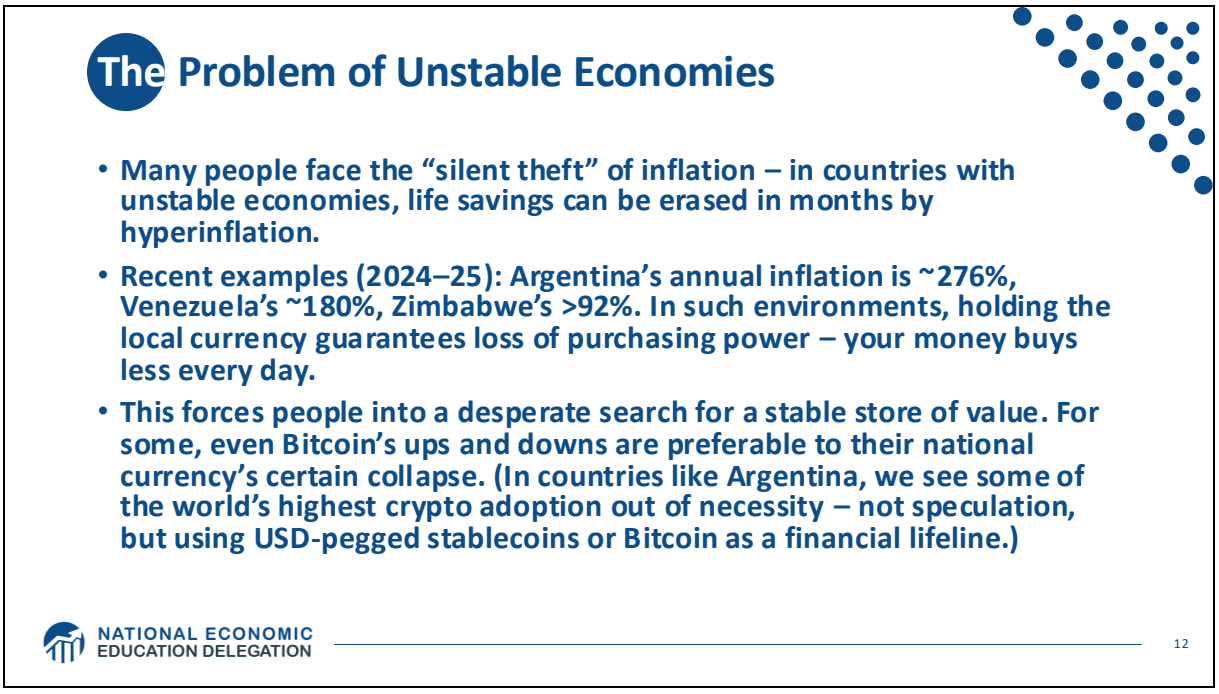


The second major problem is **financial exclusion**. While many of us take banking for granted, an estimated **1.4 billion adults worldwide are “unbanked”** – meaning they have no account at a bank or mobile money provider. This is a huge barrier to economic growth. If you don’t have a bank account, you can’t easily **save money securely**, **get a loan to start a business**, **buy insurance to protect against emergencies**, or even **receive wages or remittances efficiently**. In short, being unbanked makes it incredibly hard to escape poverty. One big reason so many are unbanked is the lack of formal IDs – millions of people can’t open an account because they don’t have government-issued identification, a problem especially acute in parts of Sub-Saharan Africa. **This is where cryptocurrency offers a paradigm shift.** Anyone with internet access and a basic smartphone can install a digital wallet, and in minutes have the ability to **send, receive, and store value globally**. No bank branch, no paperwork, no ID verification required. It bypasses the need for a traditional bank or even a government ID, potentially connecting people to the global economy who were previously left out.

M-Pesa and Bitcoin

- M-Pesa: Centralized mobile money service tied to phone number and SIM card.
- Bitcoin: Decentralized digital currency with no single controlling authority.
- M-Pesa operates in local currency under telecom & banking oversight.
- Bitcoin allows borderless, permissionless value transfer in a volatile asset.
- Both address financial inclusion, but through different models.

Unstable Economies

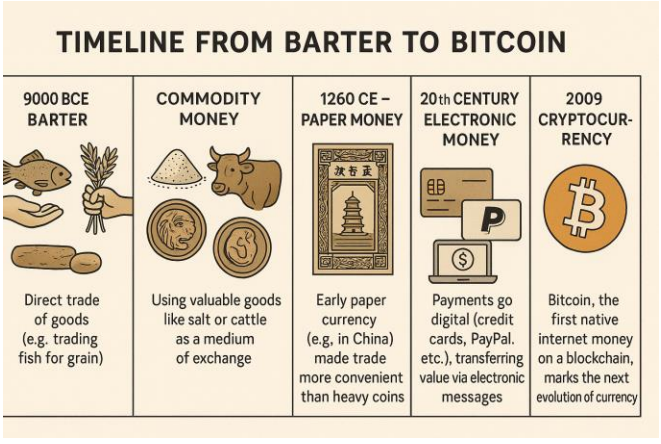


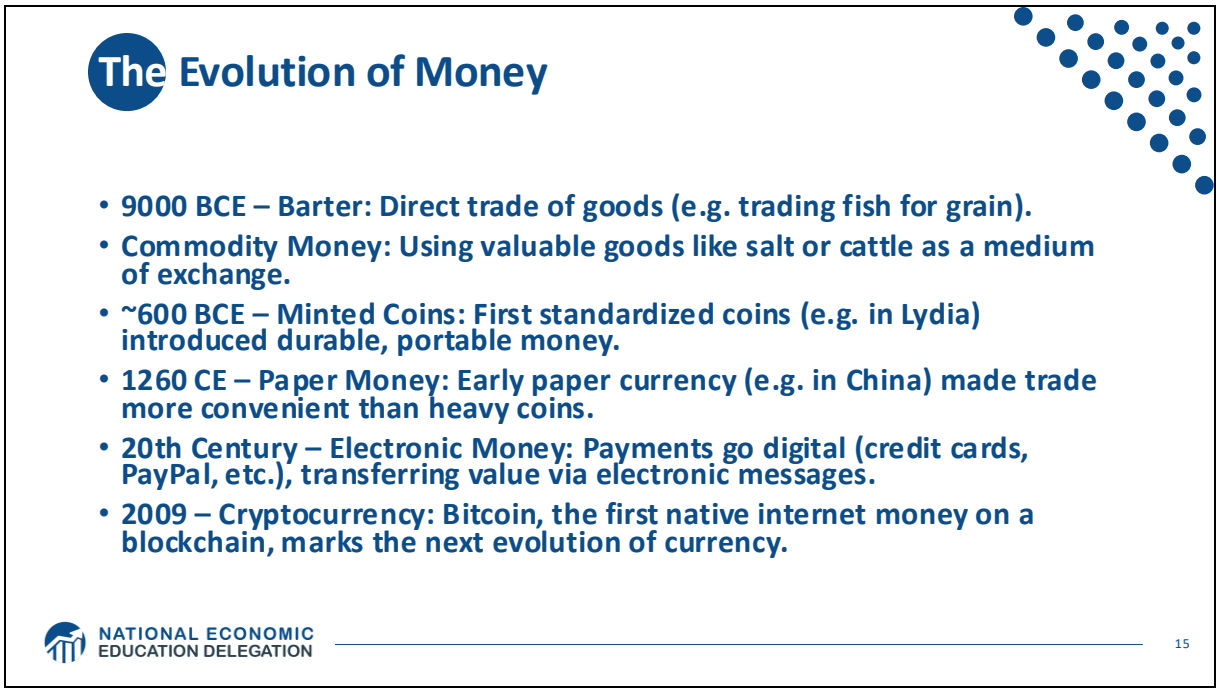
The third problem is one those of us in stable economies rarely think about: **the specter of hyperinflation**. In countries with weak economies or troubled governments, people’s life savings can **evaporate in weeks or months** due to inflation. Take recent figures: **Argentina** is grappling with over **276%** annual inflation; **Venezuela** around **180%**; **Zimbabwe** over **92%**. Imagine your money losing half its value or more every few months – that’s the reality in such places. If you hold your local currency, it’s a **guaranteed loss** – every day your paycheck buys a little less. People are forced to scramble for any asset that might hold value – whether it’s gold, US dollars on the black market, or anything resilient. This context is crucial for understanding crypto’s appeal. We often hear about Bitcoin’s volatility as a risk, but for someone in, say, Buenos Aires, **Bitcoin’s swings may be preferable to the near-certainty of the peso’s collapse**. In fact, Argentinians have become some of the world’s most active crypto users – not to chase the next “meme coin,” but to protect their family’s wealth. They often use cryptocurrencies (especially **stablecoins** pegged to the US dollar) as a practical tool to preserve the value of their labor. For them, crypto isn’t a speculative gamble; it’s a **financial lifeboat** in a sea of economic uncertainty.

A New Possibility: Digital Money

Speaker Notes:
These three problems we've discussed – **high transaction costs**, **financial exclusion**, and **wealth erosion through inflation** – are deeply interconnected symptoms of a traditional financial system that can be slow, exclusive, and fragile. Expensive remittances are a form of exclusion; lack of access to stable currency in hyperinflation drives people out of the formal economy. **Cryptocurrency emerges as a potential solution to these systemic weaknesses**. It proposes a new kind of money, built natively for the internet, designed to be **cheaper**, **more accessible**, and **more resistant to any single government or central bank's decisions**. In other words, it offers a unified technological approach to a web of financial challenges. So, what exactly is this new form of money, and **how does it work**? Let's find out.

PART 2: How It Works (Without the Jargon)
The Evolution of Money





Speaker Notes: Speaker Notes:
To understand cryptocurrency, it helps to see it as the **next step in a long history** of innovation in money. For millennia we've sought better ways to exchange value. We started with **barter**, trading goods directly – which was inefficient because you had to find someone who had what you wanted *and* wanted what you had. Over time, societies moved to **commodity money** – using items with intrinsic value like salt or cattle as currency. Around **600 BCE**, the Lydians minted the first official **coins**, creating a standardized, durable form of money. This was revolutionary, fueling trade and the growth of empires. Centuries later, the Chinese introduced **paper money**, which was even more convenient than lugging around metal coins. In the 20th century we shifted to **electronic money** – when you swipe a credit card or send PayPal, no physical cash moves, just digital messages instructing a transfer of value. Each step made transactions more efficient and abstract. **Cryptocurrency, first appearing with Bitcoin in 2009, is the next logical step** – a form of money truly native to the internet, designed for a global digital world.

Origin Story:

- **The Mysterious Satoshi Nakamoto:**
  - Lehman Brothers Bankruptcy, 9/2008
  - Halloween 2008: a white paper is published on the Internet laying out the idea and design for Bitcoin. The author (or authors) used Satoshi Nakamoto as a pseudonym.
  - **January 2009:** Satoshi releases the first version of the Bitcoin software.
  - 2009-2010: Satoshi releases new versions of the software and is actively involved in internet chatter about Bitcoin.
  - April 2011: Satoshi ceases all known and/or verified communications.
- **To this date the identity or identities of Satoshi are unknown.**

A Simple Definition

- **"Internet money that no single company, bank, or government controls."**

NATIONAL ECONOMIC EDUCATION DELEGATION

17

Speaker Notes:
If you remember only one thing today, remember this simple definition: **Cryptocurrency is internet money that no single company, bank, or government controls.** That's the fundamental difference from traditional digital payments. When you use Venmo, PayPal, or a bank app, there's a central intermediary – a company in the middle that **authorizes your transaction, takes a fee, and can reverse or freeze transactions or accounts** if it chooses. They are in control. Cryptocurrency **removes** that central intermediary. Transactions are peer-to-peer over the internet, governed by transparent rules (code) instead of corporate policies. No single actor can freeze accounts or censor payments in a truly decentralized crypto network. In short, it's **money built for the internet era, without a gatekeeper in the middle**.

The Digital Gold Analogy

Property	Gold	Bitcoin
Scarcity	Naturally Scarce	Digitally Scarce (Fixed Supply)
Durability	Physically Durable	Digitally Durable (Lives on the Internet)
Counterfeit-Proof	Hard to Counterfeit	Impossible to Counterfeit
Recognizability	Globally Recognized	Globally Accessible

Speaker Notes:
One of the best ways to understand Bitcoin, the first and most well-known cryptocurrency, is to compare it to gold. We value gold not because a government tells us to, but because it has inherent properties that have made it a reliable store of wealth for thousands of years. Gold is **scarce**; there's a finite amount of it on Earth. It's **durable**; it doesn't rust or decay. It's difficult to **counterfeit**, and it's **globally recognized** as valuable.

Bitcoin was designed to have similar properties in the digital realm. It is digitally **scarce**, with a supply that is mathematically fixed and can never be changed. It is digitally **durable**, existing on a global network of thousands of computers, making it incredibly resilient. It is cryptographically secured, making it **impossible to counterfeit** or spend the same coin twice. And because it lives on the internet, it is **globally accessible** to anyone, anywhere. This analogy helps explain why many people view Bitcoin not just as a payment system, but as "digital gold"—a modern store of value for a digital age.18

Speaker Notes:

One of the best ways to understand Bitcoin, the first and most well-known cryptocurrency, is to compare it to gold. We value gold not because a government tells us to, but because it has inherent properties that have made it a reliable store of wealth for thousands of years.
Gold is **scarce**; there's a finite amount of it on Earth. It's **durable**; it doesn't rust or decay. It's difficult to **counterfeit**, and it's **globally recognized** as valuable.
This analogy helps explain why many people view Bitcoin not just as a payment system, but as "digital gold"—a modern store of value for a digital age

What A Crypto Wallet Looks Like

NATIONAL ECONOMIC EDUCATION DELEGATION

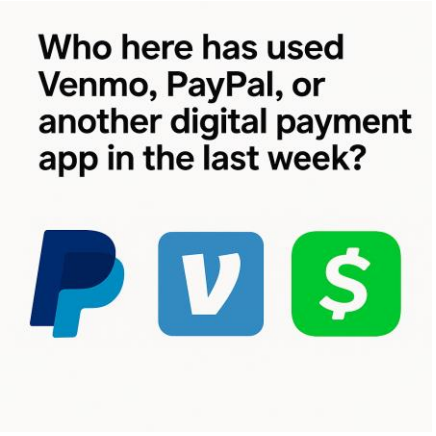
Speaker Notes:

When people hear about "cryptocurrency," they often imagine something complex and intimidating. But in practice, using it can be as simple as using your mobile banking or payment app.

This is a screenshot of a typical crypto wallet. As you can see, the basic functions are very familiar. You have your total **balance** displayed clearly at the top. You have a list of the different digital assets you hold. And you have two main buttons: **Send** and **Receive**.

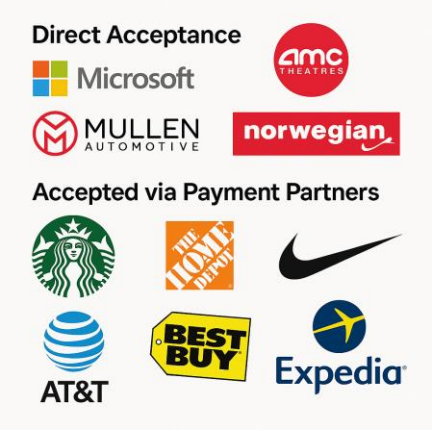
All the complex technology we'll touch on later is happening behind the scenes. For the user, the experience is designed to be straightforward. If you can use an app like PayPal or Venmo, you have the basic skills needed to use a crypto wallet. The real learning curve isn't in using the app, but in understanding the new responsibilities that come with it.

Question: The Digital Shift



Speaker Notes:
Let's do a quick poll. By a show of hands, who here has used an app like Venmo, PayPal, or Cash App in the last week?
(Pause for audience response.)
Look around. The vast majority of us are already comfortable with the idea of digital money. We trust an app on our phone to move value on our behalf. We've already made the mental leap from physical cash to digital dollars. Cryptocurrency is simply the next phase of this evolution. It takes the digital money you're already used to and removes the corporate middleman, giving you direct control. The transition is more intuitive than you might think.

Corporate Adoption Is Growing



NATIONAL ECONOMIC EDUCATION DELEGATION

21

Speaker Notes:
A key sign of any new technology's maturity is when major businesses start to adopt it. While still in its early stages, cryptocurrency is increasingly being accepted as a legitimate form of payment by a growing list of companies.
Some companies, like **Microsoft** and **AMC Theatres**, have integrated crypto payments directly, a strong vote of confidence in the technology.24 The electric vehicle manufacturer **Mullen Automotive** recently announced it would accept Bitcoin, positioning itself as an innovator in its field.
Many more brands, including household names like **Starbucks**, **Home Depot**, and **Nike**, accept crypto through third-party payment processors like BitPay or Crypto.com. This allows them to tap into a new customer base without having to manage the cryptocurrency themselves. Research shows that crypto users are often a new demographic for these businesses and tend to make larger purchases, providing a clear incentive for merchants to offer this payment option. This isn't just a niche phenomenon; it's a strategic move by businesses to engage with the economy of the future.

National Adoption: A Bold Experiment

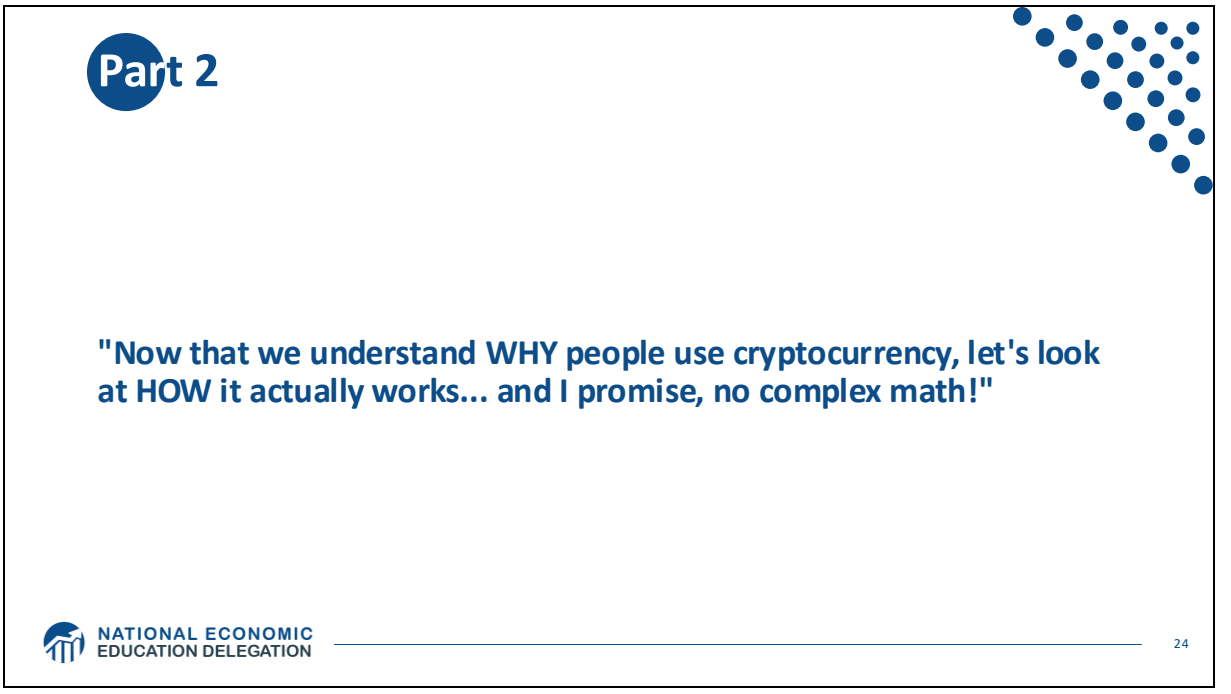
Speaker Notes:
Beyond corporate adoption, we've even seen an entire country embrace Bitcoin. In September 2021, El Salvador made history by becoming the first nation in the world to adopt Bitcoin as legal tender, alongside the US dollar.32
This was a landmark decision. The "Bitcoin Law" mandates that all businesses in the country with the technological means must accept Bitcoin as payment.32 To facilitate this, the government launched its own digital wallet, called the "Chivo" wallet, and deployed over 200 Bitcoin ATMs across the country.32
A major incentive for this move was to make remittances cheaper and easier for the millions of Salvadorans working abroad. Furthermore, to attract investment and talent, the country has made profits from Bitcoin exempt from capital gains taxes.32
This national experiment is not without its critics and challenges, including concerns about economic stability and the technical hurdles of widespread adoption.32 However, it remains a powerful, real-world test case for what happens when a nation-state integrates an open, global monetary network into its economy.

Grassroots Adoption

NATIONAL ECONOMIC EDUCATION DELEGATION

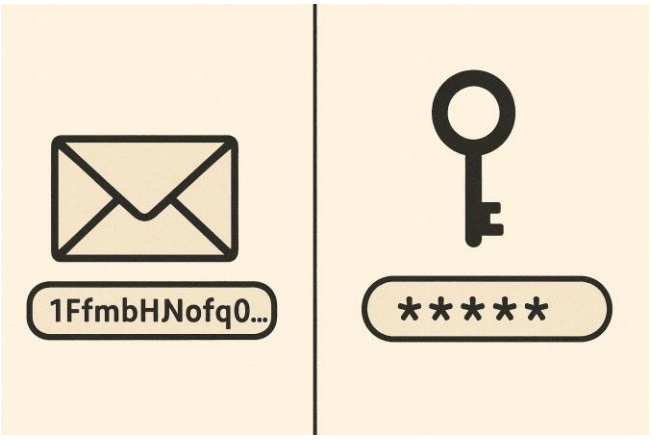
23

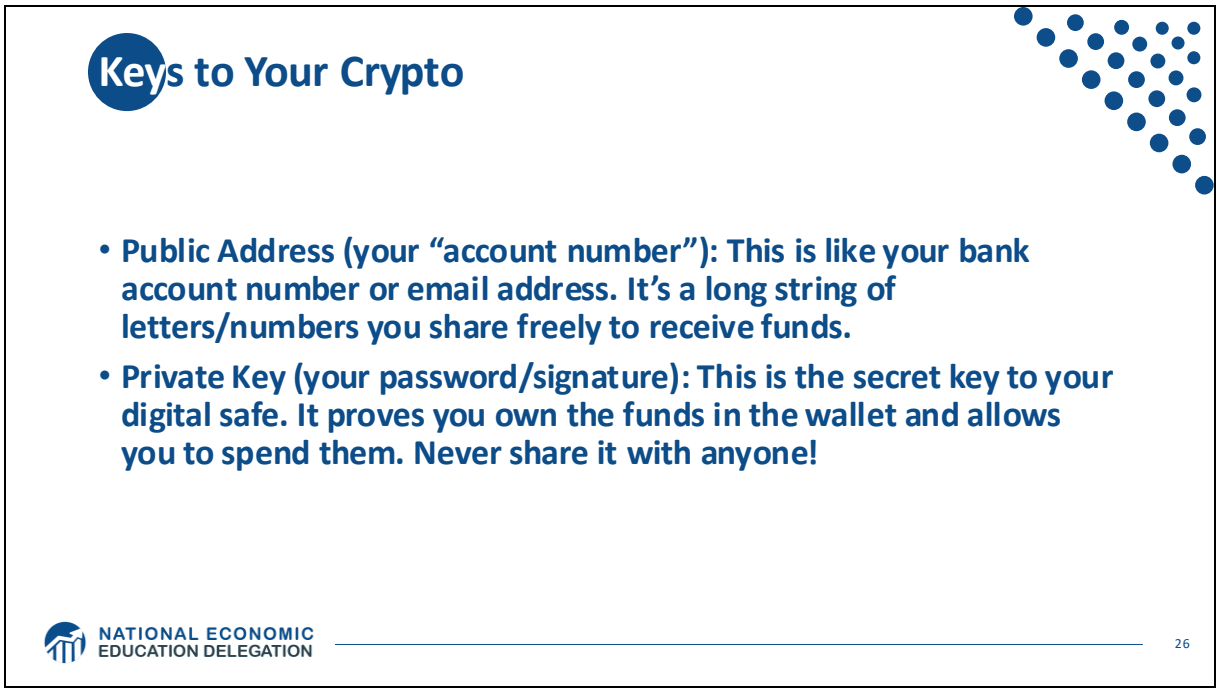
Speaker Notes:
The most powerful stories of adoption often come not from corporations or governments, but from individuals at the grassroots level who are using this technology to solve immediate, real-life problems.
The Philippines is one of the top remittance-receiving countries in the world, but fees are high. A growing number of tech-savvy Filipinos working abroad have turned to cryptocurrency to send money home. By bypassing traditional systems, they save on fees and get money to their families faster. Some have even used earnings from crypto-based online games to make enough money to return home to their families permanently, transforming their lives.
On the right, we have the story of the **savers in Argentina**. As we discussed, with inflation running at a crippling 276%, the national currency is in freefall. For millions of Argentinians, cryptocurrency, especially stablecoins pegged to the US dollar, has become an essential tool for survival. It allows them to protect their savings and transact in a stable unit of account, something their own government can no longer provide. These are not abstract use cases; this is technology as a lifeline.



Speaker Notes:
We've established the 'why'—the compelling reasons driving people, companies, and even countries to explore this new technology. Now, let's move on to the 'how'. In this this section, we'll demystify the process of actually using cryptocurrency. We'll cover digital wallets, making transactions, and where this digital money comes from, all in simple, practical terms.

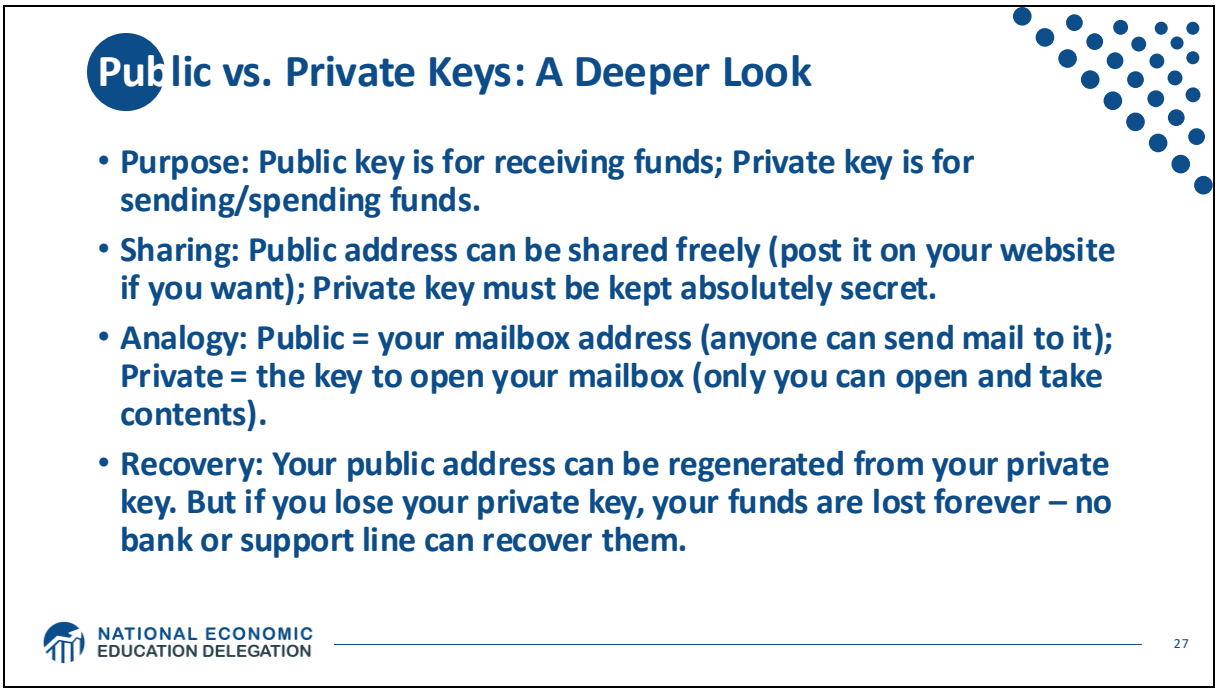
The Two Keys to Your Crypto





To use cryptocurrency, you need a **digital wallet**, and every wallet is built around two fundamental things: a **public key** and a **private key**. Understanding the difference between them is the single most important lesson in crypto security. Think of your **public key** (specifically, your public *address*) like your bank account number or email address. It's a long string of characters that you can share with anyone – no risk in that. If someone wants to send you crypto, you give them your public address.

Your **private key**, on the other hand, is like your bank account password, your ATM PIN, and your handwritten signature *all rolled into one*. It's a secret code that grants **access to your funds** and allows you to authorize (sign) transactions – basically, to send money from your wallet. **This key must be kept absolutely secret.** If anyone else gets your private key, they have full control over your money. There's no "forgot my password" link in crypto – if someone learns your private key, or if you lose it, that's it. The money can be taken and there's no authority to undo it. So, you might hear the phrase *"Not your keys, not your coins"* – it means if you don't hold the private key, you don't truly control the crypto.



Speaker Notes:

Let's break this down further, because it's that important. **Public vs. Private:** their roles are distinct. The public key (address) is for **receiving**; the private key is for **sending** or spending. How you handle them is critically different: you can paste your public address anywhere or give it to a friend, no problem. But you should **never, under any circumstance, share your private key** – not on a website, not via email, not with anyone.

The analogy: your public address is like a **mailbox**. Anyone can drop letters (funds) into your mailbox – they just need the address. Your private key is the **only key that can open that mailbox** and retrieve what's inside. Only you hold that key.

Finally, about recovery: in crypto, your public address is mathematically derived from your private key. So if you have the private key, you can always figure out your public address again. But if you lose the private key, **your funds are gone forever**. There is no central authority, no helpdesk to call. That's the trade-off for having full control – it puts *all* the responsibility in your hands.

Public Versus Private Keys

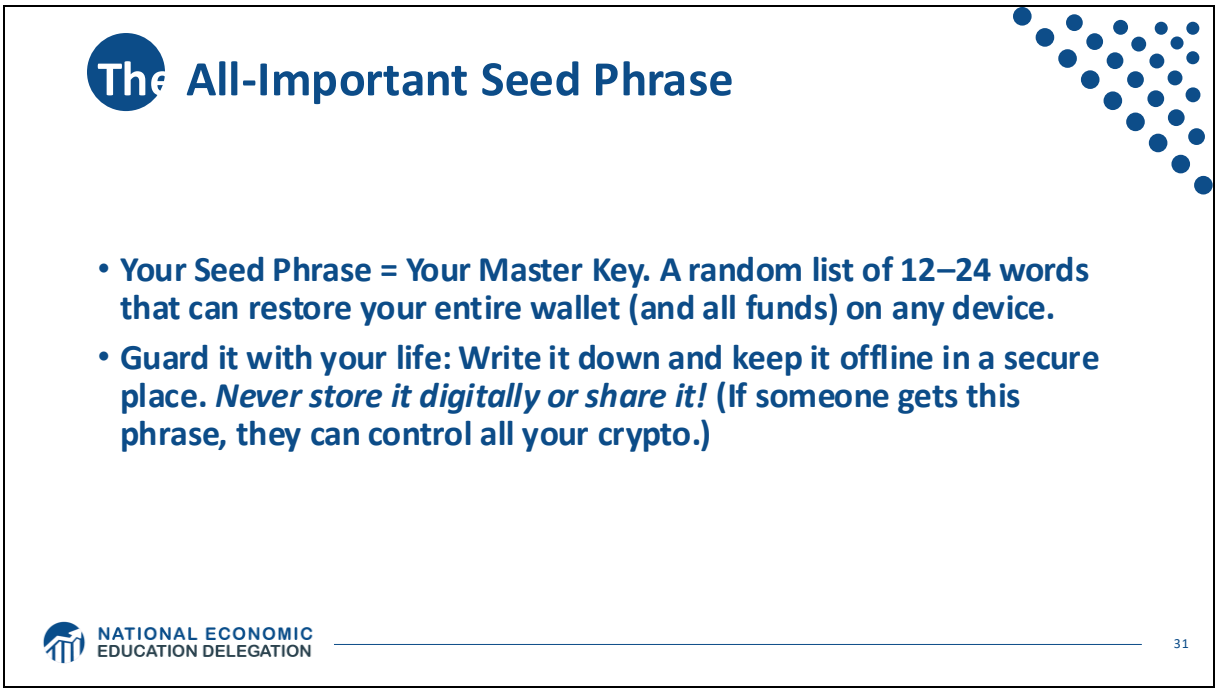
Feature	Public Key / Address	Private Key
Purpose	Receive Funds	Send/Spend Funds
Sharing	Share Freely	Keep Absolutely Secret
Analogy	Email Address / Mailbox	Password / Physical Key
Recovery	Can be regenerated from Private Key	If lost, funds are lost forever

Making It Easy: QR Codes

- Just like you might scan a QR code at a restaurant to view a menu, you can scan a QR code to send or receive cryptocurrency.
- When you want to receive money, your wallet app can generate a unique QR code that represents your public address. The sender just opens their wallet, scans your code with their phone's camera, and your long address is instantly and perfectly filled in, with no typing. It's fast, easy, and eliminates human error. This makes transactions much more user-friendly – you don't need to worry about mistyping a 30-character string.

Creating a Wallet

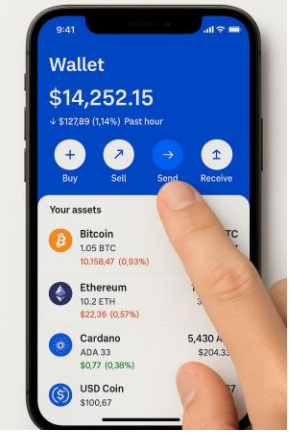
- Open the app store and download a popular free wallet app (there are many options like Coinbase Wallet, Trust Wallet, etc.). After opening the app. The first thing you will see is a big button: “Create a New Wallet.” Tap that.
- Next, the wallet app is about to generate something extremely important: a “seed phrase” (also called a recovery phrase). This is essentially the master key to my entire wallet. The app now shows you a screen with a list of 12 random words. It’s instructing you to write these down and store them in a safe place. This isn’t just a friendly tip – it’s *critical* for security. You should physically write these 12 words on a piece of paper, as recommended.



It's the heart of "self-custody." The 12-word list you will write down is your **seed phrase**. This phrase is *everything*. It's not just a password for this one app on this one phone – it's the master key that can regenerate your private keys and thus restore my entire wallet (and all its funds) on *any* new device, anywhere. In other words, **whoever holds this seed phrase holds the wallet**.

That's why the wallet strongly urged me to write it down. You should always write your seed phrase on paper (or engrave it on metal for extra safety) and store it in a **very safe, offline place** – like a home safe or safety deposit box. **Never** store it digitally (not in a phone note, not as a screenshot, not on cloud storage). If a hacker or malware finds that file, they can instantly access your funds. Also, never share these words with anyone. No legitimate person or support rep will ever ask for your seed phrase. It's effectively the **"keys to the kingdom."** Treat it like the most sensitive secret you own.

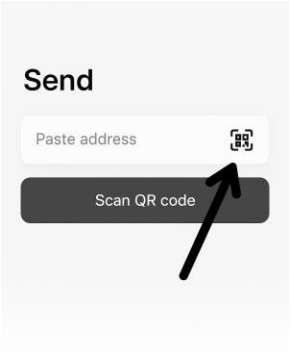
Step 1: Open Your Wallet App



NATIONAL ECONOMIC EDUCATION DELEGATION

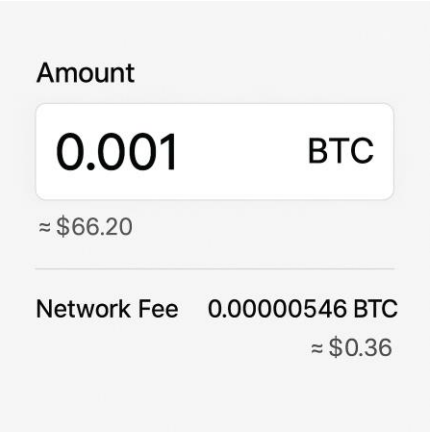
Now that we have a wallet, let's walk through the simple steps of sending a transaction. The first step is intuitive: you open your wallet app, which shows your balance, and you tap the 'Send' button.

Step 2: Enter the Recipient's Address (or Scan QR Code)



Speaker Notes:
Next, the app will ask you where you want to send the funds. You have two options. You could manually paste the recipient's long public address, but as we discussed, this carries the risk of typos. The much easier and safer method is to tap the camera icon and scan the recipient's QR code. This will populate the address field automatically and accurately.

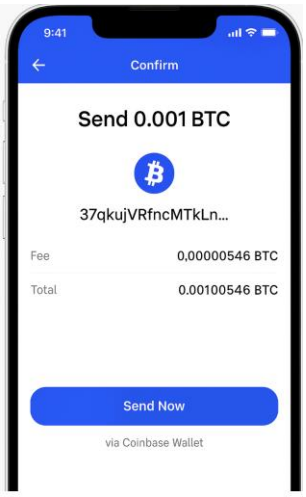
Step 3: Enter the Amount & Review the Fee"



NATIONAL ECONOMIC EDUCATION DELEGATION

Speaker Notes:
Next, I enter the **amount** I want to send. Most wallets let you enter either the crypto amount (say 0.001 BTC) or an equivalent in your local currency (about $10). Before proceeding, the wallet shows a **network fee** (sometimes called a “gas fee” on Ethereum). This is a small charge that goes to the miners or validators who will process and secure your transaction on the blockchain. It’s basically a tip or incentive for them to include your transaction. Fees can vary based on network congestion, but the wallet usually calculates it for you. It’s important to glance at this fee and make sure it’s reasonable before you hit send. In our example, since we’re on a test network, the fee might be displayed but it’s using play money. On real networks, if the fee looks unusually high, you might wait or adjust settings. But generally, crypto fees for a normal transaction are relatively low, especially compared to, say, an international bank transfer.

Step 4: Confirm the Transaction



NATIONAL ECONOMIC EDUCATION DELEGATION

Speaker Notes:
Finally, the wallet presents a **confirmation screen** with all the details of the transaction. This is your last chance to review: the destination address (does it match the intended recipient?), the amount you're sending, and the network fee being charged. If all looks good, I tap **Confirm** (or "Send"). The moment I do, my **private key digitally signs** the transaction and the wallet **broadcasts** it to the global network. At that point, the transaction is submitted. After it gets confirmed by the network, it becomes **irreversible** – the crypto will be in the recipient's wallet and I can no longer get it back, much like dropping cash in a mailbox. In our test demo, hit confirm/send, and the transaction is now on its way!

Last Transactions-Different Example

- 80e9ee6de0d2cba1ebc521867907296e0b8856131ed73df6dec67e587014207f
- Fri, 27 Jun 2025 20:55:15
- tb1qtqvm5nrdqqc5qc4ah58tsxvpyhjajvk9sv3aqt pending
- -0.0001
- 0.00000146 fee

https://bitcoinfaucet.uo1.net/

Understanding the Last Transactions List in a Crypto Wallet

- TXID 80e9ee6de0d2cba1...7014207f – This is the unique reference ID for the transaction (our transaction's "receipt number" on the blockchain).
- Date/Time Fri, 27 Jun 2025 20:55:15 – At about 8:55 PM on June 27, 2025, we initiated this transaction.
- Address tb1qtqvm5nrdqqc5qc4ah58tsxvpyhjajvk9sv3aqt – This is the Bitcoin address of the recipient. The funds are being sent *to this address*. (Because it starts with "tb1", we know it's a testnet Bitcoin address, but functionally it represents the receiver's account in this example.)
- Status pending – The transaction has been broadcast but is not yet confirmed on the blockchain. It's waiting for inclusion in a block. Once miners include it and it gets enough confirmations, this status will update to confirmed and show a confirmation time.
- Amount -0.0001 BTC – We (the sender) are sending 0.0001 BTC. The negative sign indicates this amount is leaving our wallet. If this were incoming, it would show as +0.0001. So we're paying out 0.0001 BTC to someone.
- Fee 0.00000146 BTC – In order to send that 0.0001 BTC, we're also paying a network fee of 0.00000146 BTC to the miners. This ensures the transaction will be processed. It's a very small fee (a tiny fraction of a Bitcoin).

Let's put 0.0001 BTC into perspective: Bitcoin is highly divisible – 1 BTC is equal to 100 million satoshis (the smallest units). **0.0001 BTC** is a small fraction of a Bitcoin (specifically, 0.0001 = 10,000 satoshis). It's like saying a few cents in terms of Bitcoin's currency. For new learners: don't be thrown off by the decimal places – it's normal in crypto to see very small fractions. Transactions can be for tiny amounts of a coin.
Sending 0.0001 BTC with a 0.00000146 BTC fee would in total reduce your balance by 0.00010146 BTC.

In plain English

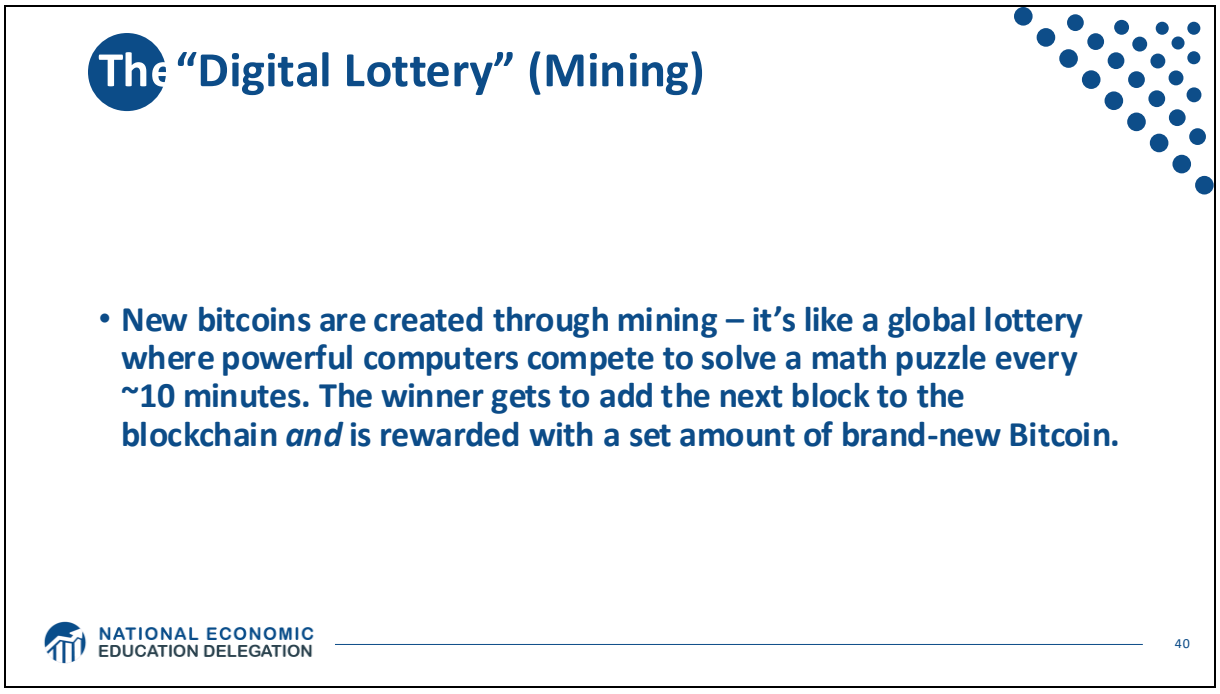
- ***On June 27, 2025, a transaction (ID beginning 80e9ee6d...) was created to send 0.0001 BTC to the address tb1qtqvm5...sv3aqt. The transaction is currently pending (not yet confirmed on the blockchain) and included a network fee of 0.00000146 BTC.*** **Once this transaction gets confirmed (with enough block confirmations), it will no longer be pending, and the recipient will officially have the 0.0001 BTC.**

The **transaction ID** lets you track and verify the transaction on the blockchain.
The **timestamp** tells you *when* the transaction happened.
The **address** tells you *who* the money is going to or coming from (like the account or destination).
The **status** (pending/confirmed) tells you *if* the transaction has been finalized on the blockchain yet
The **amount** (and its sign) tells you *how much* was transferred and in which direction (sent or received)
The **fee** tells you the *cost* of the transaction and affects how quickly it gets processed

What's Happening Behind the Scenes?

- **When you hit send, your transaction is broadcast to a global network of computers.**
- **Miners (network participants) collect pending transactions into a block and add it to the blockchain – a permanent, shared digital ledger of all transactions. Once added to a block, a transaction cannot be altered.**

Speaker Notes:
So, what happened in the network when I hit "Confirm"? My wallet broadcasted the transaction to the global peer-to-peer network of computers running the Bitcoin protocol. On this network, special participants called **miners** are constantly working. They gather recent transactions (including ours) and bundle them into a candidate "**block**". Each block is like a page in the ledger of all transactions.
Miners then engage in a **competition** to solve a complex mathematical puzzle related to that block. Think of it like a lottery or a race – the first miner to solve the puzzle wins the right to add their block of transactions to the official chain. When a miner wins, their block is **appended to the existing chain** of blocks (hence *blockchain*) and locked in place by cryptography. This blockchain is a public, shared ledger – a global "digital notebook" that everyone can see but no one can retroactively change or erase. Once our transaction is written into this ledger, it's there forever, secured by the cryptographic links that connect each block to the last. That's how, in Bitcoin, transactions become final and tamper-proof.



We’ve talked about sending and receiving crypto, but you might wonder: **Where do new bitcoins come from in the first place?** The answer (for Bitcoin) is a process called **mining**. The easiest way to think about mining is as a giant, global **lottery** that runs every 10 minutes.

Imagine thousands of powerful computers around the world, all “playing” this lottery. Every time (roughly every 10 minutes) a new round starts: the computers try to solve an incredibly difficult mathematical puzzle. It’s essentially a guessing game, and it requires a lot of computation. The **first computer to solve the puzzle wins** that round. What do they win? Two important things:

They get to add their block of transactions to the blockchain. This means they validate and officially record all those pending transactions (including awarding themselves the prize).

They are awarded a certain number of brand-new bitcoins as a reward for their work and the electricity they expended. This is how new bitcoins enter circulation – as a reward to miners for securing the network.

Right now that reward (as of 2025) is 6.25 BTC per block, but it halves every four years or so. Mining thus serves a dual purpose: it **secures the network** (because miners are verifying transactions and linking blocks) and it **releases new coins in a controlled, decentralized way**. No central bank “prints” Bitcoin – new coins have to be earned through this competitive process.

Wait, Why Does It Take 10 Minutes?

- **On the Bitcoin network, each new block averages ~10 minutes. This delay is a security feature, allowing time for the network to confirm and agree on transactions.**
- **In those ~10 minutes, miners are working to secure the block. Once your transaction is in a confirmed block, the whole network agrees it's valid and permanent. *(Note: Some newer cryptocurrencies have much faster confirmations, but Bitcoin chooses security over speed.)***

Speaker Notes:
You might have noticed that after I sent the transaction, it didn't instantly show up as "confirmed" in the other wallet. **Bitcoin's network has about a 10-minute confirmation time** by design. This isn't a bug – it's a crucial part of Bitcoin's security. That ~10 minute interval is roughly how long it takes miners to solve the puzzle and add a new block to the chain. The network uses this time to **reach consensus** globally that all transactions in that block (including yours) are valid and have been officially recorded.
While some newer cryptos confirm much faster, Bitcoin's 10-minute block time is a deliberate trade-off favoring security and decentralization over speed. It ensures that once a transaction has those confirmations, it's truly final and exceedingly hard to reverse or tamper with. Essentially, Bitcoin gives up some speed to gain very high confidence that each block of transactions is settled and immutable. So, yes – you often wait a few minutes for a Bitcoin payment to fully confirm, but that's the network locking it in with strong security.

A Fixed and Finite Supply

- **There will only ever be 21 million Bitcoin. This hard cap is encoded in Bitcoin's core software and enforced by the network.**
- **Unlike traditional currencies which governments can print indefinitely, Bitcoin's supply is fixed and predictable. Everyone knows the total number of coins that can ever exist, which makes it a scarce digital asset.**

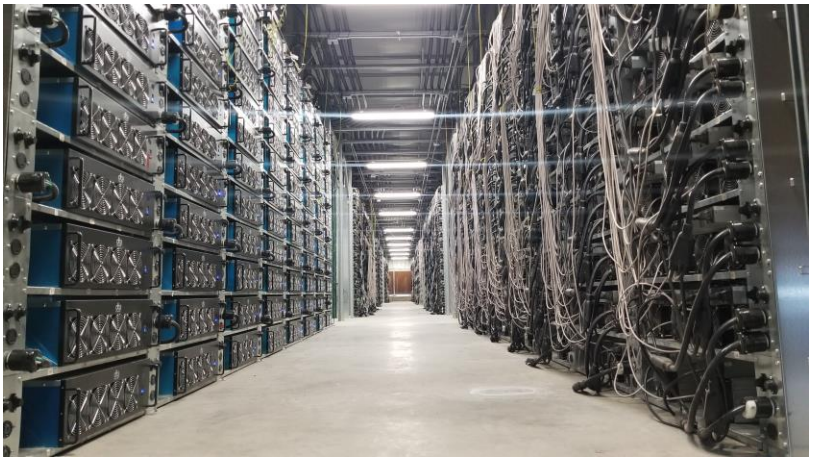
Speaker Notes:
This brings us to one of Bitcoin's most fundamental characteristics: its **absolute scarcity**. The Bitcoin protocol – the rules that all nodes follow – dictates that there will only ever be **21,000,000 bitcoins** created. Not 21 million and one. That cap is hard-coded and *every* participant in the network enforces it. It's virtually impossible to change because you'd need global consensus to alter the code that drastically.
In contrast, think about traditional fiat currencies like the US Dollar or Euro. Central banks can and do issue more money over time (often to stimulate the economy or respond to crises). There's theoretically no strict limit – they can print as needed, which can lead to inflation and devaluation of existing money. Bitcoin is the opposite: its issuance is on a known schedule that gets slower over time (the mining rewards halve roughly every four years) and then stops at 21 million. **Everyone knows exactly how many bitcoins will ever exist**, and that predictability and scarcity are a big part of its value proposition. It's akin to digital gold: scarce by design. This doesn't guarantee price stability (Bitcoin is still very volatile), but it does mean it isn't subject to dilution by a central authority printing more.
(At this point, we've covered how cryptocurrency works: wallets, keys, transactions, mining, and Bitcoin's monetary policy. Next, we'll discuss what you can actually do with these technologies – the opportunities – and the risks that come with them.)

Proof of work: Bitcoin “mining”

- The incentive for miners is that the winner of the competition to solve the puzzle gets rewarded with NEW bitcoins and transaction fees.
- However, the miner will not get the reward unless other miners agree that the puzzle was solved and add the winner’s block to the blockchain.
- In this way, transactions are added to the chain via a proof of work “consensus” of miners.

Bitcoin miners are collectively producing approximately 986.58 million trillion random numbers (hashes) every second.

Bitcoin mine



PART 3: Opportunities & Risks

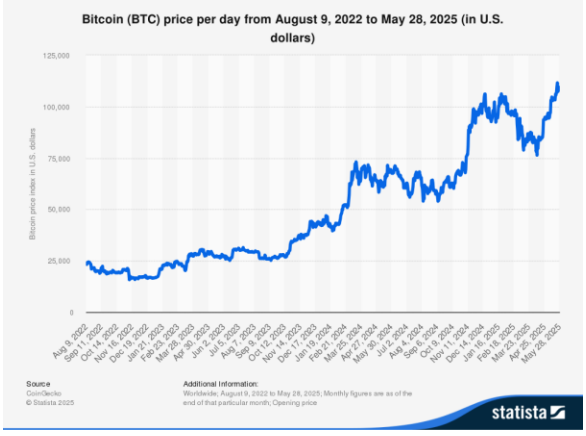
Image from chatgpt.

The Benefit of a 24/7 Global Market

- **Traditional finance runs on business hours (e.g. 9–5 weekdays), with weekends and holidays off. Crypto markets never sleep: transactions can occur 24 hours a day, 7 days a week, 365 days a year, across borders.**
- **This always-on nature means you can send value or execute trades at any time, and funds can arrive in minutes. It's a major leap in efficiency and convenience for a globalized economy where money doesn't need to "stop" on weekends.**

Speaker Notes:
A crucial benefit of cryptocurrency is its **relentless, always-on nature**. The traditional financial world is constrained by business hours, weekends, and holidays. If I initiate a bank wire on Friday at 4 PM, it might not clear until Monday or Tuesday, especially if it's international. The system basically "closes" outside working hours and on weekends. Cryptocurrency networks, however, operate continuously **24/7/365**. There's no opening or closing bell. I can send you value on a Sunday at 3 AM, and it will go through in minutes. For **international businesses**, freelancers, or families spread across different countries, this constant availability is a huge improvement. The global economy doesn't stop on weekends – and with crypto, neither does the movement of money. Whether it's midnight or a public holiday, the network is up and running. That level of accessibility and speed is unprecedented in finance.

Price Volatility



The Crypto Rollercoaster: Price Volatility

- **Extreme ups and downs: Bitcoin's price, for example, dropped 40% in a single day in March 2020 (COVID crash), then surged by hundreds of percent in 2020–21 (bull run), crashed again in 2022 (–64%, e.g. after a major exchange collapse), then hit new highs in 2024 (after US ETF approvals).**
- **This level of volatility can create opportunities for massive gains, but equally the potential for devastating losses, sometimes in short time spans. It's not for the faint of heart, and it remains one of the biggest risks in crypto.**

Speaker Notes:
Now we need to talk about the other side of the coin: **risks**. The most famous risk of crypto is its **price volatility**. This chart of Bitcoin's price over the last few years looks like a wild rollercoaster. In March 2020, at the start of the pandemic, Bitcoin plunged nearly 40% *in one day*. Then later in 2020 into 2021, it skyrocketed during a bull run fueled by things like institutional adoption (Tesla buying BTC, etc.). By late 2021, one Bitcoin was worth over $60k. But in 2022 it crashed hard – the collapse of a major crypto exchange (FTX) triggered a market-wide crisis, and Bitcoin lost about 64% of its value that year. Then 2023 saw a big recovery (Bitcoin gained over 150% that year), and by early 2024, optimism over U.S. spot Bitcoin ETF approvals drove it to new all-time highs.
The point is, the journey is **highly volatile**. If you invested $1000 at a peak and it crashed, you could lose a large chunk of that value quickly. Conversely, early or lucky investors have seen huge gains. This volatility can mean *massive upside* but also *massive downside*, and it can happen faster than in traditional assets. It's not for the faint of heart. Anyone engaging with crypto should be prepared for dramatic price swings and never invest more than they can afford to lose.

Question – please answer in chat

Bitcoin is considered by some an asset that will store value because:

a) people are easily deceived.

b) its supply is under the control of monetary authorities.

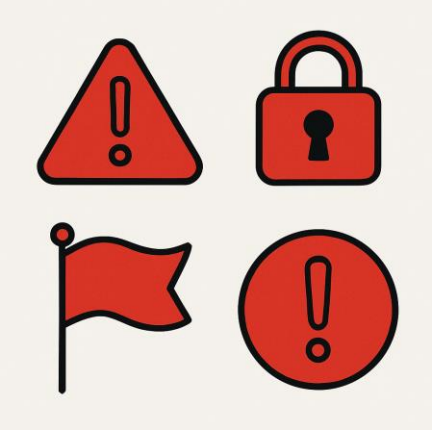
c) its supply is independently determined by code.

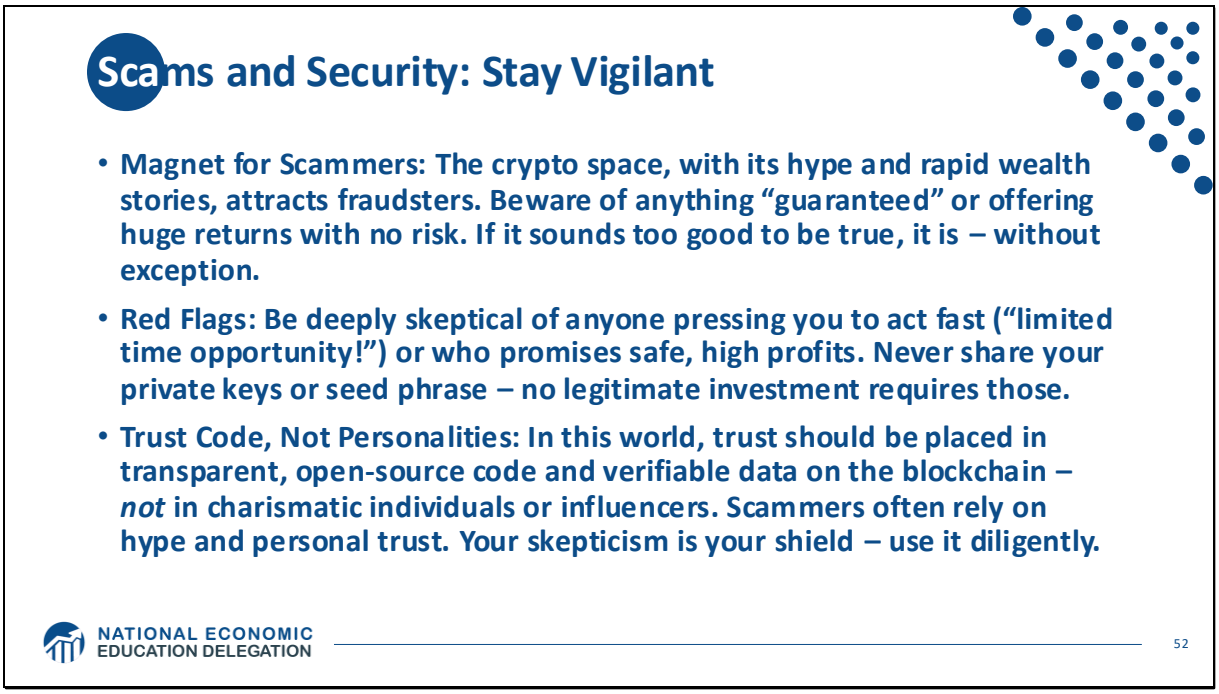
d) it is not volatile.

Retirement Savings Are Opening to Crypto

- Crypto has already made its way into American retirement systems :
- Since 2022, some 401(k) plans have allowed investments in crypto.
- Several state pension funds now have exposure to crypto through ETFs or investments in crypto-related companies.
- States like New Hampshire are even creating state-level crypto reserves with taxpayer funds.

Buyer Beware!





Speaker Notes:

Unfortunately, the crypto ecosystem – alongside the brilliant innovation – has also become a **magnet for scammers and charlatans**. With new technology and a bit of FOMO, some people let their guard down. Always remember the **red flags** we discuss for spotting scams. If someone promises you **guaranteed profits** or a "risk-free" way to double your money, **run the other way**. There are no guaranteed gains in crypto (or anywhere in investing). Also be wary of anyone who pressures you to act quickly – like "Buy this now or you'll miss out!" Scammers often create false urgency.

We saw things like rug-pulls, Ponzi schemes, fake giveaway scams (e.g. "send 1 BTC and we'll send back 2 BTC!"), phishing attacks – all sorts of fraud. **Question the hype** you see on social media. If an opportunity sounds too good to be true, *it is, without exception*. Don't trust something just because a celebrity tweeted it or some "crypto guru" on YouTube said it's a sure bet. In this space, it's much safer to **trust the technology (open-source code, verified blockchain data) rather than personalities or promises**. If someone claims a project will make you rich, check if their code or business model actually stands up to scrutiny – and often you'll find it doesn't.

Bottom line: **maintain healthy skepticism**. Your skepticism is your shield in crypto. Use it. By staying skeptical and doing your own due diligence, you can avoid the vast majority of scams out there.

(Having weighed the key opportunities and risks in crypto, we'll now move to the final part

– zooming out to the bigger picture: other innovations beyond Bitcoin, and how the wider world (governments, institutions) is responding.)

The Hidden Costs of Crypto Mining

- To generate new coins, "crypto mines" use massive amounts of energy. Many states and utility companies give these multimillion-dollar operations huge discounts on electricity. As a result, households end up subsidizing their energy use. In Texas, crypto mining has raised residential electricity costs by an estimated $1.8 billion per year and brought the state's power grid "perilously close" to failure.

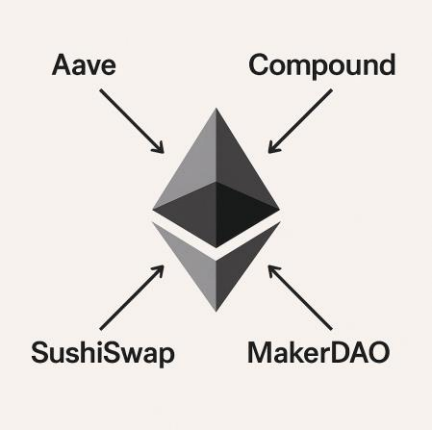
A Threat to Public Health and Quality of Life

- Communities hosting crypto mines suffer from the consequences. Residents near facilities in Texas, Arkansas, and North Dakota report constant, disruptive noise pollution that causes sleep loss and stress. Many have reported health issues they link to the mines, including hypertension, hearing loss, and migraines. The mines also raise alarms about water usage and potential contamination.

PART 4: The Bigger Picture (What's Next?)

Speaker Notes:
In our final section, we'll broaden our view. The crypto world doesn't stop at Bitcoin. Over the past decade, this ecosystem has grown from a niche hobby into a multi-trillion-dollar industry. As that's happened, governments and regulators worldwide have moved from ignoring it to actively trying to understand and manage it. So we'll look **beyond Bitcoin** at other innovations (like Ethereum, stablecoins, NFTs, DeFi), then see how the regulatory landscape is shaping up, and finally outline what your own next steps could be after this talk.

Ethereum: The World Computer

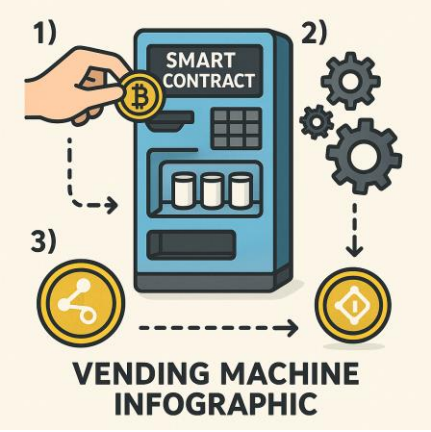


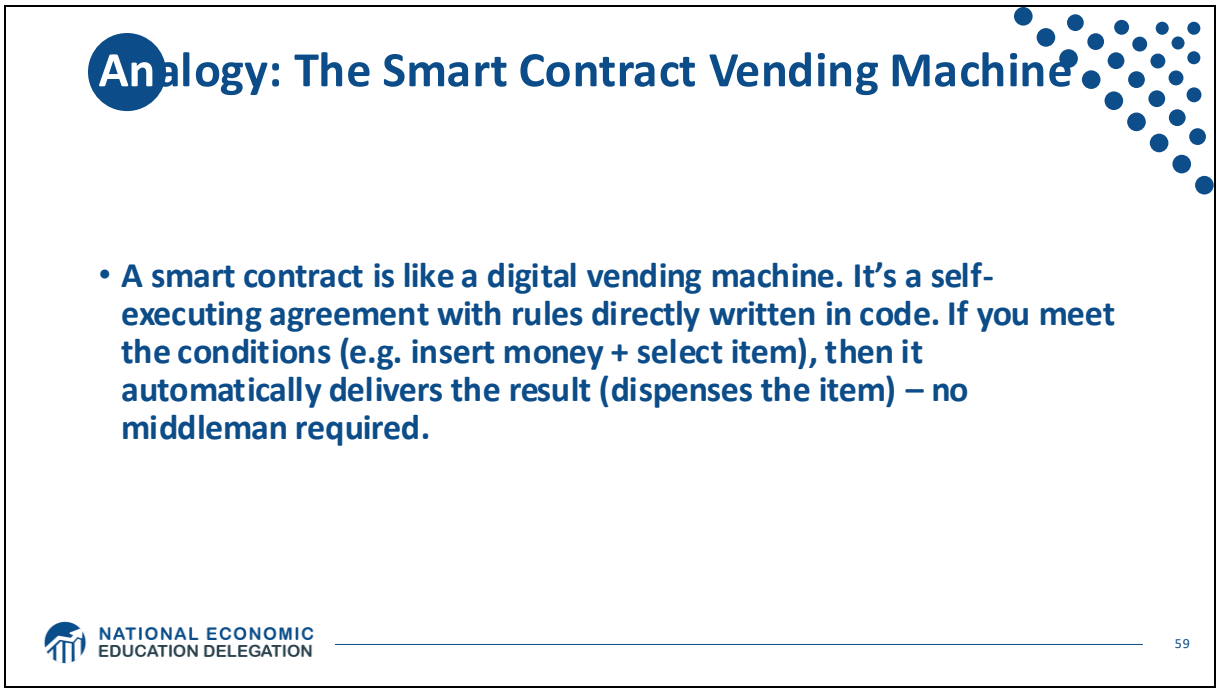
Speaker Notes:
If Bitcoin is digital gold, **Ethereum** is like a **decentralized world computer**. Launched in 2015, Ethereum took the blockchain concept and made it *programmable*. While Bitcoin's blockchain is designed to do one thing well – track ownership of bitcoin – Ethereum's blockchain is more flexible. Developers can build their own applications on top of it.
The key innovation that enables this is the **smart contract**. A smart contract is basically a small program stored on the Ethereum blockchain that executes certain actions when predefined conditions are met. This means you can create all kinds of functionality: tokens, financial agreements, games, marketplaces – you name it – that run in a decentralized way on Ethereum. Ethereum is like an **open-source, global computing platform** that anyone can use to create secure, decentralized apps. It's the foundation for a huge portion of the crypto ecosystem – many of the concepts we'll discuss (DeFi, NFTs, etc.) are built on Ethereum or similar smart-contract platforms.

Ethereum

- Ethereum is a global, decentralized platform for building and running applications. It's like a programmable blockchain-computer.
- The core innovation of Ethereum is the smart contract – code that lives on the blockchain and automatically executes agreements when conditions are met.

Smart Contracts on the Ethereum Blockchain





Speaker Notes:
The term "smart contract" can sound intimidating, so let's use an analogy: **a vending machine**. A vending machine is essentially a simple contract in physical form. The rules are pre-set: if you insert the correct amount of money and press the button for, say, a soda, the machine automatically dispenses the soda. There's no human cashier needed, no further negotiation – the contract (machine) self-executes the trade (money for soda) given the right input.
Now imagine a much more sophisticated digital version of that: a **smart contract**. It's a piece of code on the blockchain that defines rules and outcomes. When the specified conditions are met, it executes automatically. For example, a smart contract could say: *"if Person A and Person B send 1 ETH each into this contract by a certain date, then release 2 ETH to Project X's address; otherwise refund the ETH to senders."* That could facilitate a crowdfunding campaign without a company like Kickstarter. Or an insurance smart contract might automatically pay out to you if your flight was delayed (using an oracle that feeds it flight data). The point is **no middleman** is needed to enforce the agreement – the code *is* the agreement, and it will run exactly as written. This enables all kinds of complex transactions to occur **trustlessly** (you don't need to trust the other party, just the code). It's extremely powerful: we can now create services for lending, trading, insurance, etc., all as code on the blockchain (which is essentially what **DeFi** is, as we'll see).

Ethereum vs. Bitcoin: Energy Efficiency

- Ethereum now uses ~1% of the energy that Bitcoin does.
- Reason: Ethereum transitioned to proof-of-stake (PoS) in 2022 ('The Merge').
- Bitcoin still uses proof-of-work (PoW), which is energy-intensive.
- This makes Ethereum significantly more environmentally sustainable.

StableCoins: Crypto without the Volatility

Speaker Notes:

One of the biggest barriers to using Bitcoin or Ether for everyday transactions is **volatility** – the price can change so much that neither buyers nor sellers are comfortable using it for pricing things like coffee. The solution that emerged is **stablecoins**. As the name suggests, a stablecoin is a type of crypto designed to maintain a **stable value**. The most common stablecoins are pegged to fiat currencies (usually the US Dollar). For instance, **USD Coin (USDC)** aims to always be $1.00. How? For every 1 USDC out there, the issuing company holds $1 (in cash or short-term safe investments like U.S. Treasury bills) in reserve. That backing is regularly audited. So you effectively have a digital dollar that you can send anywhere in the world in minutes, with minimal fees, just like any other crypto transaction – but it won't fluctuate wildly because it's fully backed 1-to-1 by actual dollars.

Stablecoins combine the **stability of traditional money with the efficiency of crypto**. They've become a cornerstone of the crypto ecosystem. People use stablecoins for international remittances (so families can receive digital dollars instead of volatile tokens), for trading (they're the de facto "cash" on crypto exchanges), and as a safe haven during market volatility. In countries with high inflation (like we discussed earlier), some people have turned to stablecoins to preserve value in dollars when their local currency is unreliable.

Of course, using a stablecoin does introduce some reliance on the issuer (you trust they actually have the reserves). There are different designs – some stablecoins are

decentralized and use crypto collateral or algorithms – but the dominant ones like USDC and Tether are fiat-backed. The key point: stablecoins have brought relatively **stable value** into the crypto world, enabling more practical use in commerce and finance.

NFTs-Non-Fungible Tokens

NFTs: Unique Digital Ownership

- **NFT stands for Non-Fungible Token. "Non-fungible" means unique – it can't be replaced by another of the same kind.**
- **An NFT is essentially a *digital certificate of ownership* for a specific asset, recorded on the blockchain. It can represent digital items (art, music, in-game items) or even physical assets. Each NFT is one-of-a-kind, unlike cryptocurrencies or dollars which are interchangeable.**

NATIONAL ECONOMIC EDUCATION DELEGATION

64

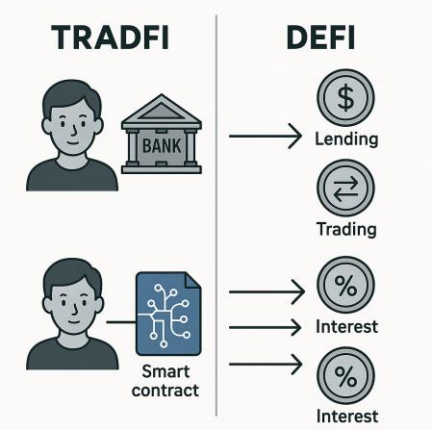
Speaker Notes:

You've likely heard the term **NFT**, which exploded into mainstream discussion in 2021. NFT stands for **Non-Fungible Token**. This concept sounds complex but it's based on a simple idea. *Fungible* means interchangeable – for example, one dollar is the same as any other dollar; if we swap, no one is worse off. *Non-fungible* means each item is unique and not directly replaceable. The **original Mona Lisa painting** is non-fungible – there's only one. You can have prints or copies (those are fungible among themselves, but none is the original).

An **NFT** is like a digital deed or certificate of ownership for a unique item. The record of that ownership is stored on a blockchain (often Ethereum). This solves a longstanding problem in the digital world: historically, any digital file (image, audio, etc.) can be copied infinitely with no loss of quality, so the concept of owning an "original" digital piece was meaningless. With NFTs, for the first time we can have **provable digital scarcity**. Anyone can still copy the image (just like anyone can buy a poster of the Mona Lisa), but only one person can own the **NFT** that represents the *original* or officially owned item. The blockchain verifies that ownership history.

In essence, an NFT is a **token that is one-of-a-kind**. It might point to a piece of digital art, a music album, a video clip, or even something like a deed to a house. The token proves "I own this unique thing" and you can transfer that token to sell the item to someone else. It opened up a whole new world of digital collecting and provenance in the digital realm.

Defi-Decentralized Finance



DeFi: Banking Without Banks

- **Decentralized Finance (DeFi) uses smart contracts to offer financial services without traditional intermediaries.**
- **On DeFi platforms, people can lend, borrow, trade, and earn interest directly with each other, governed by code. For example: lend your crypto and earn interest, or swap tokens on a decentralized exchange – all without banks or brokers involved.**

Speaker Notes:
Now to one of the most ambitious crypto frontiers: **Decentralized Finance, or DeFi**. DeFi essentially aims to **rebuild the financial system from the ground up**, using smart contracts instead of banks, brokers, or insurance companies. It's about doing all the things we do in finance – lending, borrowing, trading, investing – but **peer-to-peer on blockchain networks**, without relying on traditional institutions.
Here are some examples to make it concrete:
Lending/Borrowing: Instead of putting money in a bank to earn interest (and the bank lends it out), you can *lend out your crypto directly* to others using a DeFi protocol (like Compound or Aave) and earn interest that way. Smart contracts pool lenders' funds and automatically handle interest rates and collateral for borrowers. If you have crypto and want to earn, you deposit into the lending contract; if you need a loan, you put up collateral crypto and borrow from the pool, paying interest to the lenders. No bank needed – the code sets the rules (interest rates, collateral ratios) and enforces them.
Trading: You can trade assets on a **decentralized exchange (DEX)** like Uniswap. There's no company matching buyers and sellers; instead, smart contracts create liquidity pools and use algorithms (like automated market maker formulas) to let you swap, say, Ethereum for a stablecoin or any token for another, directly from your wallet, 24/7. No account signup, no broker – just you and a contract.
Earning Yield: DeFi also offers new kinds of "yield farming" or liquidity providing, where

users earn fees or tokens for providing liquidity to these protocols. It's a bit complex, but it's essentially a new form of investing.

Insurance/Derivatives: There are even decentralized insurance platforms (covering risks in DeFi itself) and derivatives markets – all run by code.

The **important thing** is that DeFi is permissionless – anyone in the world can access these services with a wallet and internet, no credit checks or bank accounts needed. It's transparent – the contract code is usually open for anyone to audit, and you can see all transactions on the blockchain. And it's composable – meaning you can combine these services like Lego blocks (for example, use a DEX to swap one token, then put it into a lending protocol, etc., all seamlessly).

However, DeFi is also *cutting-edge and risky*. Smart contract bugs or hacks can happen, and without intermediaries, if something goes wrong there's no FDIC insurance or banks to absorb losses. So, while it's a fast-growing area enabling a wave of innovation and higher yields, users must approach carefully. But it demonstrates the power of crypto: we can reimagine financial services in a way that's open and accessible to anyone.

(We've now explored the major expansions of the crypto ecosystem: platforms like Ethereum and smart contracts enabling stablecoins, NFTs, DeFi, etc. Next, let's consider how governments and traditional finance are reacting to this rapidly growing space.)

Transition to Regulation

- ***As this ecosystem has grown, governments have taken notice. Let's see how they're responding and what it means for you.***

Speaker Notes:
We've just glimpsed the vast and innovative universe being built on blockchain technology – from stablecoins and NFTs to DeFi and even intersections with AI and beyond. As this ecosystem exploded from a niche hobby into a global, multi-trillion-dollar industry, it unsurprisingly captured the full attention of governments and financial regulators worldwide. The "wild west" days of operating in a regulatory gray area are ending.
Let's now turn to how the official sector is responding, and what this emerging regulatory landscape means for users and investors. In other words, how is crypto moving from its freewheeling early years toward a more regulated, mainstream footing?

Trillion dollar question

- So why do we trust banks and MMFs(money market funds) with the vast majority of our hard-earned money?

Trust

- A regulatory framework that transforms risky deposits into safe assets- lender of last resort, FDIC deposit insurance.

The Shift from "Wild West" to Wall Street

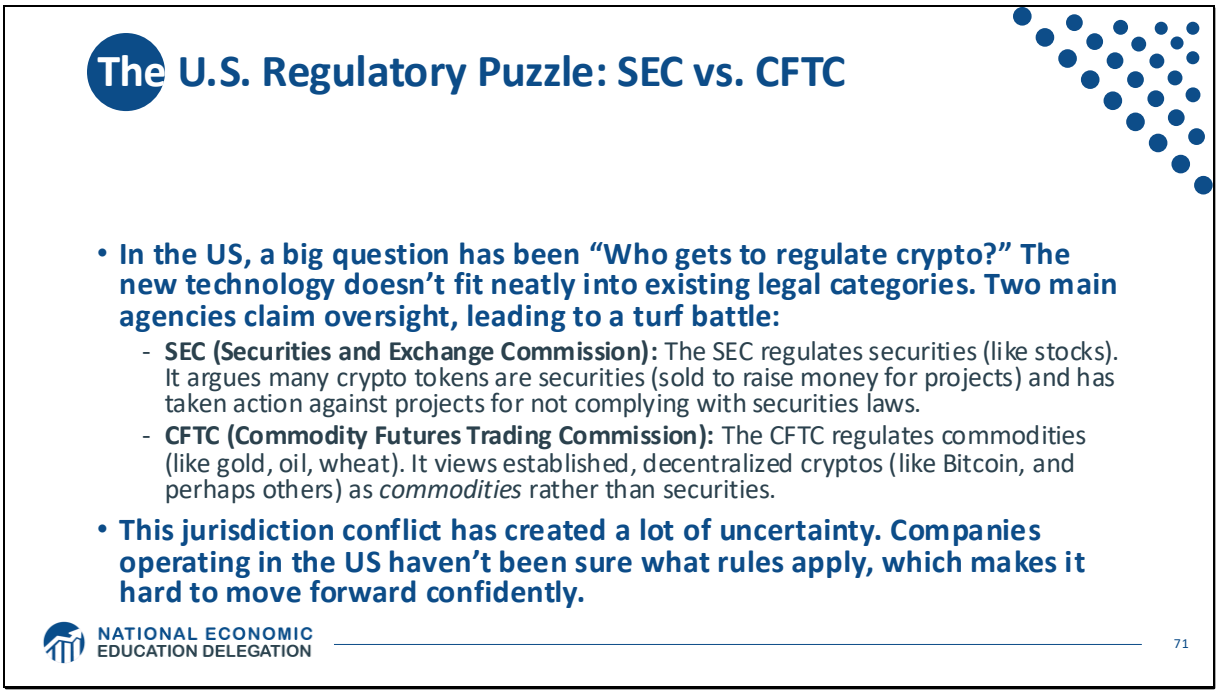
NATIONAL ECONOMIC EDUCATION DELEGATION

Speaker Notes:

For much of its early history, the crypto space was likened to the "**Wild West**" – an exciting but lawless frontier with few rules and almost no sheriffs. This lack of regulation did allow for incredibly rapid, permissionless innovation – anyone could launch a new project or token – but it also created a ripe environment for scams, fraud, and spectacular failures (we saw some of those in 2014–2017 with Mt. Gox, ICO scams, etc., and again in 2022 with things like FTX).

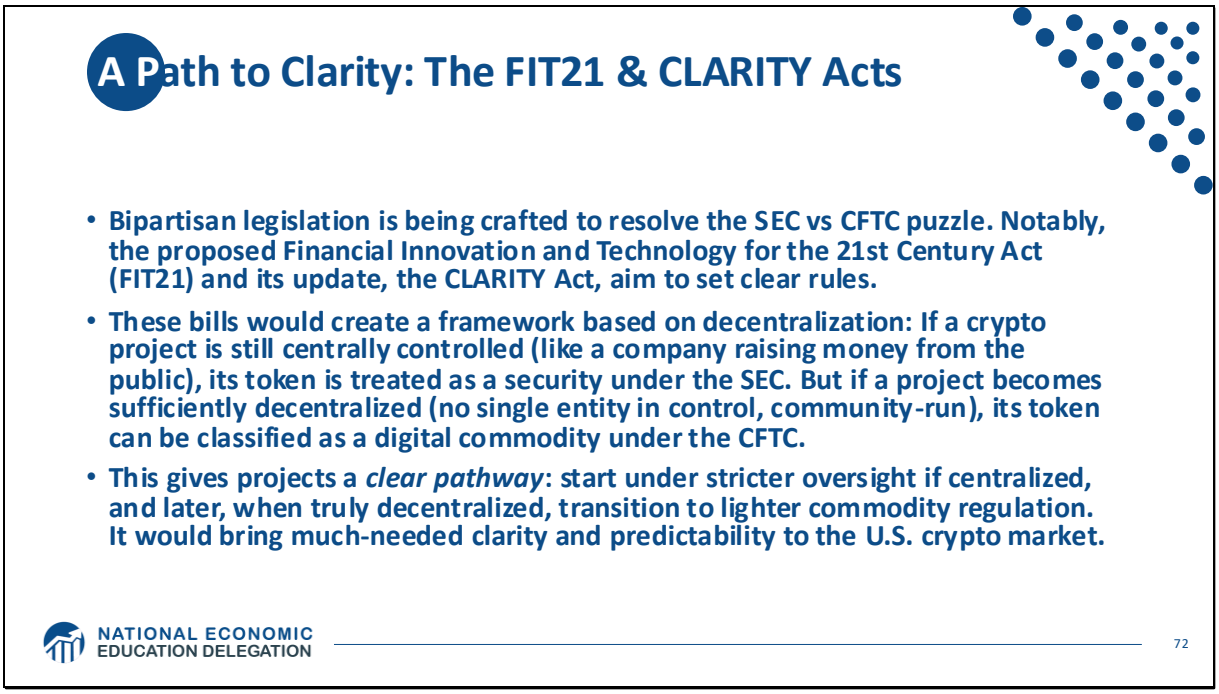
Today, we're in the midst of a fundamental shift. Governments and regulatory bodies around the globe are no longer ignoring crypto; they're actively working to lay down **clear "rules of the road."** This process is sometimes viewed with apprehension by early crypto adopters who preferred the totally unregulated approach. But it's a natural sign of the industry maturing. Frankly, clear regulations can be very positive: they **provide consumer protection**, reduce the risk for larger players (like banks or pension funds) to get involved, and generally create stability and trust that can pave the way for mainstream adoption.

We're watching the industry transition from the fringe toward the financial mainstream – essentially from the Wild West to Wall Street. This doesn't mean crypto loses its innovative spirit, but it does mean more oversight and structure.



Speaker Notes:
Let's get specific with the U.S., which is a major market: The central regulatory question here has been **"What is this stuff (crypto) and who regulates it?"** Crypto doesn't fit neatly into the old laws. We have two major financial regulators: the **SEC** and the **CFTC**, and they've had somewhat overlapping claims.
The **SEC** (Securities and Exchange Commission) is tasked with protecting investors in securities – things like stocks, bonds, etc. The SEC's stance is that *many crypto tokens are actually securities* under the law. Why? Because they're often sold to the public to raise money for a project or company, similar to a stock IPO (just without calling it stock). The SEC has been enforcing existing securities laws, essentially by suing or penalizing crypto projects and exchanges they believe violated those laws by, say, selling unregistered securities. From the SEC's perspective, if it quacks like a duck (raises money from investors with an expectation of profit from someone else's effort), it's a duck (a security). So they've gone after numerous crypto companies in the last few years.
The **CFTC** (Commodity Futures Trading Commission) oversees commodities and derivatives. The CFTC's view is that major cryptos (especially **Bitcoin**, and often **Ether**) look more like commodities – akin to digital gold or oil – rather than securities. They don't represent ownership in a company; they're more like assets people trade. The CFTC has even allowed Bitcoin and Ether futures trading on regulated exchanges. So CFTC says, hey, we should regulate crypto trading, at least for those considered commodities.

This overlapping jurisdiction has created a **regulatory gray zone and uncertainty** in the U.S.. One agency might say a token is a security, the other might consider it a commodity. Companies are stuck guessing which rules to follow, and some have faced enforcement without having clear guidance first (that's been controversial – "regulation by enforcement"). This uncertainty has arguably pushed some crypto businesses offshore or into caution. The good news is that efforts are underway to clarify this, which brings us to the next point: potential new legislation that defines who regulates what.



Speaker Notes:

To address the regulatory confusion, U.S. lawmakers have been working on landmark bipartisan legislation – notably something called the **Financial Innovation and Technology for the 21st Century Act (we'll call it FIT21)**, and a follow-up framework often referred to as the **CLARITY Act**. These bills are important because they don't just try to cram crypto into old categories – they propose a **custom-fit regulatory framework** for digital assets.

The core idea introduced is to use **decentralization** as a guiding metric. In simple terms, the law would work like this:

If a crypto project is launched in a way that's centrally controlled – say a company issues a token to raise money and is managing the network – then at that stage, it *behaves like a security*. It's a lot like a startup selling shares, so the SEC would regulate it.

However, if over time that project's network becomes **sufficiently decentralized** – meaning no single person or group controls it, it runs on a distributed community or network (think how Bitcoin or Ethereum have no central company in charge) – then the asset can be reclassified as a **digital commodity**, which the CFTC would regulate.

So projects could essentially "graduate" from SEC oversight to CFTC oversight as they decentralize. This makes intuitive sense: early on, investors need the protections of securities law (disclosures, anti-fraud, etc.), but once something is decentralized and functional, it's more like a public good/commodity and can be treated with a lighter touch.

This approach would provide a **clear path** for crypto projects, which is currently missing. It's

a major step toward giving legal clarity – entrepreneurs would know what box they fall into and what they need to do to move to the other box. It's still in proposal stages, but the fact it's bipartisan means there's real momentum. For the industry, this kind of clarity is huge: it reduces fear of arbitrary crackdowns and encourages innovation to stay onshore under clear rules.

U.S Crypto Legislation: GENIUS vs. FIT21 & CLARITY Acts

- GENIUS Act focuses on regulating stablecoin issuers (reserves, charters).
- FIT21/CLARITY Acts define who regulates digital assets (SEC vs. CFTC).
- CLARITY Act uses 'decentralization' as a key criterion for classification.
- GENIUS addresses payments and consumer protection; CLARITY addresses market structure.

Case Study: Hawaii's Journey to a Digital Oasis

- After years of being the most restrictive state for crypto, Hawaii has reversed course :
- From 2020-2024, its Digital Currency Innovation Lab oversaw $800 million in transactions.
- In 2024, restrictive requirements were eliminated, and by 2025, local exchanges are thriving.
- This shift has given 134,000 residents crypto access and is fostering a local blockchain ecosystem.

What is good regulation?

- The Principles Are Easy;
  1. Eliminate fraud, abuse and manipulation.
  2. Do not let markets be dominated by a small number of powerful firms.
  3. Allow startups with new innovations to displace incumbent firms.
  4. Minimize risk of a financial crisis.
- Legislation and Implementation: Hasn't Been Easy

Crypto Fraud Is Skyrocketing

- **Outright fraud is rampant. In 2024 alone, the FBI received nearly 150,000 crypto-related complaints, totaling $9.3 billion in losses—a 66% increase from the previous year. Older Americans are a primary target, with those over 60 losing a collective $2.8 billion.**

The Predatory Nature of Crypto ATMs

- Crypto ATMs, often marketed as tools for financial inclusion, are a growing site for fraud. They are frequently placed in lower-income and minority neighborhoods, where they charge excessive fees. In 2024, these machines were involved in scams totaling nearly $250 million in losses, with the elderly again being the primary victims.

Societal Harms and National Security

- Fueling Cybercrime: Crypto's Role in Ransomware
- Because it is difficult to trace, cryptocurrency is the preferred payment for cybercriminals. Ransomware attacks extorting hospitals, schools, and local governments have skyrocketed. These attacks disrupt critical infrastructure, from 911 emergency services to hospital operations, and are a direct threat to public safety.

A Tool for Illicit Markets

- Cryptocurrency is also a key facilitator in black markets, including the fentanyl crisis. Traffickers use crypto to launder money and evade law enforcement. Authorities in Arizona and California have traced crypto transactions to seize over five tons of fentanyl, and a single dark web operation serving all 50 states used Bitcoin for over $150 million in drug sales.

A Matter of National Security

- Adding another layer of risk, investigations have found that crypto mines in at least 12 states are owned or operated by entities with links to the Chinese government. Given the strategic importance of our energy infrastructure, this foreign control raises serious national security concerns about grid stability and potential surveillance.

Innovation in Crime-Detection Continues

- Bitcoin is pseudonymous, not anonymous – all transactions are public.
- Law enforcement uses blockchain forensics to track illicit activity.
- Criminals often caught when converting crypto to fiat (via KYC exchanges).
- Example: FBI has traced and seized billions in Bitcoin from criminal activity.
- Lesson: Blockchain transparency can help catch wrongdoers despite its perceived secrecy.

Institutional Adoption Continues

The Ultimate Sign of Legitimacy: Institutional Adoption

- **A major milestone in crypto's mainstream acceptance was the approval of spot Bitcoin ETFs in the U.S. (January 2024). These exchange-traded funds hold actual Bitcoin and allow investors to buy BTC exposure through regular stock markets (via their brokerage accounts).**
- **Financial giants like BlackRock and Fidelity launching Bitcoin investment products marked a watershed moment. It provides a regulated, familiar bridge for pension funds, corporations, and other institutional players to enter the crypto market. This influx of institutional interest adds a new layer of legitimacy and is driving the industry's maturation.**

Speaker Notes:

Perhaps the most powerful signal that crypto is entering the financial mainstream is the arrival of the world's largest, most conservative institutions. For years, **Wall Street largely sat on the sidelines** of crypto, seeing it as too risky or too loosely regulated. But that has fundamentally changed in the last couple of years.

The landmark event was the U.S. approving the first **spot Bitcoin ETFs (Exchange-Traded Funds)** in January 2024. An ETF is a regulated investment vehicle that trades on stock exchanges (like the NYSE or NASDAQ) and usually tracks some asset or index. A *spot Bitcoin ETF* holds actual Bitcoin in custody, and it issues shares that investors can buy and sell just like any stock. This means that now an investor can effectively buy Bitcoin by purchasing shares of an ETF in their normal brokerage account – no need to figure out wallets or exchanges or worry about private keys. It's Bitcoin exposure wrapped in a traditional, familiar package (with all the oversight that SEC-regulated funds require).

The fact that **BlackRock**, the world's largest asset manager, and **Fidelity**, a huge financial firm, among others, have launched or filed for these Bitcoin ETFs is huge. These are institutions that manage trillions of dollars. Their entrance was a watershed moment. It signals that crypto is no longer a fringe toy – it's being embraced as a legitimate asset class by the financial establishment.

For institutional capital – think pension funds, endowments, corporate treasuries – an ETF provides a compliant and easy way to invest in Bitcoin. And indeed since these ETFs were

approved, we've seen a surge of interest and inflows.
This institutional adoption brings a *new layer of legitimacy*. It's like a stamp of approval that crypto is here to stay. It also brings in more *liquidity and stability* (though also ties crypto more to broader market dynamics). It's a key driver of the ongoing maturation of the industry.
Of course, some crypto purists might joke that "we made a peer-to-peer currency only for Wall Street to repackage it and trade paper claims to it" – but from an adoption standpoint, it's significant because it allows far more people and big pools of money to participate in the market, which in turn generally advances development and acceptance.

Question-Do I Have To Pay Taxes?

YES.

The IRS treats cryptocurrency as property, not currency.

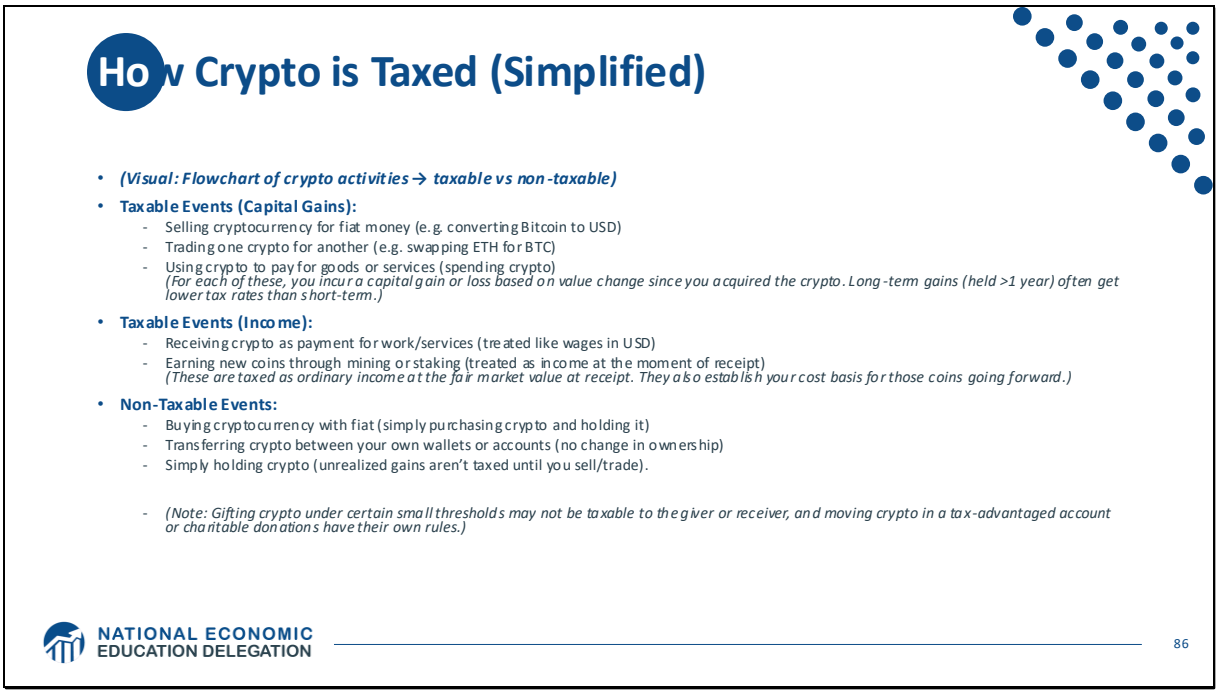
Question: Taxes?

- **Practical Question: Do I Have to Pay Taxes?**
- **Yes – crypto is taxed. In the U.S., the IRS considers cryptocurrency property (like stocks or real estate), *not* foreign currency. This means many crypto transactions are taxable events. Failing to report crypto gains or income can lead to audits or penalties.**

Speaker Notes:
Amidst all the regulatory debates, one thing has been perfectly clear from the U.S. government: **taxes**. So the question everyone eventually asks: *"If I use or invest in crypto, do I have to pay taxes on it?"* The answer is an **unambiguous yes**.
The IRS (Internal Revenue Service) has stated since 2014 that it views cryptocurrency as **property** for tax purposes. It's not treated like foreign currency (which has some different rules) – instead, it's akin to owning stock, or real estate, or gold in the eyes of the IRS. That classification has important implications:
Every time you **sell** cryptocurrency for cash, or **trade** one crypto for another, or **use** crypto to buy something, you potentially have a taxable capital gain or loss. It's as if you sold some property. You must calculate the difference between what it was worth when you acquired it and what it's worth when you disposed of it, and report that.
If you **get paid in crypto** for work, or **earn new coins** via mining or staking, that's treated as ordinary income – you owe income tax on the value of the crypto at the time you received it.
So yes, moving crypto around can trigger taxes. Simply buying and holding crypto isn't taxable (just like buying stock and holding isn't). But once you trade or sell, it is. If you move crypto between your own wallets, that's not taxable – because you still own it, it's like moving cash from your left pocket to right pocket.
The IRS is very serious about this. They have added a question about crypto on the front

page of the 1040 tax form now, asking if you dealt with digital assets. They are also implementing new reporting requirements: exchanges will be issuing a 1099-DA form to users and to the IRS to report transactions, similar to how stock brokers report your trades. The IRS has been cracking down on non-compliance – they've sent letters to tens of thousands of crypto users reminding them to pay taxes, and they've launched enforcement cases. Not reporting crypto gains can lead to penalties or worse.

So, short answer: **yes, pay your crypto taxes**. Treat it like any other investment property for tax purposes. Keep records of your buys and sells (many apps help with this). And consult a tax professional if you're not sure, because the rules (especially around things like airdrops or DeFi yield) can get nuanced. But ignorance isn't bliss here – the IRS is watching.



Speaker Notes:

Let me break down **how crypto is taxed** in practical terms (in the U.S. context) – here's a simplified guide:

Taxable Capital Gains Events:

Think of these like selling stocks or property:

Selling for cash: If you sell Bitcoin for USD, you have a gain or loss. For example, you bought 1 BTC at $10k and later sold at $20k, you have a $10k capital gain to report. If the reverse, you have a loss which might offset other gains.

Trading crypto-to-crypto: If you trade 1 BTC for 10 ETH, the IRS says you "sold" the BTC (and possibly "bought" ETH). So if that BTC had appreciated since you got it, that's a taxable event for the gain in USD terms. Yes, even if you didn't convert to dollars – trading one coin for another triggers tax on the gain/loss of the coin you gave up.

Spending crypto on goods/services: If you buy a cup of coffee with crypto, technically you sold some crypto. If that crypto went up in value since you got it, you owe tax on that gain (even if it's just a few cents). It sounds crazy for a cup of coffee, but that's how the law is currently written.

For capital gains, if you held the crypto for more than a year, it's a long-term gain and usually taxed at a lower rate (0%, 15%, or 20% depending on income). If you held for a year or less, it's short-term and taxed like ordinary income (your normal tax rate).

Taxable Income Events:

Getting paid in crypto: If your employer or a client pays you in Bitcoin, that is just like they paid you in dollars from a tax perspective. If on the day you received it, 0.1 BTC was worth $2,000, you have $2,000 of wage income (subject to income tax, and if you're an employee, it should be on your W-2).

Mining or staking rewards: The moment you successfully mine a block or receive staking interest, the fair market value of those new coins is taxable income to you. So if you mined 0.05 BTC and at that time it was worth $1,000, you have $1,000 of income. If you stake and get paid 5 ETH over the year at various times, you'd sum up the USD value at each time received and that's income.

For these, that establishes your cost basis going forward too. E.g. if you mined a coin at $100 (taxed as income then), and later sell it for $300, you'd pay capital gains on the $200 difference.

Non-Taxable Events:

Buying crypto with cash: Simply purchasing crypto with USD is not a taxable event. You might have to report that you have it (for record-keeping if later sold), but there's no gain yet.

Moving crypto between your own wallets or accounts: If I transfer Bitcoin from Coinbase to my personal Ledger wallet, that's not taxable – it's still my Bitcoin. (Important: make sure you track that transfer so later you can link the cost basis; many exchanges issue tax forms that could make it look like a withdrawal, so keep records that it wasn't a sale).

Holding crypto: If the value goes up while you're holding, that's an *unrealized* gain. In the U.S., we don't tax unrealized gains (yet), only when you sell or dispose.

Other notes (just for awareness, not on the slide):

Gifts: If you gift crypto to someone, small gifts (under ~$16k per year) usually have no tax for either party (beyond that, gift tax rules for the giver). If you donate crypto to a registered charity, you might not pay gains and could get a deduction if done right (like donating appreciated stock). But those are specifics beyond our main scope.

Also, starting in 2024, U.S. exchanges will be required to send the IRS and you a new form (likely 1099-DA) summarizing your gains, which will make compliance easier and more enforced.

So in summary: for taxes, keep good records of all your buys (date and price) and sells. Many people use crypto tax software that hooks into exchanges to calculate everything. It's wise to do so, because as this space matures, tax authorities are getting more and more data on transactions.

Alright, enough about taxes – the takeaway is: treat crypto income and trades with the same seriousness as stocks or other assets when it comes to taxes.

Transition to Next Steps

- ***So, you've seen the why, the how, the good, the bad, and the bigger picture. What should you do next?***

NATIONAL ECONOMIC EDUCATION DELEGATION

Speaker Notes:
We've covered a tremendous amount of ground today. We started with the real-world **problems** that give cryptocurrency its purpose. We then **demystified how it works**, with hands-on examples of wallets and transactions. We **weighed the opportunities against the risks** – the good and the bad. And we explored the **bigger picture** of the crypto ecosystem and how the world is adapting to it.
At this point you might be asking, "What should I do next?" or "How do I safely engage with all this information?" The goal of this session wasn't to turn you into an immediate crypto trader or to give financial advice; it was to provide knowledge and a framework so you can make your own informed decisions going forward. In closing, I'll leave you with a few guiding principles and key takeaways as your next steps.

A Closing Thought

"Blockchain is the tech. Bitcoin is merely the first mainstream manifestation of its potential." — Marc Kenigsberg

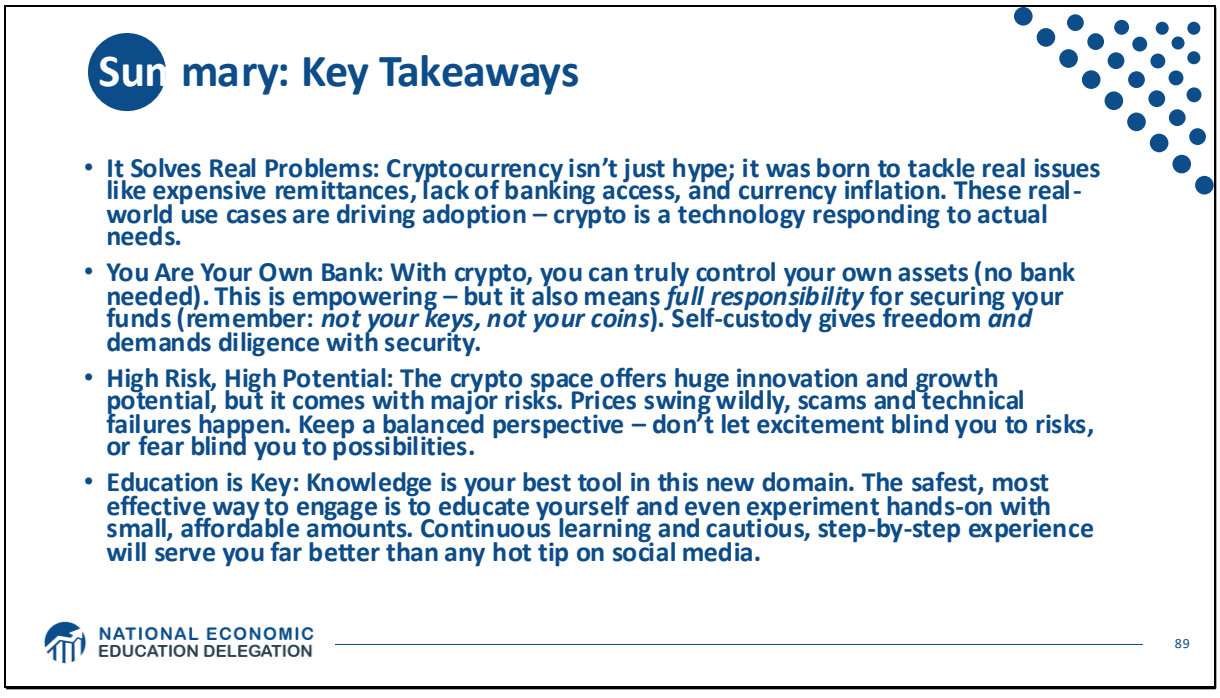
Speaker Notes:

We've covered a lot today – from the practical mechanics to the broader philosophy. We've seen how this technology can **empower individuals**: from a migrant worker in the Philippines sending money home with lower fees, to a saver in Argentina protecting their wealth from inflation. We've also confronted the **risks**: from wild market volatility to outright fraud and scams.

The key is to view cryptocurrency not as a get-rich-quick scheme or a magical solution to all problems, but as a **foundational new technology** – much like the internet was in its early days. As the quote from Marc Kenigsberg reminds us, *Bitcoin was just the first application*. The **underlying blockchain technology** is a platform for innovation that's still in its infancy. We're at the beginning of a long journey of development, much like the internet of the early 90s where email was the first mainstream app, and we couldn't yet imagine YouTube, Uber, or Facebook.

Our goal today wasn't to make you crypto experts overnight or to give you investment advice. It was to give you the knowledge and perspective to navigate this space safely and confidently. As you continue your own exploration, remember a few core principles: **start small**, **stay skeptical**, and **never stop learning**. Start with small amounts if you decide to dip your toes – amounts you can afford to lose – and learn by doing. Stay skeptical – question bold claims, do your own research, and trust data over hype. And keep educating yourself – this field evolves quickly, and knowledge is truly your best asset and defense here.

Blockchain technology has immense potential, but it’s up to each of us to approach it wisely and make the most of it.



Speaker Notes:

To wrap up our session, let's summarize the four most important takeaways:

First: Cryptocurrency is *not* a solution in search of a problem. It's addressing long-standing, real-world challenges. Think of those stories we discussed: exorbitant remittance fees that hurt families, billions of people who can't access banking, and savers watching their money evaporate in hyperinflation. Crypto offers *potential* answers to these issues by enabling cheaper transfers, more inclusive access, and alternatives to unstable currencies. It's not perfect or fully realized, but it's grounded in solving real problems, not just tech for tech's sake.

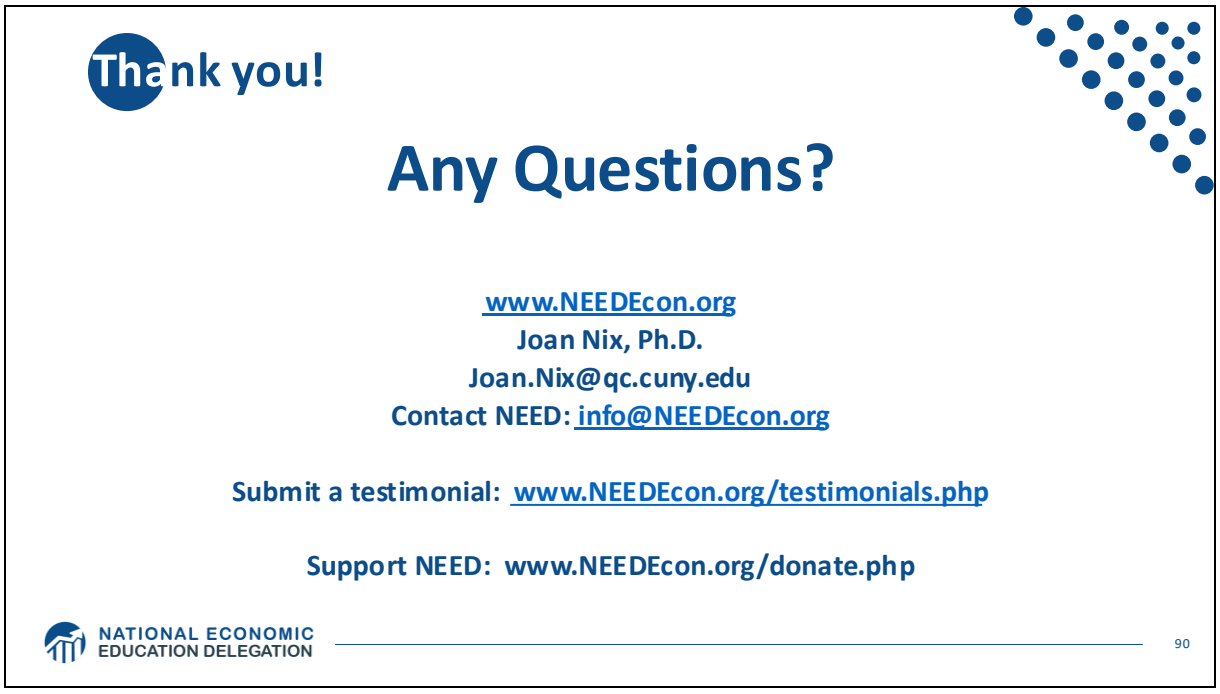
Second: The core principle of crypto is *self-custody* – you get to be your own bank. This is powerful: you have full control over your money without needing permission from intermediaries. But with that freedom comes absolute responsibility. There's no bank fraud department to call if you slip up. The phrase *"Not your keys, not your coins"* is paramount – it reminds us that if you don't hold your private keys (if you leave coins on an exchange or with a third party), you don't truly control them. So if you do take custody of assets, you must practice good security (hardware wallets, backups, etc.). *You* are in charge of safeguarding your wealth.

Third: This domain is one of both **high potential and high risk**. The opportunity for innovation, new business models, financial inclusion – all of that is immense. We might see blockchain tech underpin a new wave of the internet, new economic systems, who knows.

But on the flip side, we've seen how volatile and dangerous it can be: prices can crash dramatically, and scammers or hackers can cause major losses. It's crucial to maintain a balanced perspective. Don't get swept up in euphoria without minding the risks, and likewise, don't be so scared of the risks that you dismiss the entire innovation outright. **Balance and caution** are key.

Finally: Education is key above all. The best investment you can make in this space is an investment in learning. Start with knowledge *before* you commit significant money. I always say: learn first, *then* consider engaging with small, manageable amounts to get practical experience. The people who do best in crypto are often those who take the time to understand what they're doing, rather than chasing quick wins. And given how fast this field changes, never stop learning – stay updated, follow reputable sources, maybe even try out things on test networks or with tiny amounts just to understand how they work. Your knowledge and due diligence are your strongest defense against the risks here.

If you follow these principles – real-use focus, self-custody care, balanced risk awareness, and continuous education – you'll be well-positioned to navigate the crypto world wisely.



Thank you for your attention! We now have about **ten minutes for questions and discussion**. I'm happy to go back to any topic we covered or tackle any new questions you have. Whether it's something about wallets, regulations, a concept you want clarified, or even a skeptical challenge, feel free to ask. There are truly no bad questions with a subject this new and multifaceted. So, what would you like to discuss?

Resources

- E Prasad, *The Future of Money* (https://youtu.be/o3NuHb7V1IA)
- N. Mehta, et.al. *Blockchain Bubble or Revolution*
- E Prasad, *The Future of Money* (https://youtu.be/o3NuHb7V1IA)
- *Cryptoassets* – Chris Burniske & Jack Tatar
- *Digital Gold* – Nathaniel Popper

- Coinbase Learn: Simple, interactive lessons
- Binance Academy: Videos + quizzes, from beginner to advanced
- Coursera: "Crypto for Beginners" (U. of Michigan)
- MIT OCW: "Blockchain and Money" (advanced learners)

Speaker Notes:
Thank you once again for joining me today. Before we wrap up, I want to make sure you have avenues to continue learning on your own. I've compiled a list of **trusted, high-quality resources** for further exploration. **Happy learning, and stay safe out there!**

Resources

- Podcasts for On-the-Go Learning
- Unchained (Laura Shin): Interviews with experts
- Crypto Top Trading Signals: Market updates + education

Try It Yourself

- MetaMask Wallet (testnet version)
- Explore DeFi with Uniswap or Aave (no real money needed)