Taking the Cryptic out of Cryptocurrency

Ally Hoffman, Senior Cybersecurity Risk Specialist

Federal Reserve Bank of Dallas

SFSP
System Fintech Supervision Program

Objectives

- Define “digital assets” and identify different types, focusing on cryptocurrencies
- Introduce cryptocurrencies and their underlying motivation, supporting technologies, and common applications
- Describe some of the problems cryptocurrencies were created to solve and how they attempt to solve them
- Identify and describe the similarities and differences between types of cryptocurrencies
- Understand how early cryptocurrencies build upon one another and upon existing technologies to enable the current digital asset ecosystem

Agenda

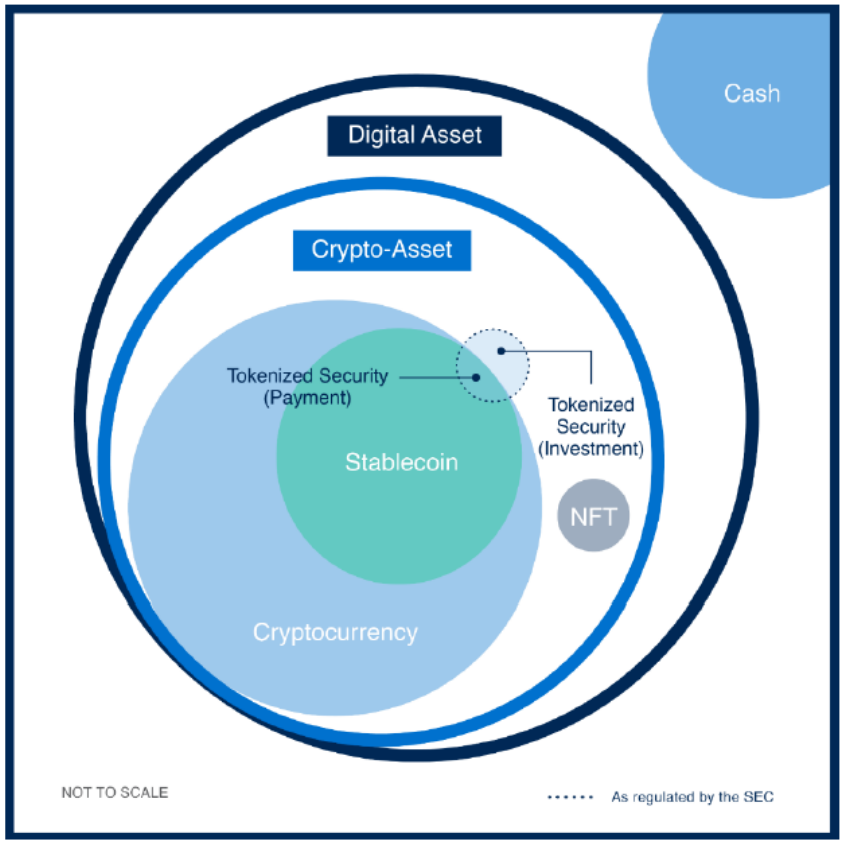
- What are Digital Assets?
- Bitcoin
  - The Origin of Bitcoin
  - The Problem Bitcoin Tried to Solve
  - How Bitcoin Works
  - Consensus Protocols
- Ethereum
  - Bitcoin vs. Ethereum
  - Smart Contracts
  - Tokens
- Stablecoins
  - How do Stablecoins Differ from Bitcoin and Ether?
  - Why do We Need Stablecoins?
- Appendices

Digital Assets

What are Digital Assets?

- Digital Assets span a broad range of asset types, each an electronic representation of value
- Crypto-assets are a type of digital asset that employs cryptographic techniques
- Crypto-assets include cryptocurrencies, which are used as a means of value transfer
- Stablecoins are a type of cryptocurrency

Figure 1. Digital Asset Taxonomy



Bitcoin

The Origin of Bitcoin

- **Who Created Bitcoin?**
  - Bitcoin was invented by the pseudonymous Satoshi Nakamoto
  - Nakamoto first described Bitcoin in the *Bitcoin White Paper*, published in October 2008
  - Bitcoin officially launched in January 2009

- **Why Did they Create It?**
  - The Problem:
    - Online transactions are overly reliant on trusted third-party intermediaries, which increase cost and inconvenience for users
  - The Solution:
    - "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

Nakamoto First Announces Bitcoin in "The Cryptography Mailing List," October 31, 2008

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

Headline from *The Times* (01/03/09) Referenced in Bitcoin's Genesis Block


THE TIMES

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

The Problem Bitcoin Tries to Solve

- **Restating Nakamoto's Solution in Simpler Language…**
  - Peer-to-peer
  - Online payments
  - Using electronic cash
  - Not reliant on a third-party (e.g., a financial institution)

- **Main Challenges with Implementing this Proposal**
  - Without a trusted third-party, how can two unknown parties trust one another in an online transaction using electronic cash?
    - Does the person sending you e-cash even have the e-cash to send?
    - Is the e-cash real or counterfeit?
    - Will they try to send that same money to someone else?
    - Will they try to claw the money back after they've sent it?
    - How can I prove that the money belongs to me and not to someone else?
  - How can this process be scaled?

How Bitcoin Works

- **Bitcoin consists of four main elements:***
  - **Blockchain:** A shared, public ledger that directly records all transactions
  - **Bitcoin Protocol:** A decentralized peer-to-peer network to validate and broad transactions, updating the ledger
  - **Consensus Protocols:** A set of rules for each node in the network to independently validate transactions and for issuing new Bitcoin
  - **Proof-of-Work Algorithm:** A mechanism for reaching a global, decentralized consensus on the valid blockchain

* Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly, 2017.

Bitcoin's Four Main Elements: Blockchain

Blockchain: A public transaction ledger

- A public record of the Bitcoin network's entire transaction history
- Not a list of accounts and balances, but this can be easily derived, e.g., by wallet software
- Represented as lists of transactions that are grouped into "blocks" (*see next slide*)
- As transactions accumulate over time, new blocks are added approximately every 10 minutes
- Each block is cryptographically linked to the prior block such that any change to a block will cascade across all subsequent blocks*

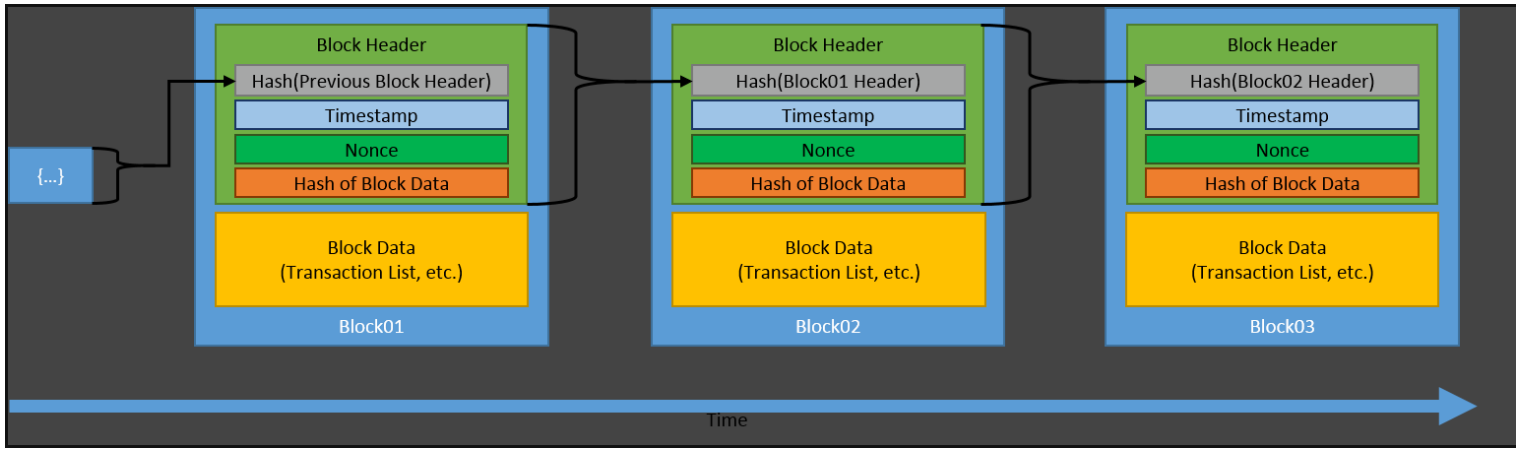
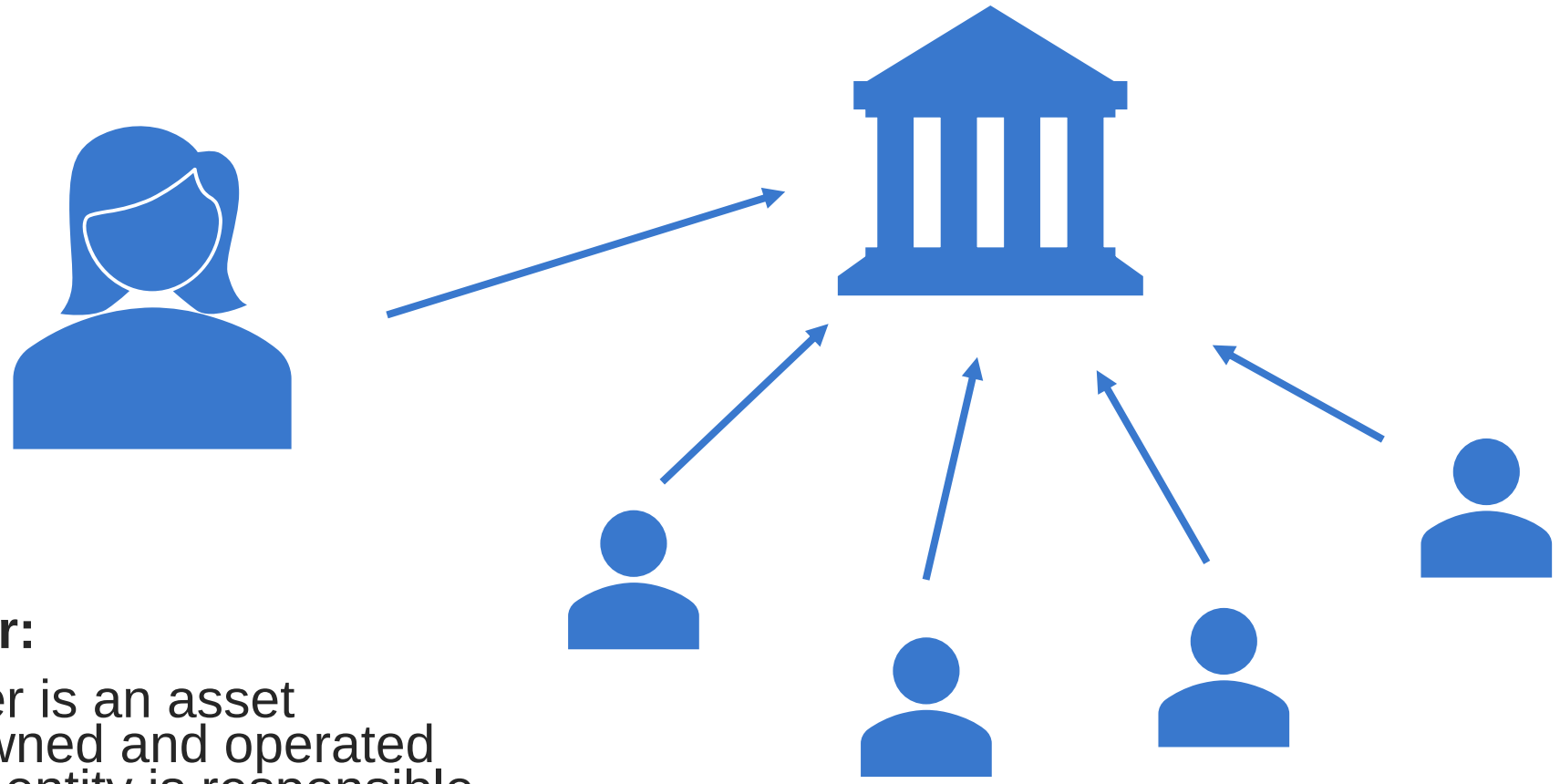


Image source: Blockchain | NIST

**Refer to "Cryptographic Hash Function" slides Appendix for technical details.*

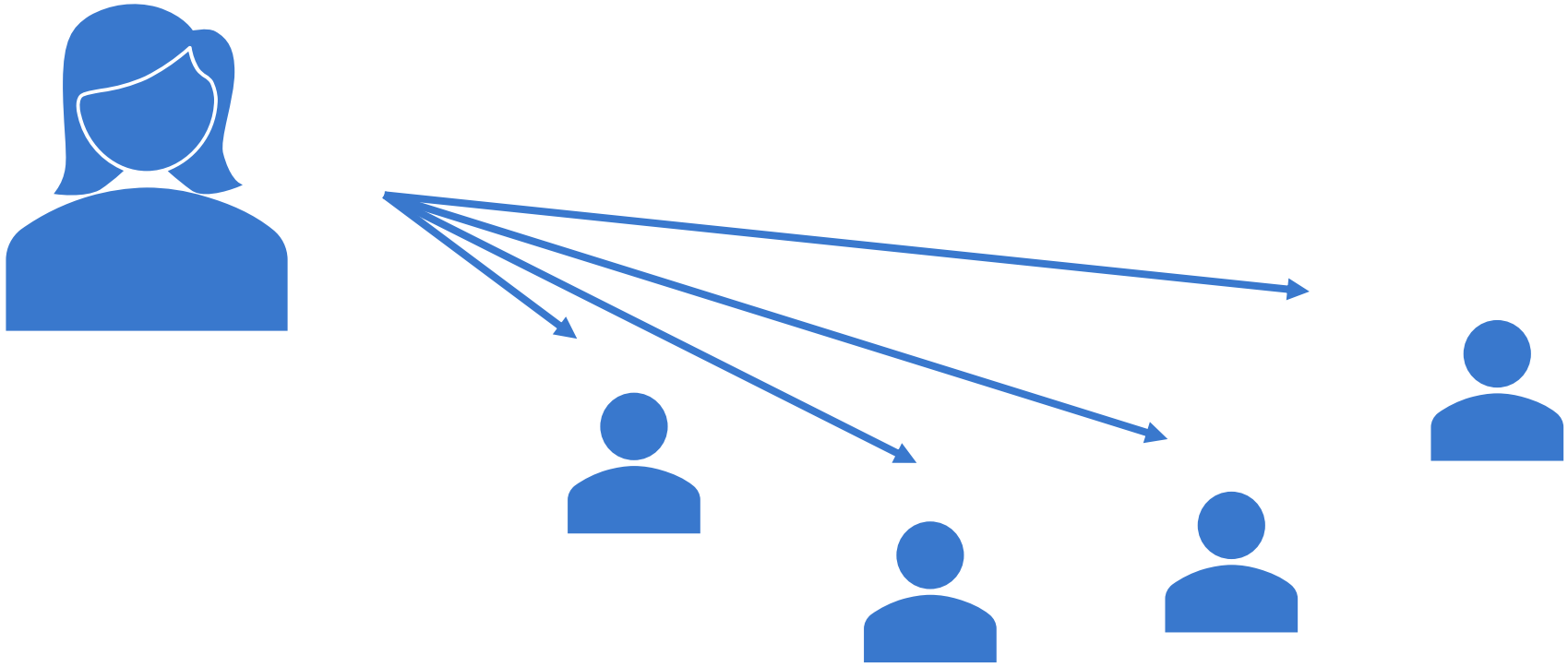
What is Blockchain?



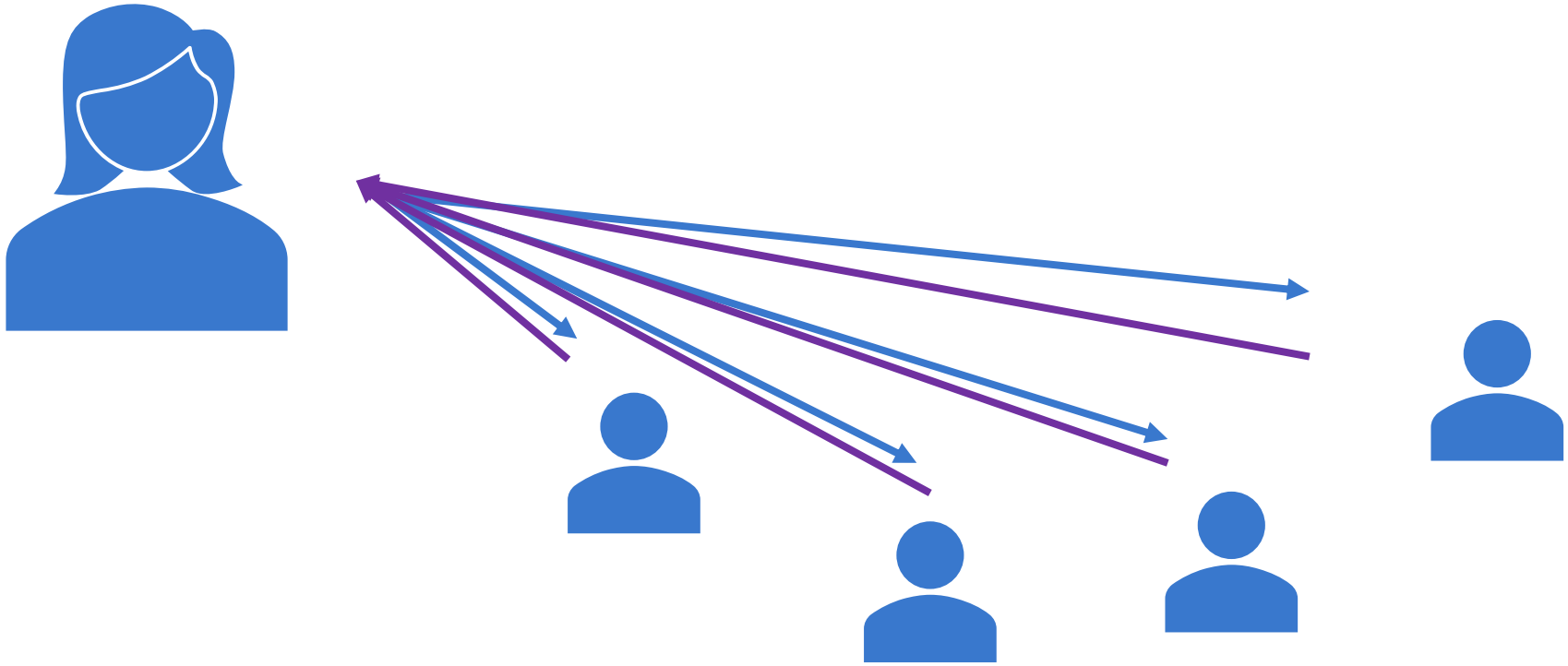
Centralized ledger:

A centralized ledger is an asset database that is owned and operated by one entity. That entity is responsible for maintaining and securing the data.

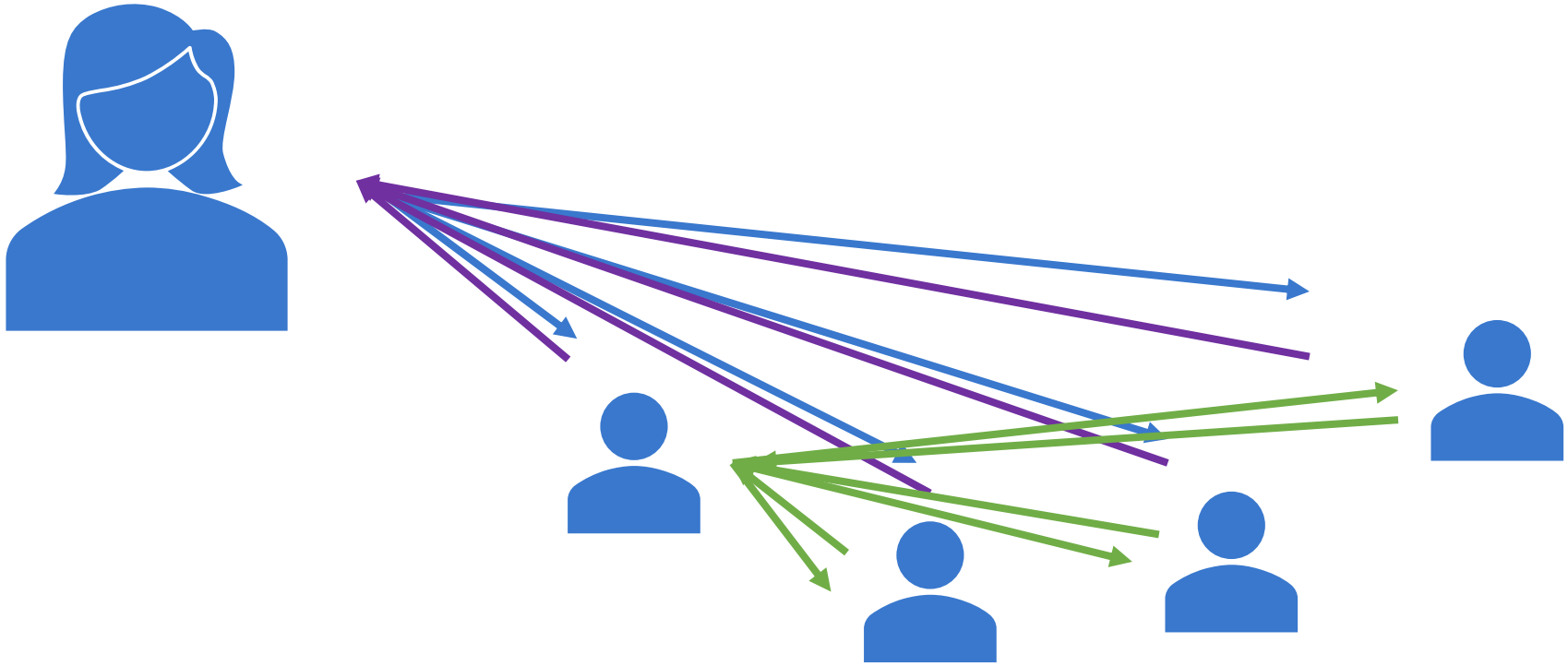
What is Blockchain?



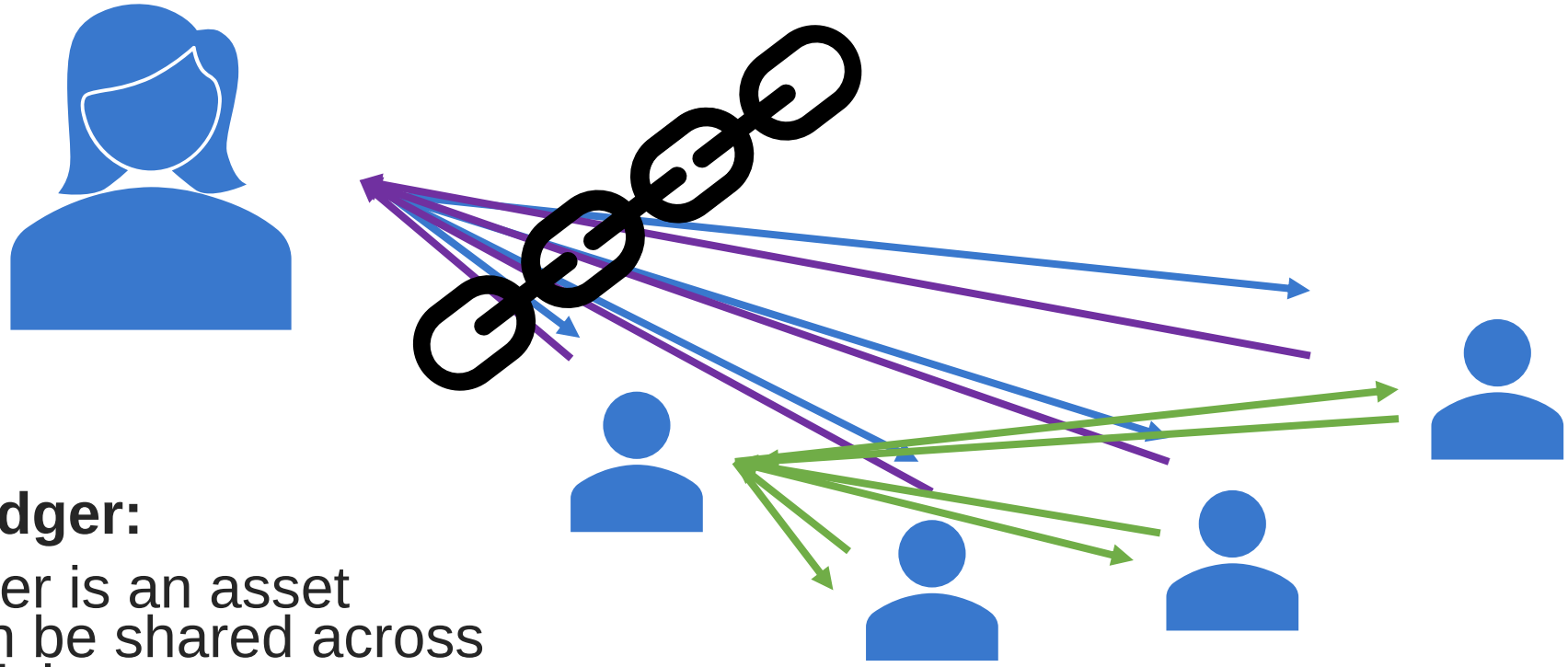
What is Blockchain?



What is Blockchain?



What is Blockchain?



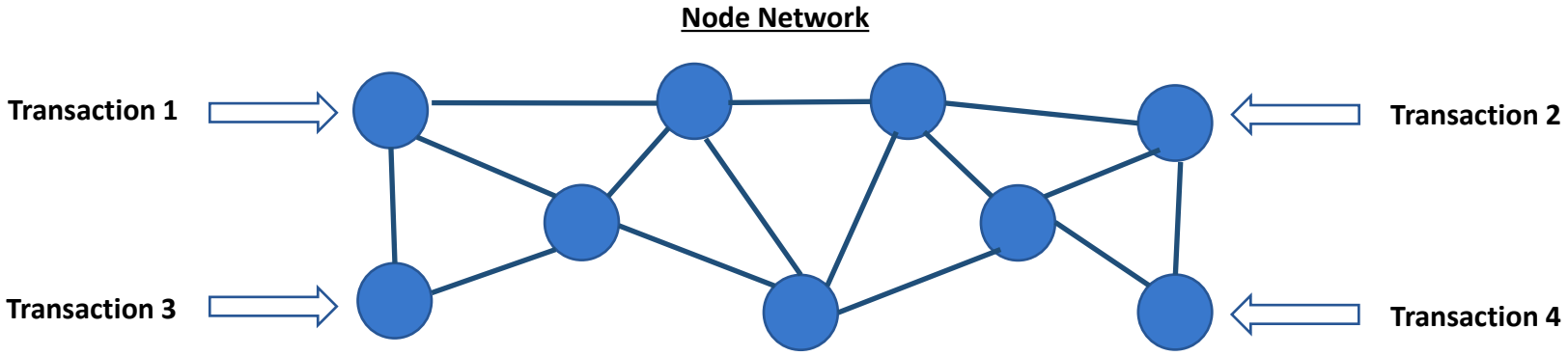
Decentralized ledger:

A distributed ledger is an asset database that can be shared across a network of multiple computers, geographies or institutions.

Bitcoin's Four Main Elements: The Bitcoin Protocol

The Bitcoin Protocol: A decentralized peer-to-peer network

- A decentralized network of computers, or "nodes", that perform various functions:
  - Verify and route new transactions to other nodes to update the ledger
  - Maintain copies of the full blockchain database
  - Mine new blocks
  - Provide wallet services to users
- Nodes may perform some or all of these functions
- Key Takeaway: nodes independently validate new transactions, update the ledger with validated transactions, and route those transactions to neighboring nodes



Bitcoin's Four Main Elements: Consensus Protocols

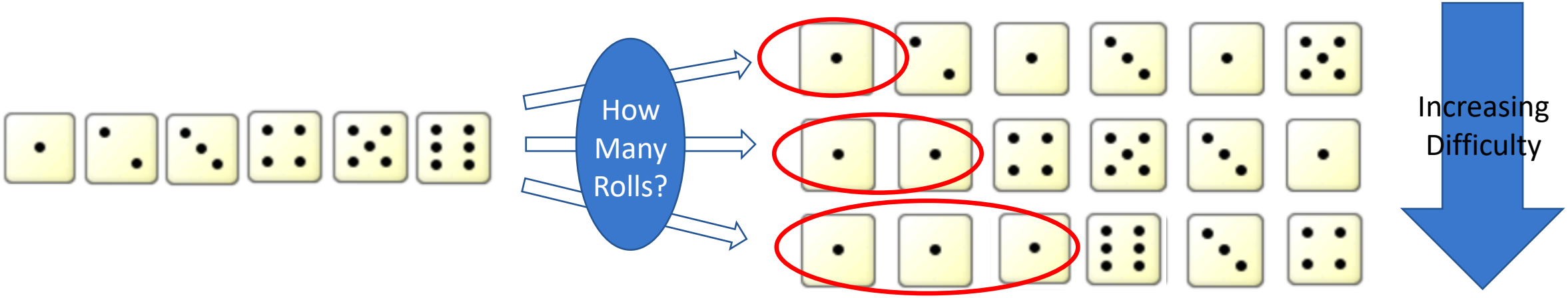
Consensus Protocol: A set of rules for independently validating transactions and for issuing new Bitcoin

- Ensures that the network can be trusted to independently update the ledger and check that each transaction is valid
- Nodes follow a comprehensive set of rules to validate each transaction:
  - Does the transaction contain the required data and are they correct?
  - Does the transaction have a valid digital signature using the sender's private key (i.e., do the funds being spent belong to the person spending them)?
- Validation is incentivized by issuing new Bitcoin as a reward to successful validators
  - Mining nodes add a transaction to each candidate block that mints new BTC and transfers them to the miner's address; this transaction will be valid only for the successful node
- Successful validators are further incentivized by receiving transaction fees paid in Bitcoin

Bitcoin's Four Main Elements: Proof-of-Work Algorithm (Las Vegas Version)

Proof-of-Work Algorithm: A mechanism for reaching a global, decentralized consensus on the valid blockchain (aka, "mining")

- Miners race to solve a complex mathematical problem; the first to solve the problem wins the ability to serve as a validator node on the network and earns the payout associated with that responsibility (see *Mining Explained: Simplified*)
- Ensures that all nodes in the network agree on a single golden copy of the blockchain



Crypto Mining: Purpose

Crypto miners serve two purposes:

1. Confirm transactions and make the network trustworthy
   - Bitcoin relies on miners to record and validate transactions because of a particular problem inherent in any system of digital currency: double spending (i.e., counterfeiting). Say, for example, that a currency user, Alice, has a $5 note and she gives it to Bob. Can Bob be sure that he's received $5 rather than a forgery? In the physical world, probably. In the digital world, probably not.

2. Generate new coins and enter them into circulation
   - Why do this? Miners mine because the writer of a new block in the blockchain has permission from the protocol to give herself a reward of new bitcoins. That reward started at 50 bitcoins per block. Every four years the protocol is adjusted, reducing the reward by half. One day the reward will be very small, but miners can also be rewarded by collecting fees volunteered by users that request transactions.

What is Bitcoin mining, and why is it necessary? - Coin Center

Crypto Mining: Payout (Today)

Breakdown of the mining payout:

6.25 bitcoins per block
=
6.25 x $19,000 (price as of 6/30/22) = $118,750

approximately144 blocks are mined each day
=
6.25 x 144 x $36,000 = $17,100,000

Crypto Mining: Payout (Peak)

Breakdown of the mining payout:

6.25 bitcoins per block
=
6.25 x $68,770 (peak price as of 11/10/21) = $429,812.50

approximately144 blocks are mined each day
=
6.25 x 144 x $36,000 = $61,893,000

Ethereum

The Origin of Ethereum

- **Who created Ethereum?**
  - Invented by Russian/Canadian programmer Vitalik Buterin
  - First described in Ethereum White Paper in 2013 and launched in 2015

- **Why was it created?**
  - According to Buterin, Bitcoin's main achievements were bitcoin (the currency) and using a proof-of-work blockchain to obtain public agreement on transaction ordering
  - Buterin noted that "**attention is rapidly starting to shift towards… how the blockchain can be used for more than just money.**"
  - He proposed a programmable blockchain that could be used to create "contracts" that would enable users to create new applications, including custom currencies and financial instruments, non-fungible tokens, decentralized financial applications, etc.
  - Or, for the more technically minded…
    - "What Ethereum intends to provide is a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" that can be used to encode arbitrary state transition functions, allowing users to create any of the systems described above, as well as many others that we have not yet imagined, simply by writing up the logic in a few lines of code."

Bitcoin vs. Ethereum

- **How are Bitcoin and Ethereum similar?**
  - Both enable decentralized, trustless, peer-to-peer, online payments using electronic cash (Bitcoin or Ether, respectively)
  - Ethereum uses many of the same technologies as Bitcoin to accomplish this (*e.g.*, public permissionless blockchains, public key cryptography, cryptographic hash functions, digital signatures, etc.)

- **What are some key differences b/w Bitcoin and Ethereum?**
  - Efficiency: Ethereum has a faster block time than Bitcoin (15 seconds vs. 10 minutes) and greater transaction throughput (30 per second vs. 7 per second)
  - Design: Ethereum incorporates a decentralized computing infrastructure that can host and run computer programs called **smart contracts**

What are Smart Contracts?

- **Smart contracts are computer programs that reside on the Ethereum blockchain**
  - They have their own accounts, called **contract accounts**
  - Once called, smart contracts can initiate or receive transactions in the same way as an individual user's account, or **externally owned account**
  - Smart contracts are:
    - **Immutable:** they cannot be changed once deployed
    - **Deterministic:** they produce the same outcome for everyone who runs them
    - **Atomic**: execution is "all or nothing"

What are Smart Contracts Used For?

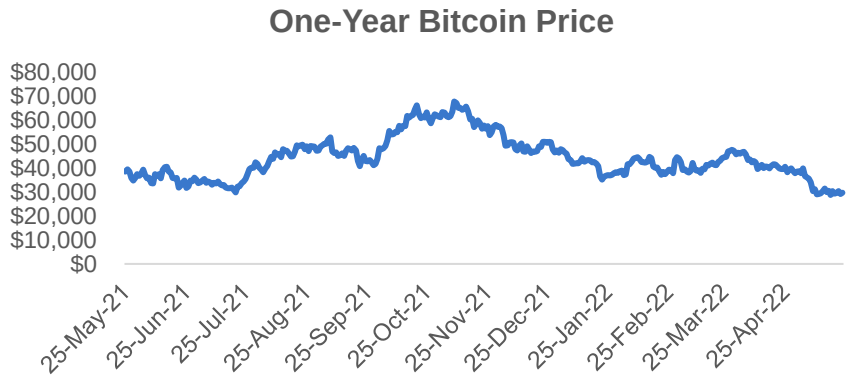
- **One common use for smart contracts is the creation and issuance of tokens**
  - Tokens are “blockchain-based abstractions that can be owned and that represent assets, currency, or access rights”*
  - Many popular **non-fungible tokens** (NFTs),which are tokens that track ownership of unique physical or digital items (e.g., art, real estate, are issued using an Ethereum-based token standard, ERC-721
  - The largest **stablecoins** are issued using a popular Ethereum-based token standard, ERC-20
- **Smart contracts have a wide range of other potential applications**
  - Smart contracts enable automatic execution of specific actions upon the satisfaction of pre-specified conditions
  - This functionality lends itself to use cases involving insurance claims, logistics and supply chain management, real estate transactions, and a variety of financial transactions
  - It also lends itself to a growing number of use cases involving **decentralized finance (DeFi),** such as automated lending, borrowing, trading, or other transactions

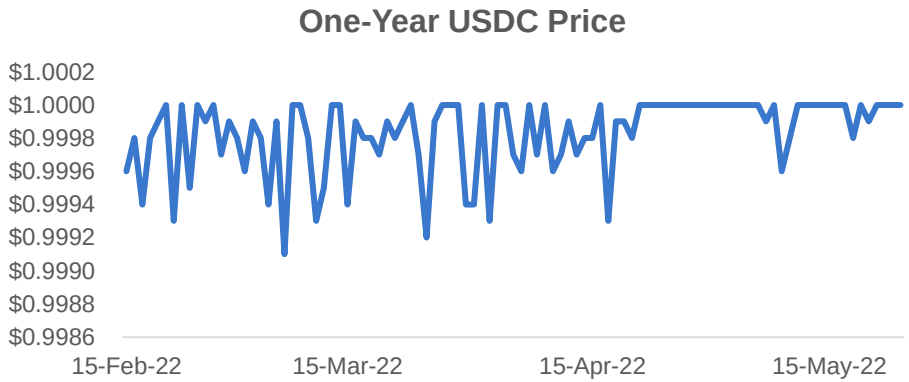
* Andreas M. Antonopoulos and Gavin Wood, *Mastering Ethereum: Building Smart Contracts and DApps*, O’Reilly, 2019.

Stablecoins

How do Stablecoins Differ from Bitcoin and Ether?

- Stablecoins, Bitcoin, and Ether are all cryptocurrencies
- But while Bitcoin and Ether are native to their blockchains, stablecoins are issued as tokens on top of a blockchain via smart contracts (as discussed in previous slides)
  - The same stablecoin may be issued on one or multiple blockchains
- Another key difference is how their value is determined:
  - Market supply and demand determines the value of Bitcoin, Ether, and similar cryptocurrencies, which can be highly volatile
  - Stablecoins seek to avoid this volatility by maintaining a fixed value (which may fluctuate within a very narrow band) against some reference asset, e.g., the U.S. dollar or an ounce of gold





How do Stablecoins Work?

- **Stablecoins are commonly backed by some type of asset**
  - Fiat currency-backed stablecoins (e.g., USDC, BUSD, USDT)
    - By far the most popular and common type of stablecoin
    - Issued by a central authority one-for-one against U.S. dollars
    - Reserves held off-chain in USD-denominated assets, typically by banks or custodian
  - Cryptocurrency-backed stablecoins (e.g., DAI)
    - Typically, over-collateralized due to the volatility of the cryptocurrency reserve assets
    - On-chain reserve assets are locked in and managed by smart contracts that can execute automated margin calls if collateral value falls below a set threshold
  - Commodity-backed stablecoins (e.g., XAUT or PAXG)
    - Significantly smaller market cap than fiat- or crypto-backed stablecoins
    - Most common reserve asset commodity is gold
    - May be exchanged for cash or for the underlying physical commodity

How do Stablecoins Work? (cont'd)

- **However, stablecoins may also be undercollateralized or unbacked entirely**
  - For example, the value of **algorithmic stablecoins** is supported by an algorithm that controls their outstanding supply
  - There are various ways to achieve this control
    - For example, using a second token to establish an arbitrage mechanism that incentivizes minting and burning of the stablecoin and associated token to maintain the stablecoin's value
  - None have proven perfect, and such stablecoins tend to be **far less stable** than their asset-backed counterparts
    - Recent examples of collapsed algorithmic stablecoins include Iron Finance (IRON) in 2021 and TerraUSD (UST) in 2022

How are Stablecoins Used?

- **Primarily for speculative digital asset investments**
  - Created to move in and out of crypto positions on-chain
  - Use has since expanded to DeFi lending and borrowing
- **Potential uses include less speculative applications**
  - Blockchain-based payments, including P2P, B2B, e-commerce, or cross-border
  - Other blockchain-based settlement activities, in which stablecoins serve as the dollar-leg of a transaction

The Stablecoin Market

- **Significant growth in stablecoin issuance over the past two years**
  - Total market cap peaked at around $182 billion in early April 2022
  - Fell to around $155 billion following the collapse of UST in May
- **Market diversification as new stablecoin issuers emerge**
  - Issuers are non-banks, although some hold Bitlicences (NYDFS)
  - The three largest stablecoins (USDT, USDC, BUSD) are all fiat-backed, while the fourth (DAI) is crypto-backed

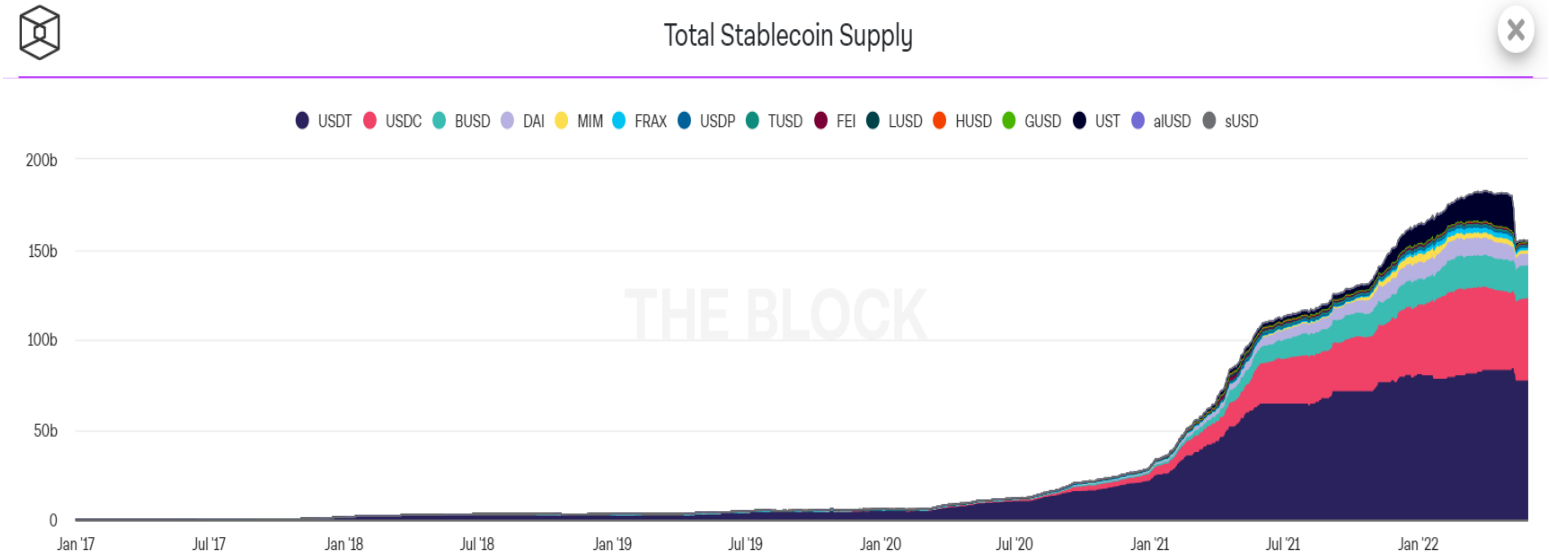


Image Source: The Block

Appendices

Additional Resources

Bitcoin and Blockchains

- Andreas M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, O'Reilly Media, 2017.
- Anthony Lewis, *The Basics of Bitcoins and Blockchain: An Introduction to Cryptocurrencies and the Technology that Powers Them*, Mango Publishing, 2018.

Ethereum, Smart Contracts, and DeFi

- Andreas M. Antonopoulos and Gavin Wood, Mastering Ethereum: Building Smart Contracts and Dapps, O'Reilly Media, 2019.
- Ethereum, *Development Documentation*, accessed June 1, 2022.
- Finematics, *Code is Law? Smart Contracts Explained*, June 12, 2020.
- Simply Explained, *ERC-20 Tokens*, February 13, 2018.
- S&R Policy Advisory Committee, *Banking without Banks*, May 2022.

Stablecoins

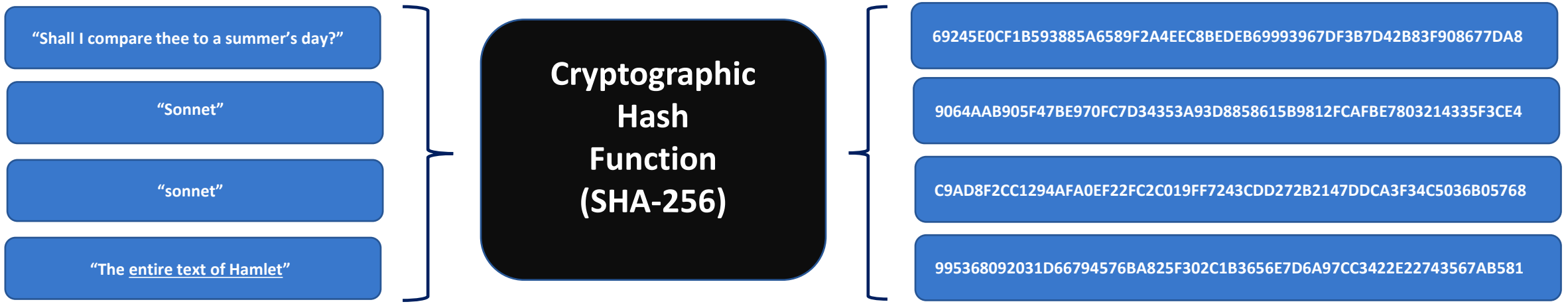
- Bank of International Settlements, *Stablecoins: Risks, Potential, and Regulation*, November 2020.
- Finematics, *Bankrun in DEFI – Lessons Learned from the Iron Finance Collapse*, June 24, 2021.
- FRBSF, *Focus on Fintech: Drivers, Design and Risks of Stablecoins*, September 23, 2021.
- Presidential Working Group on Financial Markets, *Report on Stablecoins*, November 1, 2021.
- Paxos Blog, *Understanding the Demise of UST and What Makes a Stablecoin Stable*, May 13, 2022.
- Stablecoin Issuers: Tether (USDT); CENTRE (USDC); Paxos (BUSD); Maker DAO (DAI)

Cryptographic Hash Functions

- A cryptographic hash function is a **function** that converts an arbitrary length input, called a **pre-image**, to a fixed-length output, called a **hash value** (see next slide for examples…)

Cryptographic Hash Functions

- Key properties of cryptographic hash functions:
  - **One-way**: It is very easy to produce a hashed output from an input (click here to create your own hash) but virtually impossible to do the reverse
  - **Deterministic**: the same input will always have the same hash output
  - **Collision-Free**: No two inputs will ever have the same hash output
  - **"Avalanche Effect":** Any change to the input, however small (e.g., switching one letter form upper case to lower case, as shown below), will result in a change to the hashed output, and the new hashed output will appear entirely unrelated to the previous output



Bitcoin Transactions

What does a Bitcoin Transaction Look Like?

- A Bitcoin transaction has two main components: **inputs** and **outputs**
- Each input for a new transaction is a reference to an output from a previous transaction
- Transactions may include one or more input(s) and output(s)
- To be spent, each input must be “unlocked” using the sender’s **private key**
- Outputs are “locked” using the recipient’s **public key**, ensuring that only the recipient can “unlock” it in a future transaction using their private key

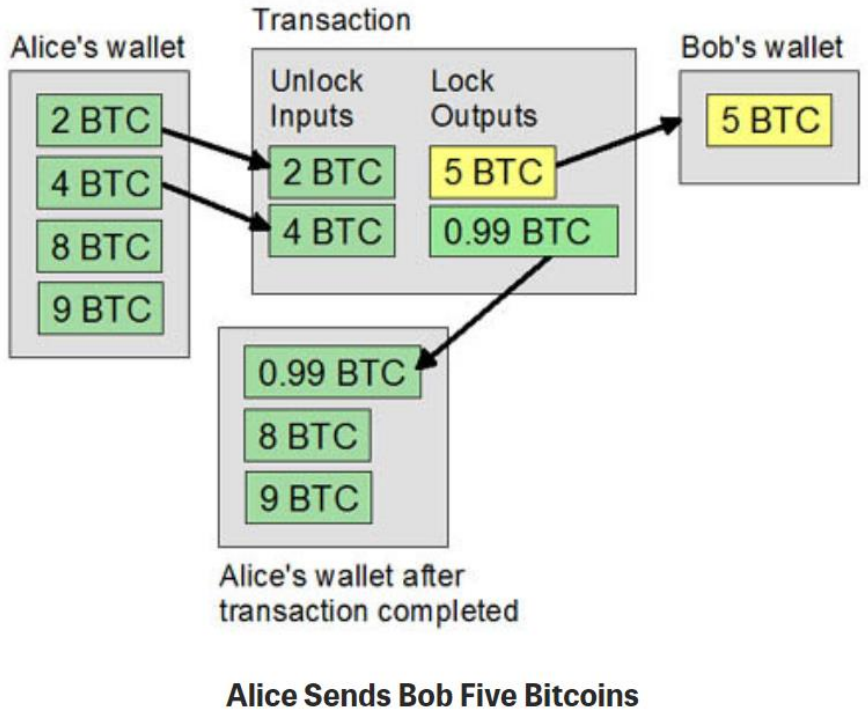


Image source: PCMag