

What Are Stablecoins and the New GENIUS Act?

Paul S. Wang, Sofpower.com

August 10, 2025

According to Reuters (July 18, 2025) “*U.S. President Donald Trump on Friday signed a law to create a regulatory regime for dollar-pegged cryptocurrencies known as stablecoins, a milestone that could pave the way for the digital assets to become an everyday way to make payments and move money.*”

The new law is the *Guiding and Establishing National Innovation for U.S. Stablecoins Act* (GENIUS Act) which passed congress with bipartisan support. It is the first major U.S. federal law that specifically and comprehensively regulates a type of cryptocurrency, namely stablecoins. It is a landmark signal that society is moving into the digital age full steam, not just in communication and commerce, but in how we define and transfer money itself.

We shall explain, in simple and easy terms, what is a cryptocurrency (crypto) and how cryptos are made to work. Then, we’ll see what stablecoins are, who can issue them, their purposes, usage, and distinction from other cryptos such as Bitcoin.

This article is part of our ongoing Computational Thinking (CT) blog published in *aroundKent* (aroundkent.net), an online magazine. Other enjoyable and engaging CT articles can also be found in the author’s book *Becoming A Computational Thinker: Success in the Digital Age*. Please see the website computize.org/CTer for more information.

Lets begin with some background information on cryptos.



Figure 1: Cryptocurrency

Making Digital Money Possible

Stablecoin is a type of *cryptocurrency* (colloquially crypto). A crypto is a **digital currency** designed to work on computing devices and networks. A crypto can be created by anyone and does not necessarily rely on any central authority, such as a government or bank, to uphold or maintain it.

A crypto can act as **digital cash** among willing users. Thus, it is different from debit/credit-card based *electronic funds* which are backed by real money and whose use must go through and be approved by an intermediary, namely a bank, who may charge a fee.

Algorithms and digital techniques are used to turn physical and tangible money (e.g. bills or coins) into digital tokens, namely coded data, that are handled by dedicated apps and transferred electronically.

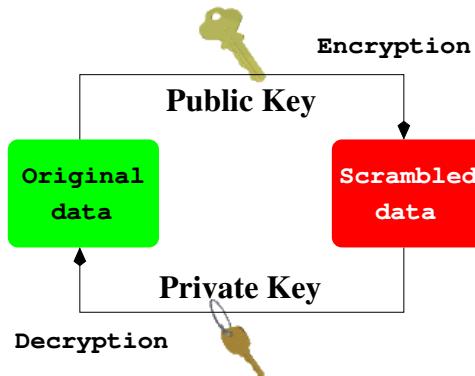


Figure 2: Public-Key Cryptography

Public-key cryptography (Figure 2) is a critical enabling technology and a

significant improvement to the usual *symmetric cryptography* where a single secret key is used to perform both encryption and decryption. To *encrypt* means to scramble data so it becomes unreadable. Whereas to *decrypt* means to unscramble data and return it to its original readable form.

The public-key system uses not one but *a pair of complementary keys*: **data encrypted by either key can be decrypted by the other**. Keep any one key secret (*the private key*); allow the other shareable (*the public key*).

In secure data communication, data to be sent is encrypted with a particular receiver's public key who then decrypts using their private key. For safety, the private key is kept strictly secret. A private key owner can encode data with it and create a **signed-by-me version** which can be decoded by anyone with the paired public key to read and know (prove): (a) who the signer is, (b) the data is unaltered.

In any given crypto system, each participating user gets a *wallet* app that can send and receive digital money. The wallet usually keeps its owner's public-private key pair. Let's see how that can overcome these three major problems that paper money doesn't have:

1. Ownership

Problem: If money is just data on a computer, how do we know who is the owner? With paper money if it's in your hand, it's yours.

Solution: Personal wallets—Every user has their own wallet (app) where they can access and spend their digital currency. Of course, only the owner has access to their wallet. The wallet is usually integrated with the user's public-private key pair. The wallet's public key identifies it as well as its owner and can be regarded as the owner's address in the crypto system. Using their wallet, a user can provide/reveal the public key to another user in order to request payment. The public-private key pair is usually generated, stored and used inside the wallet. **If an owner were to lose/forget the private key or password to their wallet, then access to all their cryptos would be lost.**

2. Transactions

Problem: With paper money, you simply hand it over to the receiver.

How do we move digital money from sender to receiver?

Solution: A sender accesses their wallet and creates a *transaction record* stating the amount and the receiver's wallet which is identified by its address or public key. The record may also include a memo with other relevant information. The transaction record is signed with the sender's private key. The signed record, together with the sender's public key, is immediately published to the crypto system for validity checking. When the transaction has been verified and placed on **the blockchain** (see item 3 below), the receiver's wallet would see it and update the receiver's balance. Offline transfers can take place but would be verified later online.

3. Prevention of Duplication/Double Spending

Problem: With paper money once you spend it, you don't have it anymore. But, digital tokens can be *copied perfectly*. What stops someone from spending the same digital token twice or even endlessly?

Solution: A crypto system keeps track of all transactions in a secure ledger, a data structure known as a *blockchain*. New transactions are verified and grouped into a data block, and this new block is then cryptographically linked to the previous one forming a chain, thus blockchain.

Data blocks on the blockchain can't be changed. Thus, the blockchain ledger is an unalterable record of who owns/has how much at any time as well as sources of funds. Depending on the crypto's policy, the validity and integrity of each new transaction to be placed on the blockchain would be verified and maintained by a central entity (e.g. a bank), by agreement among certain independent entities, or by consensus among participating public as in the case of Bitcoin or Ethereum.

These solutions and their underlying technologies open up great potentials:

- You can own and control money in digital forms
- You can couple money/payments with code and programming

- You can transfer/receive them online or by other electronic means in anonymous fashion
- You don't need to involve banks or credit/debit cards

They become the foundation that empowers all types of cryptos including **Bitcoin**, **stablecoins**, and **CBDCs** (central bank digital currencies).

Bitcoin

In 2009 Bitcoin was introduced and its software made publicly available. Almost immediately, *mining*, the process which creates newly minted Bitcoins and verifies transactions by public consensus on a distributed blockchain, began.



Figure 3: Bitcoin

It is reasonable to say that Bitcoin started the modern age of cryptocurrency. But, as it turned out, Bitcoin was, and still is, widely used in unscrupulous or illegal businesses due to its apparent *owner anonymity* property. However just the opposite is true, the Bitcoin blockchain can be used by law enforcement to track down criminals, or others for that matter, with relative ease.

Bitcoin's value is not backed by any assets. Its trading price has always been extremely volatile. In fact, it created a marketplace for wild speculations and illegal get-rich-quick schemes. Due to concerns over financial stability, illegal activities, and regulatory control, many countries such as China, Egypt, Qatar, Saudi Arabia, Jordan and others, have banned or restricted use of

Bitcoin and similar cryptos. Furthermore, according to Greenpeace, governments worldwide are increasingly expressing concerns about the significant energy consumption associated with Bitcoin mining.

Regarding its investment value, Warren Buffett famously referred to Bitcoin as “rat poison squared,” indicating his strong disapproval. He has repeatedly stated that Bitcoin has no intrinsic value and does not produce anything, aligning with his investment philosophy of favoring tangible assets.

CBDC

You may ask the question “can we create a digital form of money that is better?” The answer is yes. In fact, many countries are looking into or have already launched *Central Bank Digital Currencies* (CBDCs). In most cases, a CBDC is a digital form of a country’s currency issued by its national central bank and is legal tender.



Figure 4: Sand Dollar and e-CNY

In other words, a CBDC functions as digital cash of a country. It can be used on computing devices such as smartphones, smart cards, laptops, and so on, online or offline. Table 1 lists some countries and their live or piloted CBDCs.

Issuing and maintaining a CBDC is complex and challenging for a country. For example Bahamas’ Sand Dollar has limited adoption. And the Venezuela Petro launched in 2018 was closed down after five years.

In July 2025, the U.S. Administration has taken steps to prohibit the development and issuance of a U.S. CBDC (digital dollar), by the Federal Reserve.

The same Administration has also signed the GENIUS Act into law creating a regulatory framework for privately issued *stablecoins*. These develop-

Country	CBDC Name	Status
Bahamas	Sand Dollar	Fully launched (2020)
Jamaica	Jam-Dex	Fully launched (2022)
Nigeria	e-Naira	Fully launched (2021)
India	e-Rupee	Pilot live, expanding across cities
China	e-CNY (DCEP)	Public pilot in many cities
Russia	Digital Ruble	Official launch, pilot wallets (2023)

Table 1: CBDC Examples

ments indicate a differentiation in policy between a government-issued digital currency and privately issued stablecoins. Some view these actions as part of the US efforts to counter de-dollarization in the world.

Stablecoin

Stablecoins are digital tokens, backed by real currency (e.g. the US dollar), that transfer quickly online usually with low transaction fees, known as *gas fees*, normally paid by the money sender. Issuers make stablecoins easy and fast to transact in many directions and also aim to maintain their value stable, at \$1 for example. Basically, you give \$1 → you get 1 stablecoin. If you have one then you can turn it back into \$1. Thus, we expect stablecoins to not increase or decrease in value. They are stable by design unlike cryptos such as Bitcoin or Ethereum that can rise or crash—stablecoins are for ease of transfer, not gambling.

Still, stablecoins also play a crucial role as on-ramps and off-ramps (moving assets to/from) in the cryptocurrency ecosystem, facilitating the transition between traditional currencies and the world of digital assets.

As examples, let's list three top stablecoins in the U.S. (Figure 6):

Tether (USDT)

Issuer: Tether Limited Inc., based in Hong Kong, launched the USDT stablecoin.

Backing: USDT is backed by a combination of highly liquid and secure assets like short-term U.S. treasury bills and cash equivalents. Backing also includes riskier assets such as precious metals, secured loans, and other investments with less transparency.



Figure 5: Stable on Financial Express



Figure 6: Tether, USDC, PYUSD

USDC (USD Coin)

Issuer: Circle is the issuer of the USDC stablecoin.

Backing: USDC is 100% backed by highly liquid cash and cash-equivalent assets, primarily held in the Circle Reserve Fund and regulated financial institutions. These reserves undergo monthly attestations by an independent accounting firm.

PYUSD (PayPal USD)

Issuer: PayPal USD, as part of PayPal, is issued by Paxos Trust Company, LLC, a fully licensed limited purpose trust company that is regulated by the New York State Department of Financial Services.

Backing: PYUSD is fully backed by US dollar deposits, US Treasuries, and similar cash equivalents, according to PayPal. Paxos publishes monthly reserve reports and third-party attestations of the reserve assets to ensure transparency.

Among stabecoins, PayPal USD is perhaps the easiest to use by ordinary

people due to these reasons:

- PYUSDS are used inside PayPal and Venmo. There is no crypto wallet needed.
- No conversion fees are charged.
- Value kept stable with 1:1 backing by dollars and U.S. Treasuries.
- PYUSDS can be sent, spent, or cashed out at any time.

Why Use Stablecoins?

Use Case	Why It Helps
Instant transfers	Faster than banks or wires
Cross-border transfers	Send money globally for low fees
Digital shopping	Pay online without cards
Freelancer payments	Get paid in USD, no middlemen
On/off ramp for cryptos	Easy transfers on blockchains

The GENIUS Act

As we have mentioned, Congress passed the first major stablecoin law, the GENIUS Act. Here are key points of this law:

- Only licensed companies can issue stablecoins.
- All coins must be backed by real dollars or Treasuries.
- Regulators like the Fed can oversee, approve, or stop issuers.
- People must be able to redeem coins back to cash.
- Violations can result in fines or shutdowns.

The law regulates stablecoins issued by private enterprises. Unlike deposits in FDIC-insured bank accounts, stablecoins are not backed by the full credit of the US government.

Banks, credit card companies, and large businesses such as Amazon and Walmart are considering adopting/launching stablecoins, according to the *Wall Street Journal*.

Crypto Is Still Evolving—Stay Informed

As usage of cryptos increases, a number of dedicated ATMs are beginning to appear. A crypto ATM (or Bitcoin ATM) is a physical machine—often located in convenience stores, malls, or airports—that allows people to buy cryptos using cash or debit/credit cards and (in some cases) to sell them and withdraw cash.



Figure 7: A Crypto ATM

Even though crypto has existed for over a decade, it remains a rapidly evolving field. The technology, regulations, and user behaviors surrounding crypto continue to change and mature. This includes not only volatile cryptos like Bitcoin, but also stablecoins that are intended to be less risky.

Remember, stablecoins are not risk-free. They are still subject to:

- Operational and software vulnerabilities (bugs, hacking),
- Trust in centralized issuers and custodians (unethical behavior),
- Market disruptions or liquidity crises (bank failures),
- Regulatory changes and legal actions (money laundering).

Even regulated stablecoins may experience issues, such as temporary loss of peg value or transparency concerns about their reserves.

Users and investors are well advised to proceed with eyes wide open. Crypto assets, including stablecoins, should be used with awareness and caution. Individuals are encouraged to:

- Learn about the specific coins and technologies they use,
- Understand the risks of storing and transferring digital assets,
- Avoid overexposure to volatile or poorly regulated assets,
- Keep up with legal and technological developments.

Summary and Final Thoughts

Public-key cryptography and the blockchain are the key enabling technologies for cryptos. Digital money has come a long way and is increasing in use world-wide.



Figure 8: Using Stablecoins

In the US, the official CBDC, or *digital dollar*, has become prohibited by law since late July, 2025. Meanwhile, stablecoins came under legal regulations, making them safer and more useful. Thus, stablecoins have the potential to be a substitute for the digital dollar. Used wisely, they offer speed, access, and simplicity—while still staying stable in value.

Cryptocurrency is still young. While it holds great promise, it also carries unique and sometimes hidden risks. Enter the space informed, careful, and watchful.

To look a bit deeper, readers may find my CT articles on Bitcoin and CBDC interesting and informative. You can find them on *aroundKent* or simply contact the author and ask for a copy.

It becomes obvious that a basic understanding of digital money is an important aspect of *computational thinking*. Soon, even something simple and common as money will require some non-trivial knowledge of computing!