Digital Currency and Blockchain

Frank Schmid

Chief Technology Officer

Proprietary Notice

The material contained in this presentation has been prepared solely for informational purposes by Gen Re. The material is based on sources believed to be reliable and/or from proprietary data developed by Gen Re, but we do not represent as to its accuracy or its completeness. The content of this presentation is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.

Agenda

- Functions of Money
- Forms of Money
- Types of Digital Currency
- Fiat Cryptocurrencies
- Stablecoins
- Exchanges and Wallets
- Blockchain
- Smart Contracts
- Calls for Regulation
- Literature

- Appendix:
  - Blockchain (Additional Material)
  - Lending Platforms
  - Decentralized Finance (DeFi)
  - Nonfungible Tokens (NFTs)
  - Central Bank Digital Currency

Functions of Money

Money is what functions as money

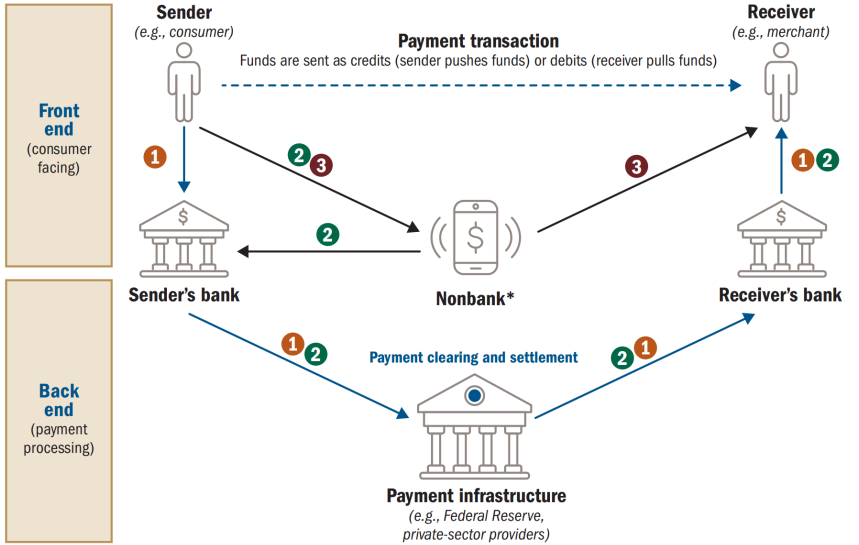
- **Means of payment**
  - A necessary condition for money to function as a means of payment is the NQA (No Questions Asked) principle to hold – Money is accepted at face value (i.e., at par) without due diligence being performed on the issuer
- **Store of value**
  - A necessary condition for money to function as a store of value is a low and stable rate of inflation, which implies that money must be sufficiently scarce
- **Unit of account**
  - In a world of n goods and services, money reduces the number of bilateral price relations (e.g., a barrel of oil priced in number of bushels of wheat) from $n \times (n-1)$ to n

See, for instance, [BG] or [PBC].
The NQA principle is due to Bengt Holmström (January 14, 2015) "Understanding the Role of Debt in the Financial System," Bank of International Settlements Working Paper No. 479, https://www.bis.org/publ/work479.pdf.

Forms of Money

Schematic of a typical payment

In this example, the general public interacts with the "front end" of the payment system by swiping their credit card at a checkout machine or using a mobile app to send money. These payments may 1 flow solely through applications operated by and accounts maintained by banks, 2 originate in a nonbank financial service and then flow through the banking system, or 3 remain only in the records of the nonbank services (though customer nonbank accounts may be funded/defunded by bank accounts).



*Nonbank financial service providers may be involved in various stages of both the front-end and the back-end of the payment chain. For example, there may be multiple paths from a nonbank to the receiver.

See [BG].

Forms of money

Central Bank Money. In the United States, central bank money is a liability of the Federal Reserve and comes in two forms: (1) physical currency circulating among the general public (with some held by banks) and (2) digital account balances held by banks and a limited number of other eligible institutions at the Federal Reserve. Physical currency has legal tender status in the United States.

Commercial Bank Money. Dollar-denominated balances held by consumers in commercial bank accounts are commercial bank money. These balances are liabilities of commercial banks, not of the Federal Reserve

Nonbank Money. Some nonbank financial services providers issue liabilities that can be considered money. These providers often hold balances on behalf of consumers or businesses and effect transfers of those balances on their own books for users that have signed up for their services.

Types of Digital Currency

Stylized categorization

Fiat Cryptocurrency

- Privately-produced money
- Fiat currency (no intrinsic value)
- Not liable to runs
- No identity verification
- Privacy-protected
- Decentralized
- Limited transferability
- Operates on blockchain
- Limited interoperability with other forms of money
- Examples are bitcoin and ether

Stablecoin

- Privately-produced money
- Pegged to the value of an asset
- Asset-backed[1)] and liable to runs
- No identity verification
- Privacy-protected
- Central issuance of tokens
- Limited transferability
- Operates on blockchain
- Interoperability with central bank money through redemption
- Examples are tether and USD Coin

Central Bank Digital Currency

- Central bank liability
- Fiat currency
- No credit or liquidity risk
- Identify-verified
- Privacy-protected
- Intermediated
- Widely transferable
- Possibly central ledger (digital yuan)
- Wide interoperability, nationally and internationally
- An example is China's digital yuan[2)]

1) These assets are typically fiat currency assets (such as short-term Treasury securities). For some stablecoins, these assets are other stablecoins or, for algorithmic stablecoins, arbitrage opportunities. See Adams, Austin, and Markus Ibert (June 2, 2022) "Runs on Algorithmic Stablecoins: Evidence from Iron, Titan, and Steel." FEDS Notes, Board of Governors of the Federal Reserve, https://www.federalreserve.gov/econres/notes/feds-notes/runs-on-algorithmic-stablecoins-evidence-from-iron-titan-and-steel-20220602.htm.

2) Most notably, China has introduced a CBDC (central bank digital currency) as a pilot in major metropolitan areas. The digital yuan (e-CNY) runs on a central ledger. The role of blockchain technology (as an alternative to a central ledger) for central bank digital currencies and their international interoperability remains a matter of debate. For details on central bank digital currencies, see Bank for International Settlements, "Rise of the central bank digital currencies: drivers, approaches and technologies," https://www.bis.org/publ/work880.htm. See also [BG], PCB, and [ECB] in Literature.

Fiat Cryptocurrencies

Currencies without intrinsic value

- Fiat currencies are not backed by assets (such as gold or silver)
  - Consequently, the currency does not accord the holder a right on redemption
- Central bank paper currency is an example of fiat currency
  - The Gold Standard Act of 1900 stipulated that the U.S. Treasury redeem U.S. dollar notes in gold
- Bitcoin and ether[1)] are examples of fiat cryptocurrencies
  - There is no right on redemption in other digital currencies or U.S. dollar notes
- Unlike bitcoin, U.S. dollar notes are “legal tender for all debts, public and private“

1) Bitcoin runs on the eponymous blockchain, whereas ether is native to the Ethereum blockchain.

Fiat Cryptocurrencies

Bitcoin and the functions of money

- **Means of payment**
  - Bitcoin has limited use as a means of payment – transacting in bitcoin is slow and costly[1)]
  - Bitcoin has legal tender status in El Salvador (since 2021) alongside the U.S. dollar, and in the Central African Republic (since 2022) alongside the regional Central African CFA franc
- **Store of value**
  - During the first half of 2022, bitcoin lost about 60% in value against the U.S. dollar, taking U.S. consumer price inflation in bitcoin terms beyond 150%
- **Unit of account**
  - A currency's status as legal tender accords it (implicitly) the unit of account function – there is no value in introducing bitcoin as unit of account alongside the existing legal tender

1) Bitcoin is only capable of supporting roughly five transactions per second, and the cost per transaction can be up to $60, depending on demand. See [BG].

Stablecoins

Crypto feels like the Wild West – Because it is!

- Stablecoins have a parallel in the U.S. Free Banking Era (1837–1863)
- In 1836, Congress closed the Second Bank of the United States
  - At the time, state banks issued their own notes, which had to be backed by specie (gold or silver)
  - The Second Bank of the United States regularly presented for payment the currency of state banks it suspected of overissuing, thus incentivizing these banks to keep an adequate supply of specie
- In 1838, New York passed a free banking act, allowing anyone to open a bank
  - The notes the bank issued had to be backed by state bonds deposited at the state auditor's office
  - All notes had to be redeemable on demand at face value
- A majority of the 33 states in the Union in 1860 had some form of free banking

See Arthur Rolnick and Warren Weber (1982) "Free Banking, Wildcat Banking and Shinplasters." Federal Reserve Bank of Minneapolis Quarterly Review (Fall 1982), https://www.minneapolisfed.org/research/quarterly-review/free-banking-wildcat-banking-and-shinplasters.
U.S. Securities and Exchange Commission Chair Gary Gensler (August 3, 2021) compared crypto to the Wild West in "Remarks before the Aspen Security Forum," https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

Stablecoins

Crypto feels like the Wild West – Because it is!

- The Free Banking Era is considered a failure
  - Although free banking laws led to the creation of a high number of banks, many of these banks failed within just a few years
  - The most important cause of bank failure were declines in the prices of state bonds, which free banks were required to hold, and which made up a significant share of the banks' asset portfolios
    - The decline in bond prices caused a run on the bank as noteholders questioned the solvency of the bank and asked for redemption of the notes
  - There were also wildcat banks, which knowingly issued more notes than they planned to redeem
    - In some states, free banks could issue notes up to the par value of the state bonds. Free banks purchased state bonds that traded at a discount to par, deposited them with the state, and issued notes equal to the par value
    - Some free banks that overissued located in inaccessible places ("where only the wildcats throve") to make redemption difficult, or simply closed after having issued all the notes

See Arthur Rolnick and Warren Weber (1982) "Free Banking, Wildcat Banking and Shinplasters." Federal Reserve Bank of Minneapolis Quarterly Review (Fall 1982), https://www.minneapolisfed.org/research/quarterly-review/free-banking-wildcat-banking-and-shinplasters.

Stablecoins

Stablecoin issuers, like the free banks of yore, make claims of asset-backing

- Tether, the largest stablecoin issuer, claims that "[a]ll Tether tokens are pegged at 1-to-1 with a matching fiat currency and are backed 100% by Tether's reserves."[1)]
- In February 2021, Tether reached a $18.5 million settlement with the New York attorney general's office, following a two-year investigation[2,3)]
  - The attorney general's office concluded that Tether made several public misrepresentations regarding the dollar reserves backing for 2017
  - Additionally, Tether agreed to publicly release quarterly statements detailing its reserves[4)]
- In October 2021, Tether was fined $41m by the U.S. Commodities Futures Trading Commission for misrepresenting itself as fully backed by assets between 2016 and 2019[5)]

1) See Tether: Transparency, https://tether.to/en/transparency.

2) See The Wall Street Journal (February 23, 2021) "Cryptocurrency Firms Bitfinex, Tether Settle New York Attorney General's Probe." https://www.wsj.com/articles/cryptocurrency-firms-bitfinex-tether-settle-new-york-attorney-generals-probe-11614093709?mod=article_inline.

3) See The Wall Street Journal (October 24, 2021) "Crypto is Shedding its Tether." https://www.wsj.com/articles/crypto-shedding-tether-stablecoin-backed-john-law-11635103866.

4) In August 2022, the Wall Street Journal quotes the Tether's Chief Technology Officer stating that an audit is "likely months" away. Instead of an audit, Tether publishes an "attestation" signed off by its accounting firm. See The Wall Street Journal (August 27, 2022) "Tether says Audit Is Still Months Away as Crypto Market Falters." https://www.wsj.com/articles/tether-says-audit-is-still-months-away-as-crypto-market-falters-11661568971.

5) See The Wall Street Journal (October 24, 2021) "Crypto is Shedding its Tether." https://www.wsj.com/articles/crypto-shedding-tether-stablecoin-backed-john-law-11635103866.

Stablecoins

Stablecoin issuers, like the free banks of yore, make promises of redemption

- Tether, in Article 3 of its Terms of Service, spells out the terms on redemption:[1)]

  The right to have Tether Tokens redeemed or issued is a contractual right personal to you. Tether reserves the right to delay the redemption or withdrawal of Tether Tokens if such delay is necessitated by the illiquidity or unavailability or loss of any Reserves held by Tether to back the Tether Tokens, and Tether reserves the right to redeem Tether Tokens by in-kind redemptions of securities and other assets held in the Reserves.

- Note that these terms do not guarantee immediate redemption, nor do they guarantee redemption in the U.S. dollar, to which the Tether token (USDT) is pegged

- On May 12, 2022, USDT temporarily broke the peg, falling from $1 to 95 cents[2)]
  - In the following weeks, investors redeemed $10 billion, while other stablecoins added market value

1) See Tether: Legal, https://tether.to/en/legal/.
2) See The Wall Street Journal (June 9, 2022) "Tether Cedes Territory to Rival Stablecoins as Crypto Investors Diversify." https://www.wsj.com/articles/tether-cedes-territory-to-rival-stablecoins-as-crypto-investors-diversify-11654739513.

Stablecoins

Crypto runs

- Runs occur when currency holders question the ability to redeem the currency at the purported peg, be it in specie (free banks) or the U.S. dollar (tether and other stablecoins)
- As in free banking, doubts about the value of the assets backing the currency may arise, possibly due to specific events or general economic developments
  - As demonstrated by the investigations into Tether, stablecoin issuers, like free banks in the past, are largely unregulated and offer little transparency – there have also been cases of misrepresentation
- The first run on a digital coin backed by assets occurred in June 2021, when TITAN, a DeFi token[1)], dropped from an all-time high of over $64 to $0 in just a few hour hours
  - Said the issuer of TITAN: "We never thought it would happen, but it just did. We just experienced the world's first large-scale crypto bank run."[2,3)]

1) DeFi tokens, like stablecoins, are backed by assets, here DeFi-related assets. Unlike stablecoins, these assets generally do not have a stable value. The market capitalization of DeFi tokens is small.
2) See Iron Finance Post-Mortem (June 17, 2021), https://ironfinance.medium.com/iron-finance-post-mortem-17-june-2021-6a4e9ccf23f5.
3) In the context of the run on the TITAN token, the related algorithmic stablecoin IRON "fell from $1 to about 75 cents, the level of collateral behind the coin," which consisted of USD Coin. See The Wall Street Journal (April 18, 2022) "Cutting-Edge Crypto Coins Tout Stability. Critics Call them Dangerous." https://www.wsj.com/articles/cutting-edge-crypto-coins-tout-stability-critics-call-them-dangerous-11650226597.

Stablecoins

The run on TerraUSD

- TerraUSD is an algorithmic stablecoin that, along with its sister currency Luna, was supposed to maintain a peg to the U.S. dollar
  - The algorithm relied on arbitrage between TerraUSD and Luna. When the price of TerraUSD dropped (even slightly) below $1, one could make money by swapping a dollar worth of Luna for a dollar worth of TerraUSD – the increased demand for TerraUSD would restore the peg.[1)]
  - The algorithm worked so long as market participants believed that the algorithm works in restoring the peg
  - When in May 2022 the discount of TerraUSD to the $1 peg became material, investors lost faith in the algorithm – the value of TerraUSD collapsed to pennies, and Luna imploded[2)]
  - Holders of TerraUSD and Luna lost a total of $40 billion[3)]

1) Conversely, when the price of TerraUSD exceeded $1, one could make money by swapping TerraUSD for Luna.
2) Currently, TerraUSD is valued at pennies, and Luna at a fraction of a penny. See CoinDesk, https://www.coindesk.com.
3) See The Wall Street Journal (June 28, 2022) "Do Kwon Tries Again After $40 Billion Crypto Crash."
https://www.wsj.com/podcasts/google-news-update/do-kwon-tries-again-after-40-billion-crypto-crash/a5c77dd5-6385-492c-aa5f-0fb353df9da8?mod=Searchresults_pos10&page=1.

Exchange and Wallets

Crypto exchanges are marketplaces for buying and selling digital currency

- On centralized crypto exchanges, known as CEXs, digital currencies can be exchanged for other digital currencies and major fiat currencies[1)]
  - For instance, fiat cryptocurrencies (such as bitcoin or ether) can be exchanged for stablecoins (such as tether or USD Coin) or fiat currencies (such as the U.S. dollar or the euro), and vice versa
  - Some CEXs support advanced features like margin accounts and derivatives trading
- CEXs offer crypto wallets – the wallet is native to the exchange and hosts the client's private (encryption) key that provides access to the crypto assets on the blockchain
  - There are questions on how to ensure that these platforms do not misuse or mishandle these assets and how customers are treated if a platform enters bankruptcy[2)]

1) In addition to centralized crypto exchanges (CEXs), there are decentralized crypto exchanges (DEXs). Decentralized crypto exchanges have small trading volume and do not offer exchange into the U.S. dollar.
2) Legal scholars have drawn parallels to the broker-dealer failures of the late 1960s and view the regulatory response to these events as a template for regulating crypto exchanges. See Dennis Chu, "Brokers Dealers for Virtual Currency: Regulating Cryptocurrency Wallets and Exchanges." Notes, Columbia Law Review Vol. 118, No 8, https://columbialawreview.org/content/broker-dealers-for-virtual-currency-regulating-cryptocurrency-wallets-and-exchanges/.

Exchanges and Wallets

Staking, leverage, and central point of failure

- Some CEXs offer features such as crypto staking, which allows the holder of cryptocurrency to earn rewards on a blockchain that uses the PoS consensus mechanism
  - Staking entails committing the crypto asset for a minimum amount of time
  - The crypto holder may join a staking pool to smooth the income stream
- Also, some CEXs, such as Binance, the world's largest exchange, allow customers to pledge crypto assets, including staked crypto, as collateral for loans to finance trading
- CEXs introduce central points of failure into the decentralized world of crypto
  - Centralized exchanges have a history of outages and temporary suspensions of withdrawals
  - Most recently, on May 19, 2022, Binance, froze for over an hour just as the price of bitcoin and other cryptocurrencies plunged, leading to the liquidation of leveraged bets in margin accounts[1)]

1) See, for instance, The Wall Street Journal (July 17, 2022) "Binance Froze When Bitcoin Crashed. Now Users Want Their Money Back." https://www.wsj.com/articles/binance-froze-when-bitcoin-crashed-now-users-want-their-money-back-11626001202.

Exchanges and Wallets

The run on FTX (1/2)

- Crypto exchange FTX and Hong Kong-based proprietary trading firm Alameda Research are both businesses controlled by Sam "SBF" Bankman-Fried
- On November 2, 2022, CoinDesk reported that "even though they are two separate businesses, the division breaks down in a key place: on Alameda's balance sheet"[1)]
  - The report alleged that the "balance sheet [of Alameda] is full of FTX – specifically, the FTT token," which "adds to evidence that the ties between FTX and Alameda are unusually close"[2)]
- On Sunday November 6, Changpeng "CZ" Zhao, the founder of Binance, announced on Twitter that it will liquidate its entire holding of FTT, alluding to "recent revelations"[3)]
  - Binance, the largest crypto exchange, had received the FTT stake as part of its 2021 exit from FTX, of which it was an early backer – at the time of the tweed, the stake was worth at least $580 million[4)]

1) See CoinDesk (November 2, 2022) "Divisions in Sam Bankman-Fried s Crypto Empire Blur on His Trading Titan Alameda s Balance Sheet." https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/.

2) FTT is a utility token. "Owners of the FTT token get discounts on FTX trading fees, increased commissions on referrals and earn rewards." See CoinDesk, op. cit.

3) See The Wall Street Journal (November 7, 2022) "Binance to Sell Holdings of FTX's Token as Relations Between Crypto Exchanges Fray." https://www.wsj.com/livecoverage/stock-market-news-today-11-07-2022/card/binance-to-sell-holdings-of-ftx-s-token-as-relations-between-crypto-exchanges-fray-VukiTcJgKWJeZEEgnG5y.

4) See Reuters (November 10, 2022) "Exclusive: Behind FTX's fall, battling billionaires and a failed bid to save crypto." https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/.

Exchanges and Wallets

The run on FTX (2/2)

- On the day of CZ's tweed, FTX customers withdrew about $5 bn (net) from their accounts[1)]
- On Tuesday morning, FTX "effectively paused" withdrawals after they had swelled to $6 bn[2)]
- Also on Tuesday, Binance entered a nonbinding agreement to buy FTX, only to walk away from the deal the next day following due diligence[3)]
  - Binance mentioned reports of "mishandled customer funds and alleged US agency investigations"
- On Thursday, there were reports of FTX having tapped into customer accounts to extend loans to Alameda for risky bets – Alameda owes FTX about $10 bn[4)]
- On Friday, SBF's $32 bn crypto empire collapses as FTX files for bankruptcy protection[5)]

1) See The Wall Street Journal (November 10, 2022) ""FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall." https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732.
2) See Reuters (November 8, 2022) "Crypto exchange FTX saw $6 bln in withdrawals in 72 hours." https://www.reuters.com/business/finance/crypto-exchange-ftx-saw-6-bln-withdrawals-72-hours-ceo-message-staff-2022-11-08/.
3) See The Wall Street Journal (November 10, 2022) op. cit.
4) See The Wall Street Journal (November 10, 2022) op. cit. Traditional, regulated brokers must keep client funds segregated from other company assets.
5) "The filing in Delaware federal court on Friday included the main FTX international exchange, a US crypto marketplace, Bankman-Fried s proprietary trading group Alameda Research and about 130 affiliated companies." See Financial Times (November 11, 2022) "Sam Bankman-Fried s $32bn FTX crypto empire files for bankruptcy." https://www.ft.com/content/afe56c4e-2d68-457e-bbb2-476752d5f02e.

Blockchain

Distributed ledger technology (DLT) vs. traditional financial system

- A typical financial system can be represented as a collection of states and transactions
  - A state is a collection of all the accounts in the system, together with their balances
  - Transactions specify how funds move between accounts
- Historically, financial intermediaries have been the key nodes in the financial system that perform bookkeeping functions, control the accuracy of customer accounts, and ensure that unauthorized persons do not have access to an account
- DLT is an alternative architecture of storing and managing information where no single entity has full control over all the states and transactions, or any subset of them
  - Instead, multiple parties (validators) hold their own copies of states and jointly decide which transactions are admissible

See [MS].

Blockchain

Blockchain as a form of distributed ledger

- A blockchain is a form of DLT in which all transactions are recorded and organized in blocks that are linked together in a time-ordered manner using cryptography
  - The bitcoin blockchain and ethereum remain the best-known applications of blockchain technology
- In DLT, there is no central point of failure
  - Because multiple copies of records exist, the corruption of a single node or copy has no effect on the security of the blockchain
  - Specifically, as long as the majority of validators are not corrupted, the security of the blockchain protocol is preserved
- Blockchain is based on the security concept of zero trust
  - For the blockchain to work, there is no need for the validators to trust one another

See [MS].

Blockchain

Permissioned vs. permissionless blockchains

- Blockchains are either permissioned (private) or permissionless (public), depending on the set of entities that are allowed to serve as validators
- On a permissioned blockchain, a set of validators is approved by a coordinating body, which may be a single entity or a consortium of institutions
  - An example of a permissioned blockchain is J.P. Morgan's Liink, a global peer-to-peer blockchain network that counts many of the world's largest banks among its members[1)]
- On a permissionless blockchain, there is no ex-ante constraint on who can be a validator
  - Examples are the bitcoin blockchain and ethereum
- Only a permissionless blockchain operates a strict zero-trust architecture as there is no central governing body

See [MS].
1) See Link by J.P. Morgan, https://www.jpmorgan.com/onyx/liink

Blockchain

Proof of Work (PoW) and Proof of Stake (PoS) as consensus mechanisms

- In permissionless blockchains, PoW and PoS are proposed solutions to the double-spend problem in the absence of a financial intermediary that maintains a central ledger
  - PoW is the original concept, proposed by Satoshi Nakamoto, and used mostly prominently by the Bitcoin blockchain and, originally, by the Ethereum platform
  - PoS is a more recently developed solution and the concept of choice for newer public blockchain platforms and the new Ethereum consensus layer[1)]
- PoW and PoS both rely on financial incentives
  - Validators are rewarded for honesty in the form of transaction fees (in existing coins) and a prespecified amount known as a block subsidy (typically in the form of newly minted coins)[2)]
  - Accordingly, PoW and PoS are designed to make it economically unattractive for a validator to launch a double-spend attack

See [MS]. See also Coinbase, "What is 'proof of work' or 'proof of stake'?", https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake.
1) Ethereum transitioned from PoW to PoS in a project known as the Merge, which was completed on September 15, 2022. For details, see https://ethereum.org/en/upgrades/merge/.
2) The issuance of newly minted coins is a dilution tax imposed on existing currency holders.

Smart Contracts

Self-executing contracts on the permissionless blockchain

- Smart contracts are "a set of promises, specified in digital form, including protocols within which the parties perform on these promises"[1)]
- Smart contracts are a foundational layer of the Decentralized Finance (DeFi) architecture
- The Ethereum blockchain is designed to execute smart contracts and build applications on top of the blockchain – this is possible by embedding lines of scripting code
- Smart contracts differ from traditional contracts in how they are executed and enforced
  - The distributed nature of the contract makes it impossible to renege on the contract or to unilaterally stop or reverse its execution[2)]
  - For execution, the contract may require off-blockchain data input, which is provided by oracles[3)]

See [MS].

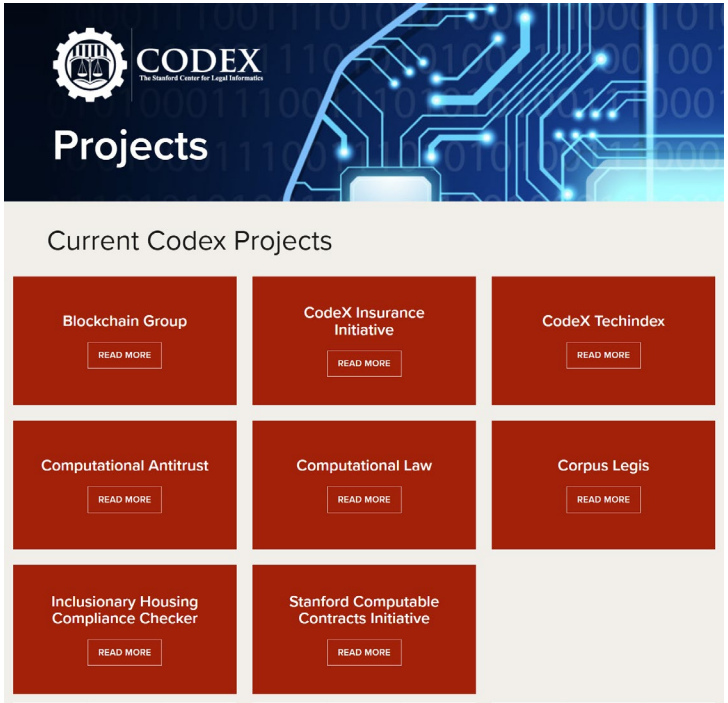
1) See Ethereum White Paper, https://ethereum.org/en/whitepaper/.

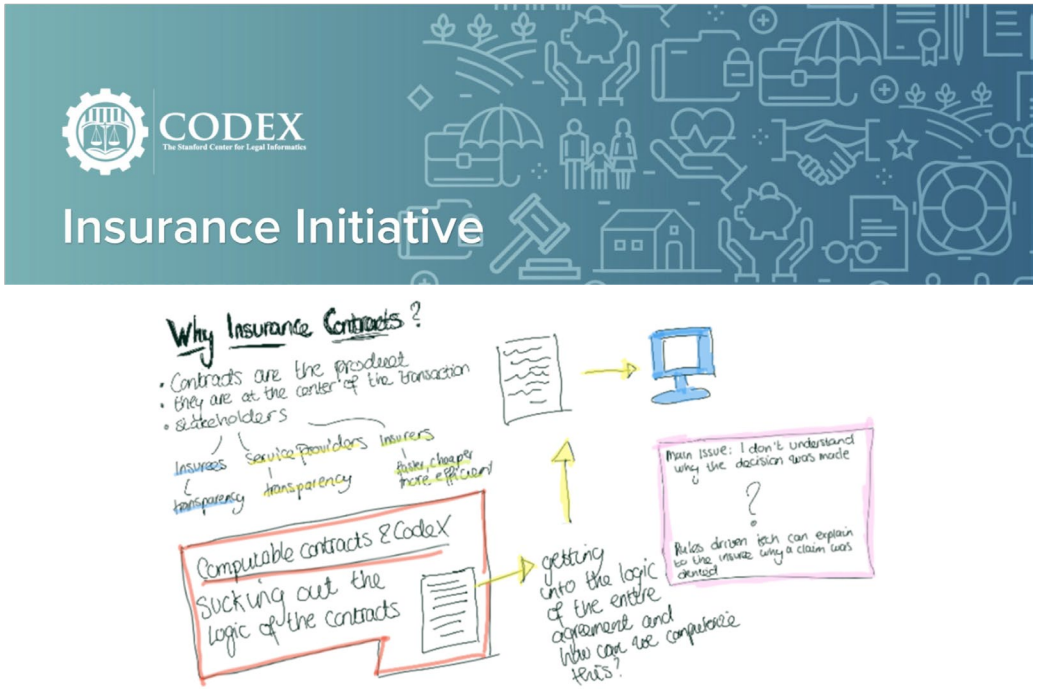
2) For smart contracts, ex-post protections afforded by traditional contract law may not be available. Such ex-post protections apply to situations of unconscionability, mutual mistake, illegality, capacity, consideration, fraud, or duress.

3) A leading provider of oracles is Chainlink, https://chain.link/.

Smart Contracts

Computable contracts as a prerequisite for smart contracts





See CODEX, Stanford Law School, https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/codex-projects/.

Call for Regulation

White House report on stablecoins

- On November 1, 2021, the White House published the "Report on STABLECOINS"
  - The National Bank Act of 1863 required newly chartered national banks to back their notes with Treasury securities, ending the Free Banking Era
  - The shortage of Treasury securities then led banks to create demand deposits, which gave rise to bank runs until deposit insurance was introduced in 1934[1)]
  - In conclusion, the report recommends that stablecoins be issued through insured banks and backed with safe assets (Treasury securities or central bank reserves)

See [PWG].
1) The Federal Deposit Insurance Corporation (FDIC) was formed in 1933, and deposit insurance began in 1934.

Call for Regulation

U.S. Department of the Treasury and Financial Stability Oversight Council

- On September 16, 2022, the U.S. Treasury issued three reports[1)]
  - "The Future of Money and Payments"
  - "Implications for Consumers, Investors, and Businesses"
  - "Action Plan to Address Illicit Financing Risks of Digital Assets"
- On October 3, 2022, the Financial Stability Oversight Council, which was convened by the U.S. Treasury in March 2022, released its report[2)]
  - "Report on Digital Asset Financial Stability Risks and Regulation"
- The overarching themes of these reports are financial stability, the future (technology) of the payment system, countering illicit finance, and consumer protection

1) See [USDT].
2) See [FSOC].

Literature

[BG] Board of Governors of the Federal Reserve System (2022) "Money and Payments: The U.S. Dollar in the Age of Digital Transformation." https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

[ECB] European Central Bank (2020) "Report on digital Euro." https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

[FSOC] Financial Stability Oversight Council (2022) "Report on Digital Asset Financial Stability Risks and Regulation." https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf.

[GZ] Gorton, Gary B., and Jeffrey Zhang (2021) "Taming the Wildcat Stablecoins." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888752.

[MS] Makarov, Igor, and Antoinette Schoar (2022) "Cryptocurrencies and Decentralized Finance (DeFi)." https://www.nber.org/papers/w30006.

[PBC] People's Bank of China (2021) "Progress of Research & Development of E-CNY in China." http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf.

[PWG] President's Working Group on Financial Markets (2021) "Report on STABLECOINS." U.S. Department of the Treasury, https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

[USDT] U.S. Department of the Treasury (2022) Reports on Digital Assets. https://home.treasury.gov/news/press-releases/jy0956.

Gen Re

DImensions

Appendix

Blockchain (Additional Material)

Proof of Work (as implemented on the bitcoin blockchain)

Satoshi Nakamoto, the presumed founder of bitcoin, described the steps of PoW on the bitcoin network as follows:

1) *New transactions are broadcast to all nodes.*
2) *Each node collects new transactions into a block.*
3) *Each node works on finding a difficult PoW for its block.*
4) *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
5) *Nodes accept the block only if all transactions in it are valid and not already spent.*
6) *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*

Step 3 involves guessing a 64-digit hexadecimal number knowns as a hash, a step dubbed mining because the first node to solve the puzzle is rewarded in newly minted bitcoin[1)]

1) The block reward consists of the transaction fees and the block subsidy. The transaction fees vary by the data volume in the block and the level of network congestion. Further, a transactor can increase the fee to incentivize miners to quickly include this transaction in a block. Currently, the block subsidy equals $6.25 and is projected to be halved in 2024 and approximately every four years thereafter.
See Nakamoto, Satoshi (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.

Blockchain (Additional Material)

Proof of Stake

- Staking serves a similar function to mining in proof of work in the process by which a network participant gets selected to add the latest batch of transactions to the blockchain
- Participants stake currency in exchange for a chance of getting to validate new transactions, update the blockchain, and earn a reward
- The winning validator is selected randomly, where the probability of being chosen is a function of the amount of currency staked, and how long it has been staked
  - Once the winner has validated the block, other validators get a chance to attest its accuracy
  - If transactions in a new block are discovered to be invalid, validators can have a certain amount of their stakes burned by the network, in what is known as a slashing event

See Coinbase, "What is 'proof of work' or 'proof of stake'?", https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake. Further, Coinbase, "What is staking?", https://www.coinbase.com/learn/crypto-basics/what-is-staking.

Blockchain (Additional Material)

Proof of Work vs. Proof of Stake

- PoW leads to duplication of effort as many validators race to solve the puzzle
- The Ethereum blockchain with the original PoW consensus layer consumed about 80 terawatt-hours per year, comparable to the power consumption of Chile[1)]
  - A single transaction used as much power as an average U.S. household uses over about seven days[2)]
- Ethereum holds that the transition to PoS reduced energy consumption by 99.95 percent
  - The Ethereum transition to PoS, known as the Merge, was executed on September 15, 2022
- Another challenge of PoW is its limited capacity[3)]
  - The transition to PoS will deliver only a minor improvement[4)]

1) Digiconomist, https://digiconomist.net/bitcoin-energy-consumption/, accessed on July 5, 2022. In comparison, the bitcoin blockchain consumes about 129 terawatt-hours per year, which compares to the power consumption of Norway (data accessed on September 14, 2022).

2) Digiconomist, op. cit. A single transaction on the Bitcoin blockchain consumes as much power as an average U.S. household consumes over about 48 days (data accessed on September 14, 2022).

3) Ethereum, using the PoW consensus layer, is capable of executing only about 15 transactions per second. See Castor, Amy (March 4, 2022) "Why Ethereum is switching to proof of stake and how it will work," MIT Technology Review, https://www.technologyreview.com/2022/03/04/1046636/ethereum-blockchain-proof-of-stake/.

4) See Ethereum, The Merge, Misconception: "Transactions will be noticeably faster after The Merge." https://ethereum.org/en/upgrades/merge/.

Blockchain (Additional Material)

Double spend attack (aka 51% attack)

- Satoshi Nakamoto envisioned that on the bitcoin blockchain, an attacker would find it prohibitively costly to outpace the network
  - On the bitcoin network, the longest chain serves as the source of truth, where length is determined by difficulty (as opposed to number of blocks)
  - An attacker would have to create a fork and marshal a hashrate greater than the network
- For smaller coins, a double spend attack can be economically viable
  - It takes only a small proportion of miners from larger coins to switch resources to a smaller coin in order to control 51% of the smaller coin's network hashrate
  - Multiple successful double spend attacks on smaller coins have been reported – some of these attacks made use of the hashrate rental market

The network hashrate refers to the total combined computational power that is used to mine and process transactions on a proof-of-work blockchain.
See Nakamoto, Satoshi (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf.
See also MIT Media: Lab Digital Currency Initiative, https://dci.mit.edu/51-attacks.

Lending Platforms

BlockFi, Celsius Network, Vauld, and Voyager Digital

- Centralized lending platforms aggregate customers' crypto assets and make them available to third parties to generate yield, a process known as yield farming
- Crypto market turmoil in May/June 2022 led four prominent lenders into financial distress
  - Three platforms froze customer accounts and suspended withdrawals
    - Celsius Network (June 22nd) was followed by Voyager Digital[1] (July 1st), and Vauld[2] (July 4th)
  - Two platforms filed for Chapter 11, and another two were rescued
    - Voyager filed for Chapter 11 bankruptcy protection on July 5th [3], followed by Celsius on July 13th [4]
    - Vauld is reported to be in the process of being acquired by lending platform Nexo[5] , whereas BlockFi, which has remained operational, was bailed out by cryptocurrency exchange FTX[6]

1) Voyager Digital also acted as a broker, connecting customers to crypto exchanges.
2) Vauld also acts as a crypto exchange.
3) See The Wall Street Journal (July 6, 2022) "Crypto Broker Voyager Digital Files for Bankruptcy Protection." https://www.wsj.com/articles/crypto-broker-voyager-digital-files-for-bankruptcy-protection-11657098630.
4) See The Wall Street Journal (July 14, 2022) "Crypto Crash Drags Lender Celsius Network Into Bankruptcy." https://www.wsj.com/articles/crypto-crash-drags-lender-celsius-network-into-bankruptcy-11657758483.
5) See The Wall Street Journal (July 5, 2022) "Crypto-Lender Nexo Nears Acquisition of Peter Thiel-Backed Lender Vauld." https://www.wsj.com/articles/crypto-lender-nexo-nears-acquisition-of-peter-thiel-backed-lender-vauld-11657041967.
6) See The Wall Street Journal (July 14, 2022) "FTX Strikes Deal With Option to Buy Crypto Lender BlockFi for Up to $240 Million." https://www.wsj.com/articles/ftx-strikes-deal-with-option-to-buy-crypto-lender-blockfi-for-up-to-240-million-11656701743.

Decentralized Finance (DeFi)

DeFi was enabled by layering smart contracts on a permissionless blockchain protocol

- DeFi replicates elements of the traditional financial system without intermediaries
  - The main applications so far have centered on trading platforms, borrowing and lending marketplaces, oracles, yield farming, and insurance[1)]
- The Ethereum ecosystem has emerged as a major platform for DeFi transactions
  - The Ethereum blockchain supports smart contracts
  - Following the Merge in September 2022, Ethereum is based on the PoS consensus mechanism
- DeFi is not as decentralized as its name suggests – on PoS blockchains, the top 10, 50, and 100 validators are reported to account for 14%, 32%, and 41% of stakes[1)]
- In trading and yield farming, DeFi struggles to compete with centralized exchanges and centralized lending platforms

1) See [MS].

Nonfungible Tokens (NFTs)

NFTs are tokens that purport to represent ownership of unique items

- NFTs purport to establish ownership of assets on the blockchain
  - NFTs replicate for digital assets properties like scarcity, uniqueness, and proof of ownership
  - NFTs are used primarily to establish ownership on intangible assets (mostly, digital art)[1)]
  - NFTs are tradeable (on the blockchain), and they can be used as collateral in a decentralized loan
- The term nonfungible means that the token is defined by unique properties
  - NFTs are digitally unique and in this way, they are not fungible
  - In comparison, dollar notes are fungible, even though they all have different serial numbers
- Artists ("content creators") can access a global market
  - Creators can retain ownership rights over their work and claim resale royalties

See Ethereum, https://ethereum.org/en/nft.

1) "[T]he legal rights conveyed by NFTs are often unclear, raising issues that courts may have to resolve." See U.S. Department of the Treasury (September 2022) Crypto-Assets: Implications for Consumers, Investors, and Businesses, page 23. https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

Central Bank Digital Currency

Central banks are evaluating the introduction of central bank digital currency (CBDC)

- About 100 central banks pursue CBDC projects, which are in various stages[1)]
- Four countries have introduced a CBDC at the retail level[2)]
- There are 29 pilots, the most notable of which is China's digital yuan
  - On January 4, 2022, the People's Bank of China released its e-CNY wallet application on cell phone app stores for users in 10 major cities, with expansion to another 11 cities announced in April 2022
  - The digital yuan is issued by the People's Bank of China to participating banks, who issue it to their customers, akin to the two-tiered banking structure of paper currency
- The digital dollar is in the research stage
  - On January 20, 2022, the Federal Reserve published "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," a discussion paper on a digital dollar, with request for comment[3)]

1) See Bank for International Settlements (August 24, 2020, updated July 1, 2022), "Rise of the central bank digital currencies: drivers, approaches and technologies – Update July 2022," https://www.bis.org/publ/work880.htm.
2) These countries are The Bahamas, the Eastern Caribbean, Nigeria, and Jamaica.
3) See [BG]. See also [ECB].

Central Bank Digital Currency

Central bank digital currency is a digital liability of the central bank

- A CBDC makes central bank currency in digital form widely available to the public
  - Currently, the only type of central bank money available to the U.S. general public is paper currency in the form of Federal Reserve notes
  - A digital dollar would be an alternative to (or substitute for) private digital currency, meeting the increased demand for digital payment services, without credit or liquidity risk
  - Specifically, a digital dollar would offer households and businesses access to innovation in digital payment systems, including more efficient cross-border payment options
- The Federal Reserve calls for the U.S. CBDC to have the following four properties:

  Privacy-protected, intermediated,[1)] widely transferable, and identity-verified

1) "The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals, and such accounts would represent a significant expansion of the Federal Reserve's role in the financial system and the economy. Under an intermediated model, the private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments. Potential intermediaries could include commercial banks and regulated nonbank financial service providers [that] would operate in an open market for CBDC services."
See [BG].

Central Bank Digital Currency

Modernization of the international payment system

- Interoperable CBDCs can lay the foundation for modernizing an international payment system that is outdated and costly to operate
- Says Sir Jon Cunliffe (Bank of England deputy governor and Chair of the Committee on Payments and Market Infrastructures at the Bank of International Settlements):[1)]

  . . . despite . . . technological advances it can still take as long as 10 days to transfer money to different jurisdictions. And that transaction can cost up to 10 percent of the value of the transfer. A payment from the UK to some countries has to go through four currencies and as many as five banks.

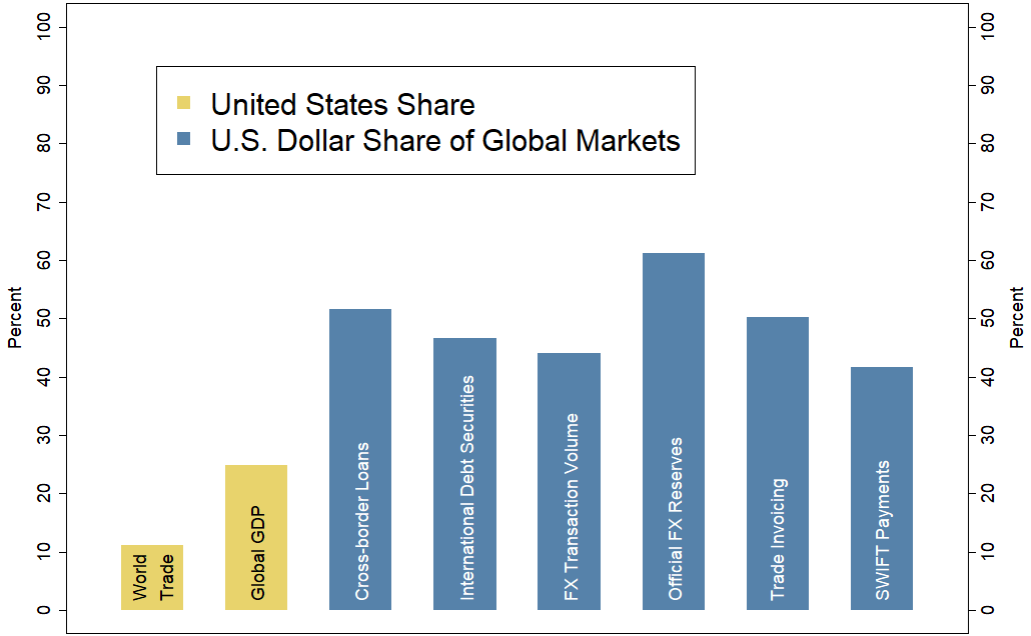
  Cross-border payment systems still use message formats developed 100 years ago for the telex machine. For decades, they have been the forgotten corner of the global financial plumbing.

See [BG].

1) Financial Times (July 13, 2020) "Cross-border payment systems have been neglected for too long." https://www.ft.com/content/a241d7e0-e1de-4812-b214-b350cbb7d046.

Central Bank Digital Currency

Preserving the role of the U.S. dollar in the international financial system



Notes:

Data and footnotes sourced from Bank of International Settlements (June 2020) "US dollar funding: an international perspective." Report prepared by a Working Group chaired by Sally Davies (Board of Governors of the Federal Reserve System) and Christopher Kent (Reserve Bank of Australia), https://www.bis.org/publ/cgfs65.htm.

FX (Foreign Exchange) Transaction Volume, which the data source stated as a share of 200 percent, was divided by 2.

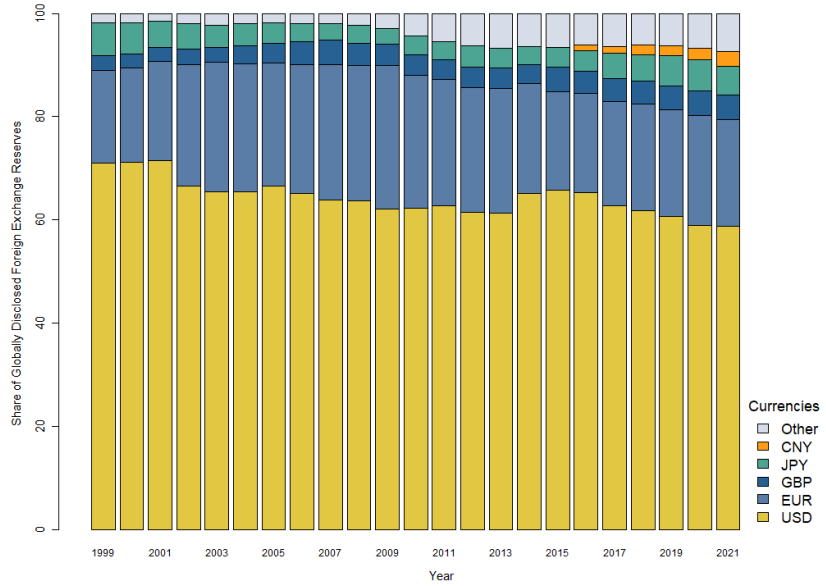
Notes in data source:

(1) Data refer to 2019. (2) Data refer to 2019. (3) U.S. dollar-denominated cross-border loans by banks to counterparties in all countries; data refer to Q4 2019 (excluding interoffice claims but including interbank claims on account of loans and deposits); loans comprise non-negotiable debt instruments that are lent by creditors directly to a debtor or represented by evidence of a deposit. (4) U.S. dollar denominated international debt securities by all issuers; data refer to Q4 2019; these securities are issued outside the local market of the country where the borrower resides, and capture issues conventionally known as eurobonds and foreign bonds and exclude negotiable loans; instruments such as bonds, medium-term notes and money market instruments are included. (5) Data refer to 2019. (6) Data refer to Q4 2019. (7) As estimated in Gopinath (2015). (8) Data refer to February 2020.

Sources: Gopinath (2015); Federal Reserve; IMF; CPB World Trade Monitor; Bloomberg; SWIFT; BIS Triennial Central Bank Survey of Foreign Exchange and Over-the-counter (OTC) Derivatives Markets; BIS locational banking statistics (LBS).

Central Bank Digital Currency

Preserving the role of the U.S. dollar as a reserve currency



Foreign central banks hold U.S. dollar reserves in Treasurys, which serve as the world's safe asset. It has been shown that, as a result of Treasurys being highly valued, the United States can borrow at lower yields than other advanced economies.[1)]

Further, it has been shown that for the period 1980-2021, the internal rate of return on holding U.S. Treasurys is about 1.5 percentage points (150 basis points) per annum lower for foreign investors (including foreign central banks) than for U.S. investors (excluding the Federal Reserve). This difference in returns is related to the timing of foreign investments. Foreign demand for Treasurys is highest at times when the value of Treasurys as a safe asset is highest (which in turn is related to financial conditions).[2)]

1) Jian, Zhengyang, Arvind Krishnamurthy, and Hanno Lustig (2021) Foreign Safe Asset Demand and the Dollar Exchange Rate. Journal of Finance 76(3), 1049–1089.
2) Jian, Zhengyang, Arvind Krishnamurthy, and Hanno Lustig (2022) The Rest of the World's Dollar-Weighted Return on U.S. Treasurys. https://www.nber.org/system/files/working_papers/w30089/w30089.pdf.
Data source: International Monetary Fund (IMF), Currency Composition of Official Foreign Exchange Reserves (COFER), imf.org.
Note: Share of globally disclosed foreign exchange reserves (allocated reserves). Foreign exchanges reserves are stated in current U.S. dollars (i.e., at current exchange rates). That is, in any given year, the shares of the various currencies in the total depend on the exchange rate at the time. Data are annual, as of Q4, and extend from 1999 through 2021. Legend entries appear in order from top to bottom. Chinese renminbi (CNY) is zero prior to Q4/2016.

Thank you

Frank Schmid

frank.schmid@genre.com

203 461 1944