1

Money and Cryptocurrencies

This chapter traces the intellectual and technological lineage of Bitcoin and digital money. While Nakamoto's white paper launched Bitcoin, its roots extend through decades of economic theory, cryptographic innovation, and activist movements. We examine how the Austrian and Chicago Schools of Economics provided a framework for stateless and noninflationary money, and also how Cypherpunk ideals shaped the push for privacy and decentralization. The chapter reviews early experiments with digital currencies such as DigiCash, b-money, and e-gold, highlighting the technical shortcomings, regulatory battles, and user adoption barriers that prevented their success but furnished essential building blocks for Bitcoin. We then contrast the classical financial attributes of money – medium of exchange, unit of account, and store of value – with additional digital requirements such as offline spendability, identity-less spendability, and fungibility. Finally, we show how Bitcoin resolved the long-standing double-spending problem without a central authority through Proof of Work, situating it as both a culmination of earlier efforts and the starting point for a new era of cryptocurrencies.

Although Nakamoto's paper marked the launch of Bitcoin, the system's intellectual roots lie in a wider lineage. Earlier work on blinded signatures by David Chaum, the structure and vulnerabilities of centralized digital gold projects like e-gold, and the ideological foundations laid by the Cypherpunks all contributed essential ingredients. Moreover, regulatory responses after 9/11 and ongoing battles over anonymity and control further shaped the environment in which Bitcoin emerged. It is more accurate to view Bitcoin as a culmination of technical lessons and philosophical motivations stretching across decades, rather than a sudden and solitary invention.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

1.1 A Brief History of Digital Money

Although Bitcoin is the first cryptocurrency, history is littered with earlier attempts to create a digital currency online. We can point to financial and technological developments that drove the push for digital currency. In finance, two schools of thought have traditionally encouraged digital money: the Austrian and Chicago schools. Adherents of the Austrian School of Economics (since the 1880s) believe that certain commodities came to be used as money naturally, and money is not an invention of the state. Digital currency can be used to circumvent the state control of money. The second school is the Chicago School of Economics (since the 1930s), whose adherents envision an economy that is governed by free markets with minimal or no government intervention. The 1974 Nobel Prize in Economics was awarded to Friedrich Hayek, an economist from the Austrian School of Economics [65], giving more prominence to the school and its aversion to central banks. Both schools oppose money printing by states and central banks, because the resulting inflation reduces the value of savings as prices of goods go up over time. The schools wanted to diminish the role of the state and central bank in modern society.

> Fiat currencies have circulated for thousands of years, and sooner or later nearly all of them have been inflated down to worthlessness by governments confronted by strained public finances.
>
> *David Yermack [404]*

In technology, the Cypherpunk movement creates and uses tools to change society. Cypherpunks saw a perfect conduit for their aims in digital currency. The Cypherpunks' aversion to central control and the schools' opposition to state and central banks created a synergy that has helped digital money become mainstream.

Info:

A Cypherpunk is an individual or group that promotes the use of cryptography and privacy-focused technologies to protect personal freedom and enable social or political transformation. Emerging in the late 1980s, the movement organized through an electronic mailing list where participants discussed how encryption could secure communication, defend privacy, and reduce reliance on centralized authorities. ♦♦

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002

From the outset, digital money encountered several fundamental problems. A significant hurdle was the need for a central authority to keep track of account balances and digital payments among users. Companies that invented digital currencies proposed to be the central authorities themselves. In a sense, rather than eliminating financial institutions, the companies tried to replace them and become de facto central banks. This approach never gained traction among digital currency users. An alternative to the central authority approach was to use a distributed, public ledger to track user balances; every user stores transactions and account balances of all others. Although straightforward in theory, this solution is unfeasible because information about transactions cannot be transmitted digitally in a fast and reliable manner. As a result, observing all transactions in real time is impossible. The networks are faulty, and malicious users try to benefit from lying about balances. In fact, the problems with this approach, known as the Byzantine Generals' Problem, have been a well-studied topic in distributed systems [229]. Up to the seminal Bitcoin paper by Satoshi Nakamoto [285], multiple times, digital currencies seemed to have finally succeeded in creating a viable payment method [175]. Hindered by laws and regulations, but mostly because of technical shortcomings, none of these currencies took root. Each failure, however, allowed digital enthusiasts to learn from the experience and propose a new building block toward a viable currency.

1.2 Attributes of Money

To understand what makes a digital currency successful, we first outline its desired attributes. We make a distinction between the financial attributes of traditional money and the attributes required for the digital world.

1.2.1 Financial Attributes

In traditional finance, money must have three attributes: *medium of exchange*, a *unit of account*, and *store of value*. As we will describe in this section, each attribute is challenging to implement in a digital currency.

As a medium of exchange, money must allow users to intermediate the exchange of goods and services. In this role, money facilitates trade by allowing people to convert their goods and services into a certain amount of money that can buy goods and services. Without a medium of exchange, a society can only use barter in trade. A medium of exchange creates efficiency in trade; goods can be sold for money, whereas in a barter system, the needs of the two parties must coincide at a specific time. The medium of exchange does

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

not specifically mention the physical properties of money, but ideally, money should be easily transportable. History has interesting examples of physical money that did not conform to this rule. On the Micronesian island of Yap, a form of stone money, known as Rai or Fei, was up to 4 m (12 ft) in diameter [162]. The stones generally remained in place, and ownership was transferred by public announcement. This stone money was traded for centuries until an Irish-American shipwreck survivor, David O'Keefe, reached the island in 1871 and introduced iron tools, making stone quarrying much easier. As production increased, new stones lost much of their value compared to the older, historically significant ones, leading to inflation in the money supply.

A unit of account is a standard monetary unit of measurement for prices of goods and services. This allows price comparisons of goods. For example, a shop that charges 10 money for a haircut is cheaper than the one that charges 11 money. Traditionally, money has denominations that can also act as units of account. For example, 1 dollar (main unit) is worth 100 cents (sub-units). With very few exceptions, most currencies have decimal denominations; the ratio between the main unit and the subunit is an integral power of 10. The number of denominations affects the written prices of goods and services. For 100 subunits, the price must allow two decimals, such as 27.99 USD.

Remark 1.1 In community practice, bitcoin (lowercase) denotes currency units (e.g., 2.5 bitcoins), whereas Bitcoin (uppercase) refers to the software, protocol, and community.

Existing digital currencies use denominations that complicate the reporting of prices. On the Bitcoin blockchain, one bitcoin contains 100 million (10^8) *Satoshis*. Rather than using this many decimals in bitcoin amounts, Bitcoin stores all transfer amounts in Satoshis. For example, 10.00000057 bitcoins (10 bitcoins and 57 Satoshis) are recorded as 1,000,000,057 Satoshis. In any case, merchants and buyers are unaccustomed to dealing with these many decimals or amounts in ordinary transactions. This problem also exists in newer cryptocurrencies. For example, on Ethereum, 1 Ether (ETH) contains 10^{18} *Weis*, a denomination that makes everyday transactions cumbersome to express. Ethereum has designated certain amounts of subunits, such as KWei = 1000 Wei, to alleviate the price issue, but these subunits are rarely utilized. In the unit of account, a further complicating issue with a cryptocurrency is the volatility of its price. The currency is not tied to a gold standard, nor is its value backed by a central government. The intrinsic value of the currency is measured by the strength of its community, market, and technology. These factors make a currency appealing and encourage its trade. However, as happened in the Mt. Gox exchange hacking in 2010, the technology can be hacked, the community

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

may lose its interest, and the market may experience sudden disruptions. For example, the price of bitcoin dropped on the Kraken exchange from $11,200 to $101 Canadian Dollars on May 29, 2019, due to a technical issue. Although it lasted only a minute or so before the price stabilized, in the past, cryptocurrency prices have seen volatility for longer periods. In these events, there is no central authority to correct or halt the price. Eventually, the price will stabilize in a worldwide distributed market, but five bitcoins from yesterday may be worth much more than six bitcoins today. During this volatility period, the currency ceases to have a unit of account that can be used for price comparisons.

Info:

Based in Tokyo, Japan, Mt. Gox was the biggest online exchange for Bitcoin, where bitcoins could be sold for or bought with fiat money. It handled over 70% of all Bitcoin transactions in 2014. In February 2014, it announced that hackers had stolen 850,000 bitcoins from its wallets. The company filed for bankruptcy. ♦♦

A third issue with the unit of account attribute is related to cryptocurrency price arbitration. The currency is traded on multiple online exchanges worldwide. In local exchanges, the price increases if there are more buyers than sellers. Although global demand and supply have a correcting effect on local prices, price differences can consistently exist over time. For example, during 2017 and early 2018, demand for cryptocurrencies in Korea was so high that Korean exchanges often sold bitcoins for up to 30% above prices in other countries. This price difference was known as the Kimchi premium. Cryptocurrency markets use the worldwide buy and sell prices of a cryptocurrency to determine its price in fiat money. In other words, a kind of averaging is done to determine the global price. In this price arbitration, exchanges usually excluded Korean prices. As a result, a good that costs one bitcoin in Korea may have been cheaper than 0.9 bitcoins in Japan, undermining the unit of account attribute of the currency.

To act as a *store of value*, money must be reliably saved, stored, and retrieved, and be predictably usable as a medium of exchange when it is retrieved. In other words, it should still be valuable in the future. In this sense, gold is the ultimate store of value as it does not decay, rust, or lose its weight over time. The store of value of cryptocurrencies is a hotly contested topic. A problem is that cryptocurrency storage depends on saving private keys associated with the storing address. Private keys are character strings such as E9873D79C6D87DC0FB6A5778633389. Coins stored in an address cannot be

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002

spent without using the associated private key. Losing the private key due to software failures, hardware problems, and theft creates an irreversible loss to the coin owner. Stories such as a user throwing away a hard drive that contained private keys for 7,500 bitcoins are not rare in cryptocurrencies.

When gold is lost, it may be found by others in the future. When coins are lost, it is not feasible to bring them back, as it would require reverse computing the private keys associated with the address, which is thought to be nearly impossible.

1.2.2 Digital Attributes

In the real world, digital money faces problems that traditional money does not. We list *offline spendability*, *identity-less spendability*, and *fungibility* as desired attributes of a digital currency. As digital money that is owned by someone does not have a physical representation, such as money bills or gold bars, digital payment cannot be accepted without verifying that the sender has the money. For example, when a credit card is used to buy a good, a bank should confirm that the spender has enough money to pay the amount. This requires that an entity that keeps track of the balances of every user stay online at all times to confirm every payment.

In real life, money bills are offline spendable, which means that bills can be handed over to complete a transaction without requiring any further verification or record. In the digital world, offline spendability would require making a payment even when the sender or the receiver is not connected to the digital world.

Offline spendability allows digital money to be used in a private and secure manner; payments cannot be tracked, and users cannot be profiled in terms of their spending habits. Although highly sought-after, offline spendability is very difficult to attain in a digital world. In Bitcoin's case, a transaction lists sender and receiver addresses and amounts that anyone can verify. However, the receiver cannot know if the specified coins have already been used in a contemporaneous transaction. This is known as the *double-spending problem*. In this sense, Bitcoin and other cryptocurrencies do not have the offline spendability attribute. In the absence of offline spendability, we may run into a problem of traceable payments among Bitcoin users. The *identity-less spendability* attribute requires that addresses, that is, digital money accounts, can be created without proof of identification, such as a passport or national identity card. Ideally, it should also be cheap and easy to create an address that sends and receives digital money. Traditional cryptocurrencies, such as Bitcoin and Litecoin, are identity-less, where anyone can take part in the blockchain network. The wallet software that connects a user to the blockchain is publicly

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

accessible and does not require a login process. In theory, the identity of an address owner cannot be learned by analyzing its blockchain transactions.

Info:

A *cryptocurrency wallet* is a software application, hardware device, or other medium that manages the public and private keys associated with a blockchain address. It enables the user to monitor balances, receive funds, and authorize transactions. The wallet does not hold the cryptocurrency itself; rather, it provides access to the digital assets recorded on the blockchain. ♦♦

Despite this identity protection, Bitcoin is only pseudo-anonymous, or *pseudonymous*. A Bitcoin transaction lists its inputs, which are outputs of earlier transactions. In such a linked transaction network, it is possible to trace how certain coins have flowed in the network. Once the identity of an address is learned by external means, it is possible to see all previous sending and receiving transactions by the address. If a bitcoin is received by theft or similar crime schemes and put into a so-called *black* address, online exchanges can shun the coin. Exchanges will not accept payments made by the associated address. Similarly, miners may choose not to include transactions that involve the black address.

We explain the risks and dangers associated with the unwanted history of an address with the *fungibility* attribute. If a unit of good can be exchanged for the same unit of good in another place, the good is *fungible*. For example, gold is fungible because a gram of gold in the US is worth a gram of gold in Russia. Bitcoins, however, may not be fungible because selling or buying tainted coins is difficult due to legal issues. In Chapter 11, we will explain how some risks in Bitcoin transactions can be alleviated. *Taint analysis* is used to find out whether a unit of currency is tainted because it is acquired through a crime such as theft or ransom.

1.3 Road to Bitcoin

One of the earliest and most influential expressions of the Cypherpunk ethos appears in “A Cypherpunk’s Manifesto” by Eric Hughes, which argues that privacy is essential for an open society and must be secured through anonymous transaction systems developed by those committed to writing the necessary code 202.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

For activists in the Cypherpunk tradition, privacy was never an optional feature of the digital age; it was foundational. They argued that large institutions would not voluntarily protect individual privacy and that digital systems needed to be designed to empower users by default. This belief led to the development of privacy-preserving tools and, eventually, efforts to build anonymous transaction systems. These systems were not intended to conceal criminal activity but to uphold the principle that individuals should control when and how their identities are revealed. Within this ethos, the creation of digital currencies that function without centralized oversight was seen not only as a technical challenge but as a moral imperative.

Having covered the financial and digital attributes of money, we now look into the problems experienced by key digital currencies of the past.

In 1994, FirstVirtual created a digital payment system where customers and merchants had to have known accounts in the system. The system functioned as follows. The merchant creates a transaction and sends it to the email address of FirstVirtual. The transaction lists the money amount, merchant, and customer information. Next, FirstVirtual sends a confirmation email to the customer; if the customer replies with OK, it pays the money to the seller after a delay of 90 days. Within this time, the customer can report a dispute for the transaction. An immediate problem with the FirstVirtual system is that it requires all parties to be known; the system does not allow identity-less payments. Offline spendability is possible in theory because the merchant can trust the customer and hand over the goods without waiting for confirmation from the bank. However, the trust-based solution is not viable because trust scales poorly. To complicate everything, the merchant could only receive the paid money on the 91st day.

In 1996, the Secure Electronic Transaction (SET) architecture brought the idea of views into the payment system. A view is an encrypted description of the transaction. SET uses dual signatures; the customer signs the order information to the merchant and the payment information to the bank. The merchant creates a view of its own and sends its view and the view from the customer to a confirming entity, such as a bank. If both views align, the bank confirms the transaction. The bank cannot see the order, and the merchant cannot see the customer's account details. However, the bank can still see the merchant's identity and infer what is being traded. SET was an improvement over FirstVirtual because it abolished email confirmation. However, SET did not have offline or identity-less spendability. SET required each participant in the system to own a public key certificate to encrypt their view, which curtailed SET adoption by the masses.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009044114.002

Info:

In cryptography, a ***public key certificate***, often referred to as a ***digital certificate*** or ***identity certificate***, is an electronic record that confirms the ownership of a specific public key. It contains the public key itself, identifying details about its owner (the subject), and a digital signature from a trusted authority (the issuer) that attests to the certificate's authenticity. ♦♦

Mondex, b-money, Digicash, and e-gold are some other digital currencies that have failed to gain wide adoption due to various reasons, ranging from technical mistakes and coding bugs to the reluctance of users to adopt key technologies. In this ecology, different currencies have developed and tested some key aspects of Bitcoin. For example, Bitcoin has adopted a Proof-of-Work mechanism with a few tweaks to email spam detection. B-money used a peer-to-peer network where peers kept (predicted) everyone's balances.

Although we list the three desired attributes of a digital currency, history shows that attaining them can put a currency on a collision course with regulatory authorities.

E-gold created a digital currency backed by gold in 1996. E-gold users did not need identity documents to open an account; hence, the system was identity-less. Once e-gold was bought, it could be instantly transferred to any account in the world. Users could keep e-gold in their accounts indefinitely, or sell it and receive the amount in their local fiat currency in a bank account. Transaction fees were approximately 1% of the amount transacted. E-gold was an enormous success; in 2004, it had reached 3.5 million users in 165 countries. In 2006, it was processing billions of USD in payments.

In 2004, regulatory authorities targeted e-gold for abetting payments among criminals. As it could be used without an identity, e-gold had become a festering ground for all sorts of criminals who needed to move money between countries. Specifically, criminals who copied credit card details and sold them for cash had been paid through e-gold for many years. The concluding investigation specifically targeted the creator of e-gold, Doug Jackson, for the identity-less system he had developed. E-gold could not weather the crisis and officially closed its services in 2008.

The financial application of blockchain technology, Bitcoin, builds on past digital currencies that we have covered in this section. Learning from mistakes and intricately linking key technologies, Bitcoin has prospered to become the main digital currency. The cryptocurrency market now commands more than

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002

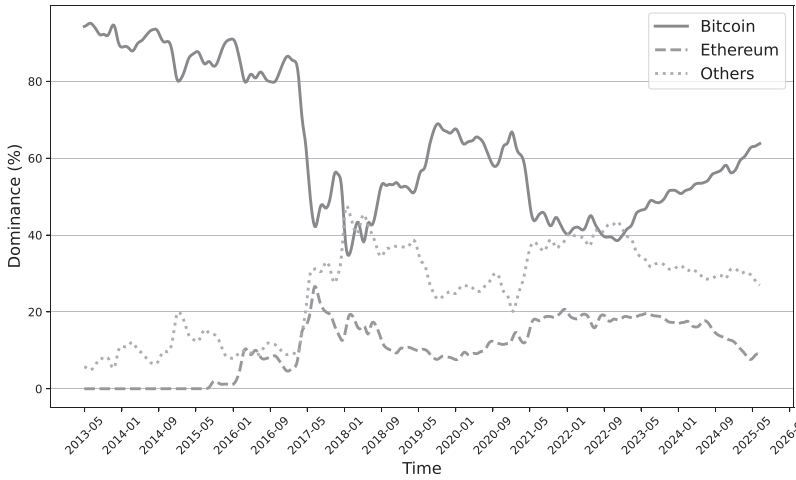


Figure 1.1 Market capitalization shares of Bitcoin, Ethereum, and other cryptocurrencies over time. Each line shows the proportion of total crypto market value held by that category at each point in time. Our data begins in 2013, which marks the earliest availability of reliable aggregated market capitalization records.

USD$4 trillion annually, and as Figure 1.1 shows, Bitcoin transactions account for over 60% of all cryptocurrency payments.

Bitcoin is accepted as money in many parts of the world, but the consequences of the first popular digital currency are not yet understood.

Emperor Wen (孝文皇帝, reign 179–157 BC) of the Chinese Han Dynasty wanted to set an example of thrift for his subjects to follow, and saying that he did not need to spend much, announced that he was relinquishing the state's monopoly of coinage [235]. His advisors protested, but the emperor did not change his decision. What happened next is instructive. Powerful houses produced their own copper money and raised a rebel army with their wealth.

Bitcoin cannot be produced as easily as copper money, but Bitcoin's source code can be forked to create new cryptocurrencies that have less restrictive coin-minting algorithms. Time will tell if such currencies will attain a large global market share.

Chapter Summary

- Bitcoin is often viewed as the first cryptocurrency, but its design incorporates decades of technical ideas and ideological motivations from earlier digital money efforts.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002

- Economic thought, particularly from the Austrian and Chicago Schools, influenced the push for stateless, noninflationary currencies by opposing central bank control over money.
- Cypherpunk activism contributed the privacy-preserving and decentralized ethos that underlies many digital currencies, especially Bitcoin.
- Digital money efforts before Bitcoin, such as e-gold, Digicash, and b-money, faced technical and regulatory challenges that prevented mainstream adoption. However, they provided building blocks for future systems.
- Money in traditional finance must serve as a medium of exchange, unit of account, and store of value. Cryptocurrencies struggle particularly with stability and consistent valuation.
- Digital currencies face additional design challenges: enabling offline transactions, ensuring spendability without identity, and preserving the fungibility of currency units.
- Bitcoin introduced a breakthrough by probabilistically solving the double-spending problem without a central authority, using a decentralized consensus mechanism based on Proof of Work.
- Regulatory resistance, user adoption barriers, and technical vulnerabilities continue to shape the success or failure of digital currency systems.
- The historical trajectory shows that each failed system contributed lessons that culminated in Bitcoin's success, though the evolution of digital money is still ongoing.

1.4 Reading List

- Yermack [404]: The author explains where cryptocurrencies fall short of being real money.
- Ammous [35]: Chapter 2 gives a history of money and the artifacts that were used to store value. Chapter 3 talks about gold and its history in the Roman Empire, the Renaissance, and the Belle Époque. Chapter 4 explains printed money in the modern age. Ammous (https://twitter.com/saifedean) is a fierce and controversial critic of state and central bank control on money and the economy. The book has been published in more than 20 languages.
- Burniske [80]: Chapter 1 gives a short history of how Bitcoin was created.
- Rid [329]: The author provides a history of the Cypherpunk movement that gifted us many privacy tools.

Exercises

1.1 In a typical digital currency, about what piece of information do we need consensus?

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002

1.2 What are the three attributes of a currency (money) in traditional finance?
1.3 What are the three attributes that an ideal digital currency would have?
1.4 How is the price of a bitcoin in a fiat currency determined?
1.5 If a good is worth the same value anywhere in the world, the good is considered fungible: True/False.
1.6 How does Bitcoin achieve the identity-less spendability attribute of a digital currency?
1.7 The price of a cryptocurrency can change too much over time (either increasing or decreasing). In that case, which traditional attribute of money does the cryptocurrency violate? Please explain your reasoning.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 21:51:19, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009004114.002