



# Historical Perspectives on Bitcoin

DR. JONATHAN TIEMANN

*“The mining, however, it turns out, has been principally done in the London Stock Exchange, instead of in the ‘diggings.’”*

— “S,” *London Correspondent for San Francisco Alta California newspaper, April 16, 1854.*<sup>1</sup>

## Nothing New Under the Sun.

Over the fast few months, cryptocurrencies have attracted a great deal of attention, and if the price action in Bitcoin is any indication, a significant amount of money. A number of high-profile businesspeople, including Tesla chief Elon Musk, have touted cryptocurrencies, and several mainstream financial institutions have grown cautiously supportive. The nation of El Salvador has begun an experiment in treating Bitcoin as legal tender. The listing of shares of cryptocurrency exchange Coinbase Global, Inc. (COIN) in April added a further veneer of legitimacy to the market for cryptocurrencies.

Since Bitcoin’s appearance in 2009, it has run up in price, attracting significant attention, several times. The current episode feels different from earlier ones, though. As Bitcoin’s price passed \$60,000 in April, more and more individual investors began expressing interest in Bitcoin, perhaps thinking that if they hesitate, they might miss out on big gains. More and more observers have begun to predict that cryptocurrencies will become a permanent feature of our financial landscape. Since some of this commentary and promotion is pure hype, teasing the truth out of the noise is the challenge for investors.

Advocates make several arguments for cryptocurrencies that go well beyond hype and appeals to greed or fear of missing out. Bitcoin’s proponents sometimes call it “digital gold,” because, like gold and unlike conventional money (which crypto-proponents deride as “fiat currency”), Bitcoin does not rely for its value on any claim against another party. Payments in bitcoin do not require a trusted intermediary for clearing and settlement, which means, proponents claim, that Bitcoin operates in a decentralized environment. Because the protocol limits, by fiat, the total supply of bitcoins ever to be created, they say it is

inflation-proof. Some also argue, unconvincingly, that bitcoin transactions clear quickly and at low cost.

For many, part of the appeal of cryptocurrencies derives from their use of technologies in cryptography and data communications. Despite these novel features, history can still help us see what might happen if they do become part of the mainstream economy. They will not blaze some new trail, skirting the costs and frictions of more familiar forms of money. A fully-developed crypto-economy is likely to include familiar features – and risks.

---

<sup>1</sup> “London Correspondence,” San Francisco *Alta California* newspaper, April 16, 1854. California Digital Newspaper Collection, [cdnc.ucr.edu](http://cdnc.ucr.edu)



Bitcoin, for example, simply cannot support the volume of transactions in a modern economy without a significant parallel infrastructure of intermediaries, often facilitating transactions with substitute instruments analogous to paper money. Its architecture seems likely to lead a concentration of economic power in the hands of a few well-capitalized firms, particularly in mining. And broad adoption of cryptocurrencies would drive a proliferation of ancillary schemes, many with merit, but also some straight-up swindles.

Intermediaries issuing credit-based instruments run counter to the fantasy that the crypto-economy can be trust-free and credit-free. Concentration of economic power undermines cryptocurrencies' purported virtue of decentralization. And a large enough number of successful swindles could erode confidence in cryptocurrencies in general and induce a regulatory response. A practical system would be far different from proponents' romantic ideal of technology-enabled money, free of institutional intermediation and centralized control.

## You Can't Hold a Bitcoin in Your Hand.

What is Bitcoin, really, and how does it work? The paper<sup>2</sup> outlining the design proposal for Bitcoin describes not a currency, but a mode of electronic payment not reliant on financial institutions as intermediaries. Bitcoin itself is just an arbitrary unit of account. Rather than requiring users to trust either a governmental issuer of currency or a bank, it relies on a peer-to-peer network. Anyone willing to download and run Bitcoin software can participate.

The futuristic coins bearing a stylized letter "B" decorating news stories about Bitcoin are just illustrations. Bitcoins exist entirely in a great general ledger called the *blockchain*, and bitcoin holdings at any point in time are nothing but the end result of a calculation

tracing all blockchain transactions since Bitcoin Day 1, early in 2009. This calculation associates each bitcoin position with a specific address, or "wallet." Each holder owns one or more wallets.

The Bitcoin network and blockchain have no central, authoritative record-keeper. Any time a bitcoin transaction occurs, the relevant data emanate throughout the Bitcoin peer-to-peer network from the transaction's point of origin to all users. The basic data for the transaction include the address (the wallet)



Just an artist's rendering. No coins exist.

of the sender, an address for the recipient, the number of bitcoins in the transaction, and authenticating information. The authentication, both of individual transactions and the blockchain, relies on data cryptography (hence the term "crypto-currency.") Each transaction record contains a digital signature derived from a password called a private key, which, hopefully, only the sender knows.<sup>3</sup> Encryption preserves the privacy of this key while authenticating the signature.

Using cryptographic techniques to validate transactions is clever, but the system also has to keep users from spending the same bitcoin several times. This is the most ingenious part of the design. Users — not a centralized party — validate transactions and commit them to the permanent general ledger, the blockchain. Users performing this function are bitcoin "miners." Any user with a suitable hardware rig, the right software, and willingness to pay for the power to run them can become a miner. As transactions occur and users broadcast them to the network, miners pick them up and assemble them into blocks. The miners verify the transactions by comparing them with the existing account (address) balances implicit in the blockchain history, and then apply a cryptographic algorithm in an effort to be first to create an encoding of a new block of transactions that meets a specific set of requirements. Cryptographers call this encoding a *hash*, and the encoding algorithm the *hash function*.

<sup>2</sup> Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" available at <https://bitcoin.org/bitcoin.pdf>. "Satoshi Nakamoto" is a pseudonym, and the true identity of "Satoshi" — whether an individual or a group — remains a closely-guarded secret. The paper looks like an academic working paper, such as a researcher might circulate professionally before submitting it for publication in an academic journal.

<sup>3</sup> A more complete description of bitcoin transactions is at <https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work>. The [Bitcoin Foundation's](https://bitcoin.org) site, [bitcoin.org](https://bitcoin.org), also gives a good deal of background.



Running the hash function isn't very hard, so the Bitcoin protocol adds a "proof of work" test to increase the effort the miners have to expend. To validate a block, the encoding must meet an arbitrary format requirement — it has to start with a minimum number of zeroes. The raw data of the block won't produce that result, so miners have to find a string of nonsense data, called a *nonce*, which, when added to the block, yields a hash meeting this requirement. The only practical way to generate this result is by the brute-force method of guessing a nonce, calculating the encoding, seeing whether it works, and if not, going back and guessing another one. This is the "complex mathematical puzzle" news reports sometimes say miners must solve.<sup>4</sup>

creasing the reward as the total number of bitcoins accumulates. It will fall to zero when about 21 million bitcoins exist, after which miners would have to rely entirely on transaction fees, or stop mining.

By design, the average time interval between successive blocks is about ten minutes. As miners apply more computing power, they verify blocks more quickly. If successes become too frequent, the protocol increases the number of initial zeroes required for a valid hash, increasing the difficulty of mining.

A miner's broadcasting a solution for a block doesn't necessarily close the book on those transactions. The network as a whole — actually, as a collection of individuals — has to accept the mined block, and hence the newly-extended blockchain, as valid. A miner accepts a new block by beginning to work on the next one. The basic rule is that the longest existing version of the blockchain is the "real" one, but if enough miners chose to treat a block as invalid, they could go back and rework it, and then overtake the previous version of the blockchain by successfully solving the next block. For that reason, Bitcoin advocates sometimes caution users to wait for several blocks to pass before regarding their transactions as irrevocably recorded.



Eventually, a miner will hit on a nonce that produces the required encoding. That miner broadcasts the result to the network, adding the newly mined block to the end of the blockchain. The successful miner receives a bounty, or reward — the privilege of beginning the next block with a transaction awarding itself a specified number of newly created bitcoins, along with any fees that users have offered miners to prioritize their transactions. (Miners do not try to validate all outstanding transactions at once, because the computing power and time necessary to calculate a hash for a block increase with its size. Bitcoin traders offer fees to induce miners to prioritize their transactions.) Currently, the bounty stands at 6.25 bitcoins, worth around \$250,000 at prices exchanges<sup>5</sup> are quoting. The Bitcoin protocol includes a schedule de-

Bitcoin and other cryptocurrencies embody a number of interesting, innovative concepts and technologies. Even so, many of the issues that are likely to arise if cryptocurrencies become permanent features of our economic landscape are more familiar and prosaic, and economic history provides analogies that provide insights as to how that might unfold.

## Historical Lesson 1. Re-intermediation.

Authenticating and processing direct bitcoin transactions — transfers recorded definitively on the blockchain — is inefficient, slow, and expensive. According to data from Coindesk, a cryptocurrency data and information service,

---

<sup>4</sup> If we think of the hash as an essentially random string of zeroes and ones, then each bit has a 50-50 chance of being a zero. If the solution requires 20 leading zeroes in its hexadecimal (base 16) representation, for instance, then on average the proof-of-work would require  $2^{80} = 1.2$  septillion ( $1.2 \times 10^{24}$ ) trials.

<sup>5</sup> Bitcoins, of course, aren't convertible into conventional currency unless someone is willing to trade one for the other. Quoted prices vary rather widely. The price is also quite volatile, so this estimate will undoubtedly be wrong in a short time. For this note, I am using a price of \$40,000, a level reasonably typical for much of 2021.





the blockchain records around 250,000 bitcoin transactions per day. Bitcoin miners add one block about every ten minutes, or about 144 blocks per day, to the chain. If the miner processing each of those 144 blocks receives about \$250,000 worth of new bitcoins, the Bitcoin community pays miners, on average, \$144 (in bitcoin) per transaction. All bitcoin owners bear this cost whether they trade or not.

Transaction fees and trading volumes vary widely. According to Coindesk, bitcoin transaction fees in the second half of May 2021 averaged perhaps \$17 to \$22 per transaction, but by mid-June the average fee had fallen into single digits. Figures for the average daily dollar value of transactions range from about \$5.5 billion to perhaps \$19 billion. Based on 200,000 to 250,000 transactions per day, the average on-blockchain bitcoin transaction size is on the order of 1 bitcoin. A \$5 fee, plus a \$144 dilution effect, on a trade worth \$40-50,000 is only about 0.3%, so commercial traders may regard bitcoin trading as cheap. Visa, MasterCard, American Express, and Discover charge fees several times higher on many of the 100 million or so transactions they handle daily. But while the Bitcoin protocol permits units as small as 1/100 millionth of a coin, trading costs are prohibitive for retail trades, and the network's processing capacity is far too small for retail volumes.

The metaphor that Bitcoin is digital gold invites study of a gold-based economy for hints about how a Bitcoin economy might work. In US history, probably the best approximation of a purely gold-based system was Gold Rush California. The gold dust the California miners produced, like Bitcoin, did not rely on a trusted intermediary for its value and transferability. But, also like Bitcoin, gold dust — heaps of flakes of metallic gold, mixed with sand and earth, and sometimes alloyed with other metals — was not money. Like cryptocurrency holders today, miners faced the vexing and costly problem of transmuting their dust into money.<sup>6</sup>

Gold miners had an important advantage over their crypto-counterparts. Congress had connected gold to money by defining the US dollar in terms of gold, at approximately \$20.67 per ounce. Anyone holding physical gold could convert it into money by sending it for coinage, but only through a trusted intermediary, the Mint. Before the branch Mint in San Francisco opened in 1854, coining California gold meant sending it to Philadelphia.

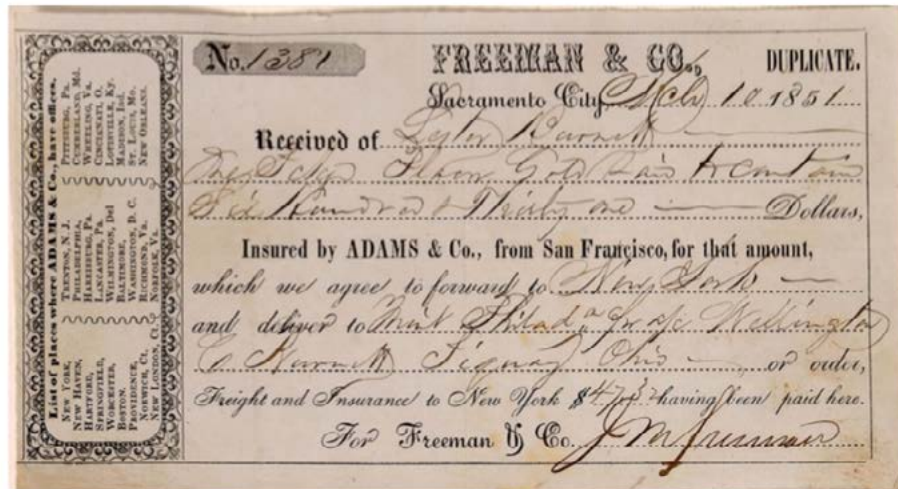
On March 10, 1851, a Lester Burnett send a package containing, he declared, \$631 worth of gold dust to the Mint in Philadelphia through Freeman & Co., an express shipper in Sacramento. Freeman, in turn, consigned the package to Adams & Co. in San Francisco. Burnett paid \$47.32, 7.5% of his declared value, for freight and insurance to New York. The Mint was to credit the coin they produced to the account of Wellington C. Burnett of Piquay, Ohio. We do not know Burnett's actual Mint return on his dust. He may have

understated its value to save on insurance, or he may have overestimated it.

understated its value to save on insurance, or he may have overestimated it.

Holders of gold dust had two other choices broadly resembling those available to holders of bitcoin. They could use their dust as direct payment in ordinary commerce, or they could sell it for cash. Either choice required a willing counterparty. Transaction costs and delays impede the use of cryptocurrencies for direct payments. Gold dust presented a different problem. Merchants kept sets of scales for weighing dust that miners presented for payment, but the weight of the dust was only one factor in its value. Its purity, which was harder to determine, also mattered.

The only reliable way to evaluate the purity of gold dust was by physical assay. Like bitcoin mining, this process was cost-effective for large quantities, but too slow and expensive for everyday transactions. The practical result



Receipt for shipment of gold dust from Lester Burnett to the Mint at Philadelphia, March 10, 1851. (Author's personal collection.)

<sup>6</sup> I make this point in "Discounting gold: Money and Banking in Gold Rush California," Case Study #22 for the Global History of Capitalism Project, Oxford Centre for Global History, University of Oxford, April 2021. Freely accessible at <https://globalcapitalism.web.ox.ac.uk/discounting-gold-money-and-banking-gold-rush-california>



## Lesson 2. Substitute Instruments.

was that in everyday commerce, all but the most obviously contaminated gold dust passed from hand to hand at a standard price. Holders of dust naturally tried to use their poorer dust for everyday purposes, and save their better dust for the Mint. This adverse selection tended to depress that standard price, although competition among merchants and bankers tended to support it.

Because sending dust back east was so expensive, many miners sold theirs to bankers and dealers in California. These intermediaries aggregated quantities large enough to support the cost of assay and to allow them to negotiate favorable rates for freight and insurance on gold they shipped east. The cost structure of blockchain transactions similarly favors large traders, so small holders rely on cryptocurrency exchanges and other intermediaries — supposedly anathema in the crypto-economy — to perform the alchemy of turning money into cryptocurrency and back again.

Cryptocurrency transactions through intermediaries can take several forms. First, the exchange might act as dealer, trading cryptocurrency for cash, facilitating the customer's interaction with the blockchain, and perhaps taking custody of the customer's cash and cryptocurrency wallet. In this scenario, the customer bears the full brunt of the delay, dilution, and fees associated with the blockchain.

In the second model, the exchange holds bitcoin wallets on behalf of its customers, like securities brokers holding stocks in "street name." Customers wishing to sell their holdings post offers, and prospective buyers post bids. The exchange matches buyers and sellers, clearing trades by transferring specific bitcoin wallets from sellers' accounts to buyers' on the exchange's books. This keeps the transactions off the blockchain, sparing customers the associated costs and delays, but it requires both sellers and buyers to accept the exchange as a trusted intermediary, and pay its fees.

The third possibility is a banking model, in which customers hold bitcoin-denominated claims against the exchange's master, or "house" account. Cryptocurrency trades then become transactions between customers and the custodian, and customer holdings are obligations of the exchange, like bank accounts. The exchange can pool external activity into larger transactions. As efficient as it is, this setup muddies the determination of the prices for converting money into cryptocurrency and back.

Economies with money as clumsy and costly as Bitcoin often facilitate commerce by developing substitute instruments, documents representing claims for payment in the underlying money. California history provides an example here too, this one from the decades prior to the Gold Rush. California was then primarily agrarian. Crop production mostly took place at the string of 21 Franciscan Missions extending from San Diego to Sonoma. A second group of large properties were the *ranchos*, land grants of various sizes, most commonly about 55 square miles. The *rancheros* raised cattle, primarily for their hides and tallow (rendered fat, for making products like soap and candles). In the 1830s and 40s a number of American merchants in California (still part of Mexico) plied the "fat and skins trade," brokering the sale of tallow and hides to Yankee traders, who came around Cape Horn from New England. The New Englanders sometimes bought for cash, but they mostly traded eastern manufactured goods in demand in California.<sup>7</sup>



"Hide Droghing", illustration from *Two Years Before the Mast*.  
Source: [https://en.wikipedia.org/wiki/California\\_hide\\_trade#/media/File:Hide\\_Droughing.jpg](https://en.wikipedia.org/wiki/California_hide_trade#/media/File:Hide_Droughing.jpg)

---

<sup>7</sup> This is the trade that Richard Henry Dana, Jr. described in his 1840 classic, *Two Years Before the Mast*.





Cash was chronically in short supply in California, and processed cattle hides emerged as a form of *ersatz* currency — Californians sometimes facetiously called them “California bank notes.” Hides were workable as money because they were durable, reasonably uniform, and had a steady end market with the Yankee traders, so Californians could expect to trade them for cash or other items of value.



William A Leidesdorff

Hides also had important deficiencies as money. They were not exactly portable. Merchants could transport them from one place to another, but moving them was a laborious operation. They also were not divisible. Merchants dealt in integer quantities, often crediting hides to one another at a value of \$2.

California’s economy grew and became more complex with increasing settlement in the 1840s. Yet cash remained scarce, and hides remained a cumbersome form of money. In the years just prior to the Gold Rush, California merchants did much of their business with one another on account, not making actual payments in either cash or cattle hides (corresponding to on-blockchain transactions) until the opportunity presented itself.

My case study on William A Leidesdorff, one of the leading merchants of pre-Gold Rush San Francisco,<sup>8</sup> highlights two examples. In one, a merchant named A. B. Thompson drew a check, payable in cattle hides to a James Watson, on Leidesdorff.<sup>9</sup> Watson endorsed the check to a third party, a Captain Clapp, to whom Leidesdorff delivered the hides. Clapp presumably bought them from Watson to take them to New England. The single instrument (Thompson’s check) mediated adjustments of Leidesdorff’s balance with Thompson, Thompson’s balance with Watson, and Watson’s sale of the hides to Clapp, with just one physical delivery. In the crypto-economy, the analogy would be a chain of three transactions, only one of which took place on the blockchain.

Leidesdorff also maintained an extensive trade relationship with another San Francisco merchant, Henry Mellus. They kept detailed accounts, but only rarely settled up. An opportunity to make some settlement arose in October 1846 when Leidesdorff received bills of exchange from the Russian-American Company for the sale of supplies for the company’s fur-trading post in what is now Sitka, Alaska, and possibly other services. These bills were presumably payable in St Petersburg or London, but Mellus accepted them from Leidesdorff – at a 12½% discount.<sup>10</sup> He likely sent them to his bankers in Boston, who negotiated or collected on them. Leidesdorff and Mellus relied on each other’s credit, in effect creating additional money, to expand their trading capacity beyond what the cash in the economy could support.

Like their 1840s counterparts, participants in the crypto-economy have developed a variety of ways to make small transactions without the delay and overhead of committing their activity to the blockchain. One strategy involves derivative substitutes, such as exchange-traded notes, swaps, futures, and options.

One heavily-advertised Bitcoin-related product is the Greyscale Bitcoin Trust.<sup>11</sup> Although it resembles an exchange-traded fund, it is not a registered investment company at all. Investors buy fractional undivided interests in the Trust’s holdings of bitcoin. Its disclosures carefully, and accurately, say it seeks returns associated with movements in the dollar price of bitcoin, acknowledging that it may or may not achieve its objective. To date the approximation has been weak, since the Trust has no market mechanism tying its share price to the value of its holdings. Television advertising for the Trust avoids making any investment claim beyond providing “Bitcoin exposure.” Instead, one set of commercials alternates between a fanciful action-thriller scenario and a four-person videoconference call. When one conferee inserts himself into the scenario, declaring, “I love Bitcoin!” the protagonist objects archly, “This is *my* fantasy!”

---

<sup>8</sup> I describe the use of cattle hides as money in California, and the arrangements merchants made with one another, in more detail in “Money, Cattle Hides, and William A Leidesdorff: California before the Gold Rush,” Case Study #19 for the Global History of Capitalism Project, Oxford Centre for Global History, University of Oxford, August 2020. Freely available at <https://globalcapitalism.history.ox.ac.uk/files/case19-cattlehidespdf>.

<sup>9</sup> Check payable in hides, dated Monterey, June 24, 1843. William A Leidesdorff Collection, 1834–57, 1928, MS1277, California Historical Society, Manuscript Collection, San Francisco.

<sup>10</sup> “Mr. William A Leidesdorff in Acct Current with Henry Mellus,” October 30, 1846. Leidesdorff Collection.

<sup>11</sup> See, for example, the [Greyscale Bitcoin Trust Annual Report](#) on form 10-K for 2020.



Another product's advertising depicts non-investment situations in which a prudently hesitant person misses out on large benefits that arise ludicrously quickly. The metaphor this product's promoters want viewers to see may lie in something other than the absurdity of the scenarios.

Bitcoin proponents often claim that because of the hard cap on the number of bitcoins the protocol will create, the cryptocurrency is inflation-proof. But a number of entities offer the ability to borrow and lend cryptocurrencies, or to borrow and lend money against cryptocurrencies as collateral. If the crypto-economy develops further, the use of cryptocurrency-denominated claims in lieu of the tokens themselves would most likely expand. This expansion of credit, just as with conventional money, would expand the effective supply of cryptocurrency, even if the number of actual tokens remained fixed.

### Lesson 3. Concentration of Economic Power.

Since no government is part of the creation of cryptocurrencies, proponents argue that they are more decentralized than money, somehow democratizing commerce. But because of the capital-intensiveness of Bitcoin mining and the network economics of cryptocurrency exchanges, the opposite is true. The Bitcoin protocol sets the difficulty its proof-of-work mining task based on the total computing power devoted to mining. The first miner to validate each block by completing this brute-force, trial-and-error task earns the reward for that block. The more trials a miner can complete, the greater the miner's odds of success. This makes mining a lottery, in which each participant's chance of winning is proportional to its capacity to complete trials – its computing power. This gives the advantage to enterprises with the capital necessary to build and operate larger installations.

Some cryptocurrencies, in part reflecting concerns over the energy-intensiveness of Bitcoin mining, substitute a “proof-of-stake” concept for Bitcoin's “proof-of-work.” Proof-of-stake validation replaces the lottery based on computing capacity with one based on the participants' ownership of the token – creating an advantage for the largest owners.

Network effects are likely to confer advantages to the largest crypto-exchanges. If cryptocurrencies gain in importance, economic power in the sector is likely to become concentrated in a small number of hands – the largest miners in proof-of-work

tokens, the largest owners of proof-of-stake tokens, and the largest exchanges. History again provides a metaphor illustrating how this concentration might evolve.

In 1741, Vitus Bering, a Danish explorer in the service of Russia, left the port of Petropavlovsk in the Russian Far East with two ships on what we now call the Great Northern Expedition, aiming to discover and map the lands to the east of the Kamchatka Peninsula. Bering and his companion, Aleksei Chirikov, became separated in fog. Bering's ship wrecked on the island east of Kamchatka that bears his name, and Bering himself perished there. Chirikov returned safely after visiting Alaska, most likely the Panhandle. Along with information about the lands he discovered, Chirikov and his crew brought back a cargo of 900 sea otter skins.<sup>12</sup>

Sea otter – the sleekest, richest, blackest, and most highly prized (and valuable) of all furs – commanded high prices at market in China. Chirikov's haul set off a fur rush among the merchants and trappers of Siberia. For the next several decades, private expeditions from Kamchatka, and later from the port of Okhotsk, sailed to the east to trap and trade for furs. At first these were modest affairs. An enterprising trapper would form an alliance with a merchant, who would



raise capital to build and equip a ship. Meanwhile, the fur trapper would hire a navigator and recruit other trappers to sail the ship. In the early years, they could hope to sail the short distance from Kamchatka to nearby Bering or Medny (Copper) Island, spend the winter trapping, and bring home a valuable cargo of furs.

<sup>12</sup> This and other descriptions of the Russians' progress along the Aleutians are from Berkh, Vasilii Nikolaevich, Author. Хронологическая история открытия Алеутских островов или подвиги Российскаго Купечества. (Chronological history of the discovery of the Aleutian Islands, or Feats of the Russian Merchants) 1823. Pdf. <https://www.loc.gov/item/2018694164/>.





As over-hunting depleted the furs on the nearest islands, the trappers ventured farther east. Their voyages became longer, spanning multiple winters. By the 1780s, these Russians were trapping in the eastern Aleutians and Kodiak Island, near the Alaskan mainland. There they encountered substantial native populations, with whom they competed for furs in their hunting grounds. The multi-year voyages, traversing greater distances and meeting increased resistance from Alaskan natives, required larger ships, larger crews, and more capital. By 1790 two companies had established settlements in Alaska, requiring still more capital. In a half-century, the Russian maritime fur industry changed from a collection of small, independent entrepreneurs with modest capital, to a capital-intensive industry dominated by just two firms.

In 1799, a decade of political maneuvering by the head of one of the two remaining firms, Grigoriy Shelekhov, and direct lobbying at Court by his son-in-law, Nikolai Rezanov, bore fruit when Emperor Paul I, son and successor of Catherine the Great, granted Shelekhov's company a charter as the Russian-American Company. This charter gave the Company a protected monopoly (putting Shelekhov's remaining competitor out of business), along with Imperial patronage and protection. The Tsar and other high officials at Court later became shareholders.

The same progression – starting with thinly-capitalized freelancers, but with increasing capital intensity driving concentration, perhaps ultimately leading to a state monopoly and takeover of the industry – may befall cryptocurrencies. At first, bitcoin mining required only modest capital, but increased competition has required escalating quantities of computing power – and capital. Mining has accordingly become increasingly concentrated. According to various reports last year, some 65% of all Bitcoin mining activity was in China, with about half of that concentrated in one region.<sup>13</sup> A state crackdown has since driven many miners out of China.

Among the crypto-cognoscenti, one fear that mining concentration raises is that some malicious actor with sufficient computing power might hijack the blockchain. While that is possible in principle, the bigger issue is that a small number of actors may extract the bulk of whatever economic benefits cryptocurrencies deliver. This is another reality antithetical to the romantic ideal of decentralization and democratization. And if a large fraction of the computing power going into bitcoin mining again concentrates in one country, a state takeover in the fashion of the Russian-American Company is not outside the realm of possibility.

## Lesson 4. There will be (and probably have been) Swindles.

Where innovations introduce potential new sources of value, the best ways of realizing that value are often unclear at first. Ventures arise. Some are legitimate speculations – successful or not – but many prove to be swindles. Often-times the swindlers target investors who are remote, either geographically or conceptually, from the source of value, and appeal to them with conjuring words that have taken hold in the public imagination, and, if possible, star power.

For an idea of the shape that cryptocurrency swindles might take, we look again to that age of swindlers, the California Gold Rush. Two examples are particularly instructive. One was a straight-up fraud involving forgeries of paper instruments that substituted for money, and the other was a series of stock-promotion schemes selling shares in dubious enterprises. The examples do not resemble specific recent or current events, but they hint at the types of scams and schemes that could arise in the crypto-world.

The first example is the story of Henry “Honest Harry” Meiggs. Born in 1811, Meiggs came to California from New York in 1849 with a load of lumber, and he soon established himself as a leading lumber dealer. He built mills in San Francisco and at Mendocino (then called Meiggstown), well north of the city on the Pacific Coast. He enjoyed a sterling personal reputation, which he monetized in an unusual way.



California Lumber Manufacturing Co. share certificate issued to and by Henry Meiggs, March 21, 1853 (Author's personal collection.)

<sup>13</sup> Jeffrey Gogo, “65% of Global Bitcoin Hashrate Concentrated in China,” bitcoin.com, May 7, 2020.





In the Gold Rush years, the City of San Francisco paid many of its expenses by issuing scrip, called Comptroller's warrants. These circulated locally, generally trading at about 75% of their face value. In 1854 business conditions deteriorated, the price of lumber collapsed, and Meiggs found himself in trouble. Over several weeks, he borrowed somewhere between \$250,000 and \$500,000 from a wide variety of lenders, from bankers to individuals. For collateral he offered his own good name, plus City Comptroller's warrants, generally posting \$2 in warrants for each dollar he borrowed.

On October 6, Meiggs lodged a letter with his principal creditors, confessing a judgment of \$200,000, against which they attached much of his property. Several days later Meiggs, along with his brother John – the City Comptroller – and their families, boarded a ship carrying a substantial quantity of gold and cleared for "Ports in the Pacific." When Meiggs's absquatulation came to light, his creditors tried to collect on their collateral, but the warrants Meiggs had posted were all forgeries. Meiggs had also borrowed against shares of his lumber company, which he had over-issued to himself for the purpose.

Honest Harry never returned to California. He was reported seen in Tahiti that November, after which he traveled to South America, where he made a name building railroads in Chile and Peru.

The Gold Rush also saw its share of stock-promotion schemes. In 1850, a San Francisco banker named Joseph C. Palmer began promoting a series of stock issues that played on the excitement the Gold Rush created outside California. Palmer was not a conventional banker, dealing in gold dust and remittances to the east. Instead, he dealt in land speculation and politics. One of Palmer's most important political connections was John C. Frémont, who earned fame in the 1830s and 1840s as The Pathfinder for his explorations of routes across the Rocky Mountains, and became one of California's first US Senators in 1850.

On November 10, 1851, Frémont leased to a group of Philadelphia investors, including newspaper publisher Solomon Alter, mining rights to two veins of gold-bearing quartz on his property at Mariposa, near what is now the entrance to Yosemite National Park.<sup>14</sup> The deal had everything: star power, technology, and best of all, gold.

The technology portion of the deal involved recovering gold from quartz. Miners pulverized the quartz rock, added water to create a slurry, and passed this slurry through an amalgamator – basically a pan with quicksilver, liquid mercury metal – in the bottom. The mercury and gold formed a natural alloy called an amalgam. To recover the gold, they heated this amalgam in a retort, boiling off the mercury and leaving behind the gold.

In the early Gold Rush years, California prospectors did not bother with quartz mining, because working the placers – alluvial deposits in rivers and streambeds – was much easier. But investors in Philadelphia did not necessarily know that. And if Philadelphia suited Palmer's purposes, London served even better. On October 2, 1851, Palmer launched the Agua Fria Gold Mining Company, "For working the Agua Fria mine, on the Agua Fria River, Mariposa District, California, U.S. (Under Lease to Messrs. PALMER, COOK & Co., Bankers, St. Francisco, from the Hon J.C. FREMONT...)"<sup>15</sup>, making the necessary filings with the Registrar of Companies in London. The prospectus waxed eloquent about the richness of the lode on the property. Palmer had also made sure that Mariposa, Frémont, and quartz were all effective conjuring terms for investors in London.



Share certificate of the ironically-named Quartz Reduction Company, successor to the Agua Fria company. It went into voluntary liquidation in 1859.

14 "A Section of Las Mariposas: a tract of land granted by General Micheltorena, etc." Map 452, California Historical Society, San Francisco.

15 "The Agua Fria Gold Mining Company," Photostat copy of prospectus, Bancroft Folio f F862.3.A35.phot., Bancroft Library, UC Berkeley, 1851.



The Agua Fria company raised £66,387 from share sales, and granted Palmer and his partners one-third of its 100,000 shares of £1 each. The company paid Palmer and Cook an additional £6000 in fees, and they appear to have sold nearly 25,000 of their 33,333 shares. The company did actually produce some gold – about £6200 worth. But that was never the point.

By 1854, enthusiasm in London for California quartz mining companies was on the wane. A London correspondent of the San Francisco *Alta California* newspaper wrote in a letter that appeared on April 16, 1854, “Most of these companies were originally based on leases obtained by divers persons from Col. Fremont’s agents....The mining, however, it turns out, has been principally done in the London Stock Exchange, instead of in the ‘diggings.’”<sup>16</sup>

Not every paper instrument in Gold Rush California was forged, and not every venture was fraudulent. Nor is every cryptocurrency-related instrument or enterprise. But speculators in cryptocurrencies and investors in cryptocurrency-related ventures should be wary. The great Gold Rush swindles show that the further removed an instrument or enterprise is from the core activity to which it pertains, the greater its scope for fraud. Physical distance does not mean as much today as in the 1850s. But conceptual distance does. The more steps intervening between the blockchain and any particular cryptocurrency investment, the greater the scrutiny that investors should apply.

## Conclusion.

As novel as Bitcoin and other cryptocurrencies are, history nevertheless has lessons for how the crypto-economy could unfold. Bitcoin advocates urge that bitcoin transactions require no trusted intermediary, but cryptocurrencies cannot become useful in broader commerce without some re-intermediation. If applications of cryptocurrency expand, so will the array of substitute instruments, representing crypto-denominated claims. If the crypto-economy grows, so will the capital necessary to compete in the marketplace. As the capital requirement increases, so will the concentration of economic power, another development antithetical to the romantic ideal of cryptocurrencies. And finally, as the market develops and becomes more complex, some, although by no means all, of the new developments will be scams and swindles.

As clever as the idea behind Bitcoin is, as much attention as cryptocurrencies have garnered, and as many resources as promoters and investors have devoted to the crypto-economy, for ordinary investors the best attitude toward cryptocurrencies is still one of caution. The marketplace for them will almost surely produce responses and problems that are only too familiar from history.

— Jonathan Tiemann  
Menlo Park, California  
October 29, 2021

Tiemann Investment Advisors, LLC is an SEC-registered investment advisor based in Menlo Park, California. For more information, please send your request to: [information@tiemann.net](mailto:information@tiemann.net) or visit [www.tiemann.net](http://www.tiemann.net).

---

<sup>16</sup> “London Correspondence,” *Alta California*, April 16, 1854.