Cryptocurrencies & The Future of Money

Osher Lifelong Learning Institute at Boise State University

Joan Nix,
Associate Professor of Economics
Queens College, CUNY
February 27, 2024

NATIONAL ECONOMIC EDUCATION DELEGATION

Outline of the Talk

- What makes Bitcoin different?
- Is Bitcoin Digital Gold? Is it a store of value? Is it a medium of exchange?
- Pros and Cons of Bitcoin
- What about Ethereum?
- Are Smart Contracts the result of Genius level thinking by Vitalik Buterin? Should we struggle to understand a new way of computing?
- What about illicit activities?
- What are the market solutions to the problem of using crypto for illicit activities- Chainalysis and Elliptic.
- Are Stablecoins the solution to Crypto's volatility?
- Should the Fed compete in this arena with a CBDC?

NATIONAL ECONOMIC EDUCATION DELEGATION

ormation

Slides will be available from the NEED website tomorrow (https://needelegation.org/delivered_presentations.php)

Money- where does it come from?

- **There is over $2 trillion in notes and coins in circulation.**
- **"Yet it might surprise the man or woman on the street to learn that the lion's share of our money did not roll off the presses at either the Bureau of Engraving and Printing or the U.S. Mint."**

Banks are Important

- ". . ., by far and away the largest source of money within the U.S. economy is monetary liabilities—contractually enforceable promises—issued by private financial institutions."

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.**

Not everyone feels good about the current arrangements!

- "A new Coinbase report on the state of crypto has revealed the disillusionment of younger generations (Gen Z and Millennials) with the traditional American dream and **the financial system**. It shows **young Americans** are more open than older generations to unconventional paths to financial independence, such as crypto, than older generations.
- According to the report, young people find the American dream less achievable, partly due to high housing costs, inflation and an **outdated financial system**. Instead of following conventional paths, they are actively building new models of work, ownership and finance that are more flexible and don't rely on legacy intermediaries."

The user base is young

Screenshot of Coinbase's Q3 report. Source: Coinbase

- Younger generations are actively exploring fresh economic prospects.

  They are establishing the groundwork for a modernized system and a rejuvenated version of the American dream, empowered by technologies like cryptocurrency as a means to modernize the system, according to the report.

We have innovation- credit cards for online payments!

- **Credit cards were introduced in 1958 but didn't do so well at first because of massive delinquencies.**
- **But getting consumers to carry them and merchants to accept them was the key to developing a multi-billion dollar business.**

Will Bitcoin follow the same path?

- **Need users and merchants to make it a viable medium of exchange!**

Original story: no central bank

- **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.**

Original story : no central bank

- "At the time, Nakamoto discussed Bitcoin in a few narrow ways. Although he often responded to interested potential users or did outreach himself trying to bring the revolutionary technology in front of cryptography fans, hardcore coders and libertarians Nakamoto presented Bitcoin as a fairly utilitarian and spartan project. When someone created the first Wikipedia page for Bitcoin in July 2010, Nakamoto said it was too "promotional" for his taste.
- "Just letting people know what it is, where it fits into the electronic money space, not trying to convince them that it's good," Nakamoto added."

Original story : no central bank

- "But the chief innovation Nakamoto knew from the beginning was that **Bitcoin has no central issuer, or "mint,"** as he sometimes called it. "There isn't a central mint or company running it. As long as there are users, it survives," he wrote in that 2010 email . . ."

Original story : no central bank

- Asking a Central Banker if he likes Bitcoin is like asking a King if he likes Democracy!

But wait!

- Regulatory structure and the existence of a lender of last resort are needed to trust that the banking system's model of borrowing short-term and lending long-term works out okay most of the time. Correct? Yes, but what about a different model for creating value that transfers across the internet?

No central bank to the rescue!

- Bitcoin's protocol fixes Bitcoin's supply!
- New Bitcoin does not come from the Bureau of Engraving and Printing or the U.S. Mint or Banks, it comes from solving a puzzle.

Solving a puzzle?

- That's right- a puzzle, but not the kind a human solves for fun.

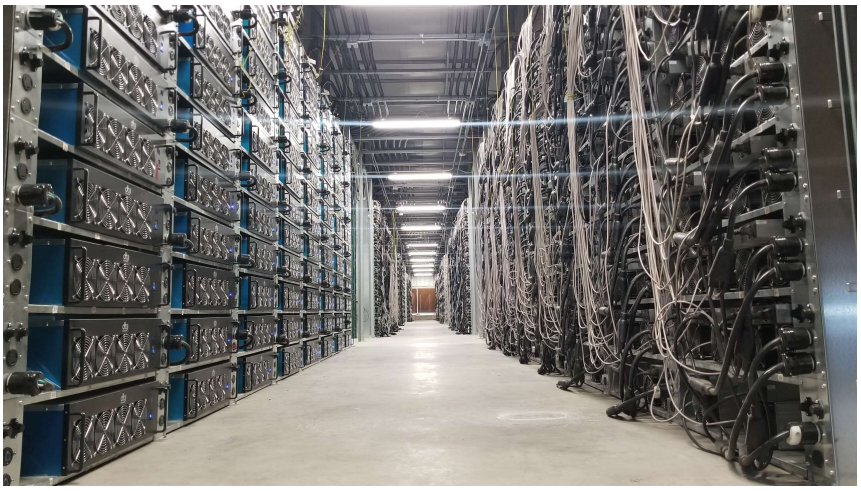
Proof of work: Bitcoin “mining”

- The miners’ competition involves generating long, random numbers (“hashing”) until one of the numbers fits a precise set of attributes.
- Presently, miners produce on the order of 200 million trillion random numbers per second. The miners use dedicated hardware for this job.
- The winning miner then adds the new block to the previous block in the blockchain. The total process takes about 10 minutes.

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 mine



Bitcoin's environmental impact

Annualized Total Bitcoin Footprints

Carbon Footprint	Electrical Energy	Electronic Waste
51.60 Mt CO2	92.51 TWh	51.63 kt
Comparable to the carbon footprint of **Sweden**.	Comparable to the power consumption of **Philippines**.	Comparable to the small IT equipment waste of **the Netherlands**.

Source: https://digiconomist.net/bitcoin-energy-consumption

So how does it work?

- Bob, exchanges dollars for Bitcoin. There are a number of ways to do this. The easiest is to set up an account at a crypto exchange like Coinbase, deposit dollars using your debit card, and one click is all you need to purchase Bitcoin.
- But the ownership of Bitcoin is not legally defined in terms of property rights like your checking account.
  - For example, if the exchange goes under, there is no deposit insurance, and you become an unsecured creditor of the exchange.

So how does it work?

- Another way is through a wallet (think of it as a piece of software) that generates keys for each transaction.
- There are private keys that only you should see and public keys that anyone can see.
  - Public keys act like a mailing address.
- "Not your keys, not your Bitcoin" is a motto of the Bitcoin maximalists.

So how does it work?

- Bob can send his Bitcoin to Alice by using Alice's public key and verifying that he has unspent output to send to Alice by signing the transaction with his private key.
- The new transaction waits its turn to be confirmed and added to a new block of transactions on a large number of different computers that make up the Bitcoin blockchain. The wait for small valued transactions to get confirmed averages about an hour until the transaction is safely on the blockchain.
- Bitcoin Miners gather about 3000 new transactions into a "block."
- A decentralized mechanism is involved because the state of affairs regarding confirmed transactions is widely shared across computers with the Bitcoin blockchain.

Where the rich store their keys!

Question

- 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.

This sounds complicated

- Is Bitcoin the future of digital payments?

  No!

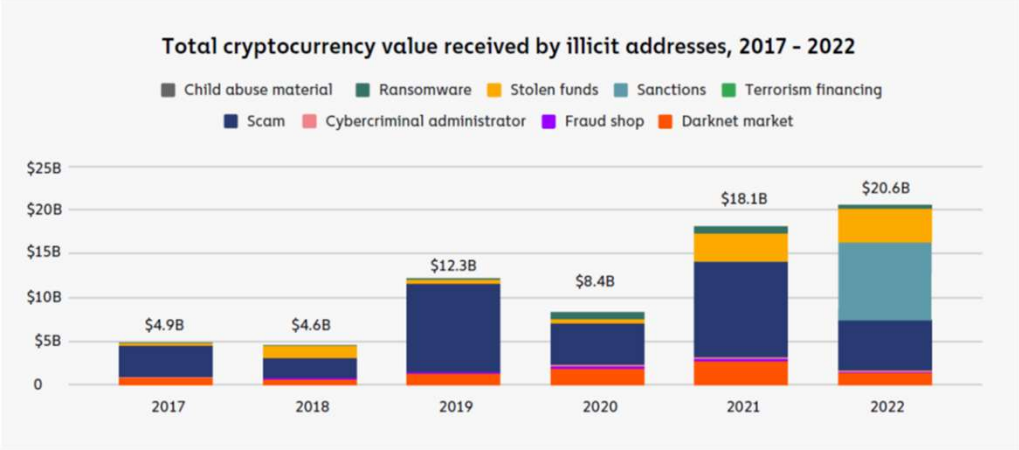
1) Extreme volatility
2) Exchange rate differences across exchanges.
3) Fraud
4) No rewards like credit cards offer
5) Few merchants accept it

Pros of Bitcoin?

Yes:

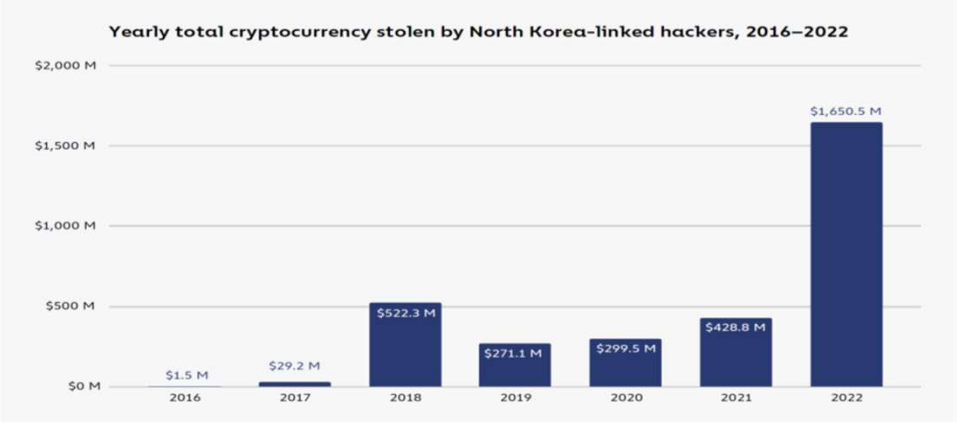
- **Micro-transactions will become cheaper than using credit cards.**
- **Cheaper for merchants to use Bitcoin, with a 1% transaction fee compared to 2.0-3.5% with credit cards.**
- **Remittances are much cheaper compared to Western Union.**
- **Global transactions are easier.**
- **Venture capital is flowing into this space, suggesting entrepreneurs are going to find solutions to some of Bitcoin's problems.**

Is Bitcoin bad money?



Source: *The 2023 Crypto Crime Report*, Chainanalysis, 2/23

Kim Jong Un's new revenue source



NATIONAL ECONOMIC EDUCATION DELEGATION

Source: *The 2023 Crypto Crime Report*, Chainanalysis, 2/23

Terrorist financing

- **"Crypto is 'a problem' but it is not the main source of funding for Hamas,** said Shlomit Wagman, a Harvard scholar and former chair of the Israeli Money Laundering and Terrorism Financing Prohibition Authority, who testified at a Senate Banking Committee hearing on terror financing this week.
- State actors, like Iran and Turkey, are the main funding drivers for Palestinian terrorist groups, followed by business portfolios with real estate and investments, humanitarian aid and fund-raising, including crypto."

NATIONAL ECONOMIC EDUCATION DELEGATION

Ledger characteristics - Can find out much from tracing addresses

Some aspects of crypto may limit its use by terrorists.

- The open digital ledgers where crypto transactions are recorded can be (and are) traced to catch bad actors.
- In April, Hamas's armed wing announced it would stop Bitcoin fund-raising because the activity was tracked and exposed donors.
- Yaya J. Fanusie, the head of the anti-money laundering unit at the industry group Crypto Council for Innovation, told DealBook that a terrorist crypto crowdfunding campaign "is like putting your bank account number on the internet and telling people 'donate to Hamas here.'"

Ledger characteristics - Can find out much from tracing addresses

- **Market solution- Firms such as Chainalysis and Elliptic provide services to law enforcement. Services that create distributions of addresses that trace to real-world identities**

But what about as an financial investment?

- It is hard to argue with the fact that Bitcoin has provided outsized returns for many, albeit very volatile.
- Financial assets are promises by the issuer
- The "fundamental value" of a financial asset is the value of those promises based on the time value of money and the risk that the promises will not be kept.
- What does Bitcoin promise?

How did Charlie Munger think about the stock market?

- We have a liquid stock market which is two things at once
  1. it's a place for people who are doing long-term investments rationally to go and make their transactions, and
  2. it's a place for another bunch of people to do casino gambling.
- If we mix them up totally it would be an absolutely insane thing for the country. It would work a lot better if we didn't mix up
- Now they trade billions of shares every day. And the computers are trading with one another. One computer algorithm is trying to outwit the other. Now, what earthly good is it for our country to make the casino part of Capitalism more efficient and more attractive, and more seductive? It's an insane public policy.

dience Feedback

- Do you agree that Bitcoin is an example of a development that belongs in what Charlie Munger called “the casino part of capitalism?”
- A) Yes
- B) No.

Do crypto assets have technological legs to stand on, or are they a fancy way to gamble?

- “The internet is incomplete”.
- There is no denying that the web has brought us endless abundance. But it’s missing two critical components:
- Internet users do not have digital property rights.
- The internet does not have a credibly neutral, shared, secure, permissionless, global accounting system — to record the state of its users and enable global commerce on one shared ledger.

Do crypto assets have technological legs to stand on, or are they a fancy way to gamble?

- Internet users do not have digital property rights.
- The internet does not have a credibly neutral, shared, secure, permissionless, global accounting system — to record the state of its users and enable global commerce on one shared ledger.
- This is the core value proposition of public blockchains — which are installing a new data layer into the internet.
- We take the concept of ownership and property rights for granted when it comes to our physical reality.
- Yet we struggle to make the same connections to our digital lives."

dience Feedback

Why are Baby Boomers reluctant to invest in Bitcoin?

- A) Too confusing to understand its value proposition.
- B) The main use case is criminal activities.
- C) The current system works fine.
- D) All of the above.

Do crypto assets have technological legs to stand on, or are they a fancy way to gamble?

- "This means that the digital economy relies on centralized services to maintain the ledgers and the state of internet users across time. As a result, the economic activity of billions of individuals globally is recorded and stored by a handful of private internet businesses — which control both the user interface and the database/accounting ledger."

Do crypto assets have technological legs to stand on, or are they a fancy way to gamble?

- "To grasp the magnitude", we'd like you to consider the potential impact of a global ledger & and computing platform such as Ethereum:

1) It can securely connect 8 billion people globally.
2) All the world's financial assets could be securely stored and transacted globally in a peer-to-peer manner on this ledger.
3) It has the potential to remake just about every business model on the internet via the introduction of smart contracts and digital property rights.

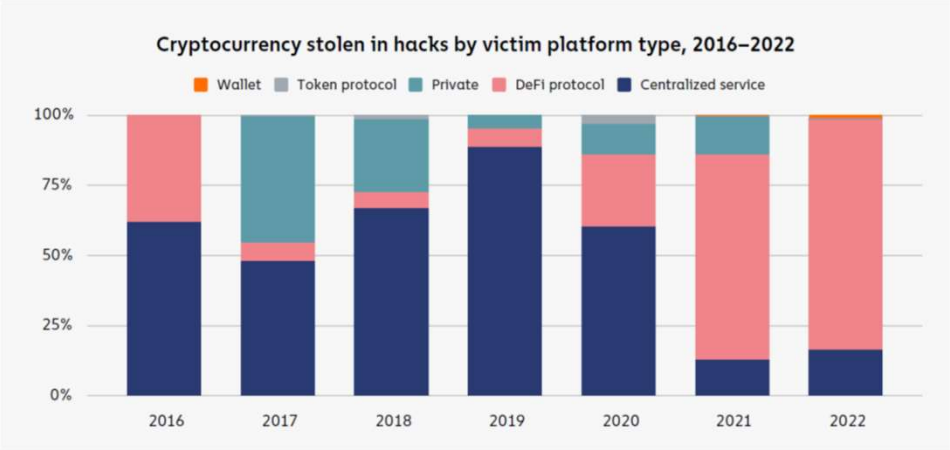
Do crypto assets have technological legs to stand on, or are they a fancy way to gamble?

4) **B2B interaction could be fundamentally transformed — with shared ledgers + automation via smart contracts (ERP for business interactions).**
5) **The global financial services industry could utilize this ledger for payments, trading, settlement, custody, lend/borrow, and ownership records.**
6) **Art, collectibles, music, gaming, brand loyalty/advertising, digital content, digital identity, social media, web hosting, and cloud computing business models could leverage this new ledger & computing platform — creating net new markets in the process.**

Smart contracts on the blockchain

- **A Smart Contract is a computer code that resides on the block chain and is executed based on incoming information.**
- **Example, Parametric Hurricane Insurance via the Blockchain:**
  - Computer program on Ethereum continuously monitors Charleston Executive Airport wind speed for 1 year.
  - If the windspeed is greater than 150 miles per hour, 100 bitcoin is immediately transferred to the Seabrook Island Property Association.
  - If the windspeed is less than 150 miles per hour, but more than 125 miles per hour, immediately transfer of 75 bitcoin; etc.
- **Smart Contracts are Automatic, Immediate, Irreversible and Uncontestable.**

Clearly, not good news for Defi



Source: *The 2023 Crypto Crime Report*, Chainanalysis, 2/23

NATIONAL ECONOMIC EDUCATION DELEGATION

45

The value of the new technology?

- **Don't Throw the baby out with the bathwater!**
- **The value of cryptographically protected digital tokens is nuanced:**
- **Blockchain technologies have significant promise some of which is already being realized.**
  - Private blockchains, Walmart and its produce suppliers
  - Public Blockchains, Ethereum and smart contracts

See: Mehta N,. Agashe A., P. Detroja *Blockchain Bubble or Revolution,* 2021

NATIONAL ECONOMIC EDUCATION DELEGATION

46

Also, crypto assets are still small in scale

- Bitcoin was the first and largest in terms of market cap (total value of all Bitcoins) of about $979 billion.
- Ethereum is in second place with a market cap of about $359 billion.
- Presently, there are 8,868 different varieties with a total market cap of about $2 trillion. (https://www.coingecko.com/en)
- The market cap of domestically listed US companies is about $40 trillion.

Need regulations to protect investors and allow for innovation.

- Gary Gensler, Chair of the SEC
- Rostin Benham, Chair of the CFTC
- Janet Yellen at Treasury.
- They will act, but they would need Congressional legislation, too: Cash markets in cryptocurrencies are viewed as commodities and face light touch regulations.

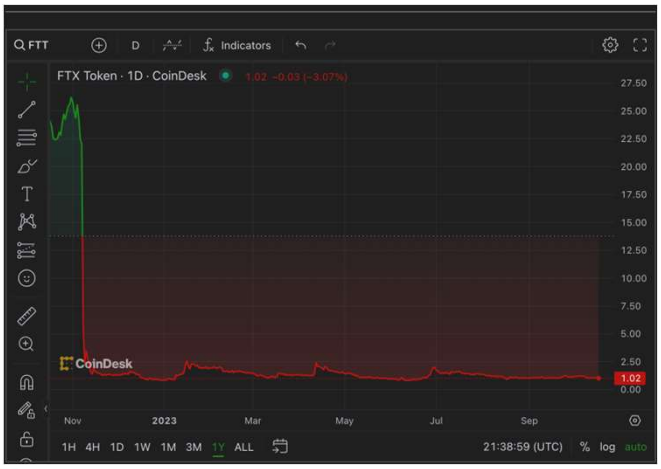
Sam Bankman-Fried & FTX

- In August, *Fortune* compared the 30-yr old to Warren Buffet.
- Helped save BlockFi and other crypto firms in May 2022.
- Mid-November $32b firm declares bankruptcy; SBF's net worth goes from $16 billion to 0.
- Misused customer funds to prop up his investment firm Alameda Research.
- Regulation is needed! Same as Traditional finance or different?

Another sad tale of hubris

- But wait . . .
- "John J. Ray III is the new CEO of FTX.
- In his eyes, he has been handed a complete mess.
- 'Never in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred here,' he said in a court filing."

Governance token of FTX



NATIONAL ECONOMIC EDUCATION DELEGATION

dience Feedback

- If Bitcoin drops significantly in value, the Federal Reserve will serve as a lender of last resort and buttress its value through buying Bitcoin.
- A) True
- B) False.

Gemini exchange offered an earn product

- "One of the Earn investors was Complainant No. 1, a 73-year-old mother, grandmother, and resident of the State of New York. She and her husband, who are both retired, invested their life savings of over $199,000 in Earn because they believed Gemini's marketing statements that Gemini was a safe and secure choice. Complainant No. 1 had hoped to use this money to pay for her grandchild's education. Outside of her Earn investment, she and her husband have little savings."

Believe it or not?

- According to the NYAG, Gemini knew their exposure to Genesis was high risk, but continued to promote the Gemini Earn lending product to retail customers as a safe way to earn profits on their crypto holdings.
- According to the NYAG, Gemini at one point revised its internal evaluation of Genesis' creditworthiness to "junk grade", some of their own risk personnel withdrew their own funds from the Gemini lending program, and one exec compared Genesis' condition to the Lehman Brothers shortly before its collapse — but no communication was ever made to customers to inform them that the product had become riskier, nor did Gemini ever really stop working with Genesis (despite gestures at doing so a month or two before Genesis ultimately halted withdrawals)."

Who should know what?

- "Another Earn investor, Complainant No. 2, is a 56-year-old resident of the State of New York. Complainant No. 2 invested approximately $20,500 in Earn, virtually all his savings. Complainant No. 2 chose Earn because he researched the product and came to believe, based on Gemini's statements, that Earn was more secure than other interest-bearing cryptocurrency investments."

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

Can we turn our back on digital money?

- The Bank for International Settlement (BIS) and a number of central banks are exploring how the development of Central Bank Digital Currency (CBDC) "contribute to an open, safe and competitive monetary environment that supports innovation and serves the public interest."
- CBDC would be a government-backed stable coin
  - Retail vs wholesale
  - Blockchain
  - Privacy

Source of quotes, BIS *Annual Report* 2021

The devil is in the details

- Many countries as diverse as Sweden, Ecuador, and China have begun experiments with CBDCs.

- Where's the Fed?

Source: E. Prasad, *The Future of Money*

Who should design our payment system?

Glossary

- *Traditional Money* is currency plus bank checking accounts.
- *Currency* is paper and coin issued by the government. Currency is legal tender and must be accepted for all debts. Transactions using currency are *immediate* and *final* (can't be undone without the agreement of both parties.)
- *Digital Payments* are used for purchases where no physical money is exchanged. Examples include many online banking payments, credit card payments, PayPal.
- *Digital Currency* or Virtual currency is a form of money that exists solely in digital form, such as a *digital token* (i.e., as data on a computer). Examples: cryptocurrencies, central bank digital currencies and virtual currencies used in online gaming.
- *Cryptographic identity protection* assigns people two account numbers, or *keys*, one public and one private. Public record keeping is done using the public key and transactions are authorized using the private key.
- *Cryptocurrency* is a digital currency where the owner's identity is protected using cryptographic encryption and where record keeping is done with a public blockchain, e.g., Bitcoin.
- *Stablecoin* is a cryptocurrency with a stable value of $1, somewhat like a money market mutual fund.

Glossary (Cont.)

- *Distributed ledger* is a database for recording transactions or other information, where the information or ledger is shared on a network of many computers simultaneously.
- *Blockchains* are distributed ledgers where new transactions (new blocks) are added to the chain sequentially when a consensus of the network agrees that the transactions are valid.
- *Decentralized Finance (DeFi)* is peer-to-peer financial activity conducted through public blockchains and smart contracts.
- *Smart Contracts* are computer programs that execute automatically based on external conditions. Example, travel insurance that pays off automatically when a flight is cancelled.
- *Central Bank Digital Currency (CBDC)* is a digital currency issued by a central bank. Different central banks are experimenting with various forms of CBDCs, including some using blockchain technology, electronic wallets and cryptography.

Resources to Learn More

- N. Mehta, et.al. *Blockchain Bubble or Revolution*
- E Prasad, *The Future of Money* (https://youtu.be/o3NuHb7V1IA)
- Presidential Working Group on Financial Markets, 11/1/21 (https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf)
- Federal Reserve White paper (https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf)
- Executive Order: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/

Economic Needs Don't Go Unmet for Long

Meeting the Banking Needs in Less Developed Countries: Mobile Money.

M-Pesa:

1. Started in Kenya in 2007 and now available in 10 countries.
2. Buy M-Pesa credits from "agents" (local shop) which can be transferred to others with an M-Pesa account via cellphone.
3. 96 percent of Kenyan households have a mobile account

Grameen Foundation:

Making Cash Digital is the Key to Possibility

When Poor Women Control their own money, it no longer controls them.