Texas Appleseed Written Testimony
Pensions, Investments, and Financial Services Committee

August 25, 2022

Submitted by Ann Baddour, Director, Fair Financial Services Project

Chair Anchia, Vice Chair Parker, and Committee Members:

Thank you for this opportunity to submit written testimony regarding blockchain and virtual currency, often called cryptocurrency. We are in an era of unprecedented technological and financial developments and, therefore, believe it is paramount to stay up-to-date with industry developments to ensure consumer protection throughout the whole process. Blockchain and cryptocurrency have qualities that may ultimately improve financial transactions, but there are systemic problems that must be addressed.

Texas Appleseed is a public interest justice center working to build policies that enhance the ability of Texans to achieve their full potential. In partnership with pro bono partners and collaborators, we develop and advocate for innovative and practical solutions to complex issues. As part of our work, Texas Appleseed also conducts data-driven research to better understand inequities and identify solutions for concrete, lasting change. We are part of a non-profit network of 17 justice centers in the United States and Mexico.

Enhancing Positive Economic Impacts and Sustainability of Cryptocurrency

Texas, which is home to approximately 40% of US cryptocurrency mining and numerous crypto enterprises, is playing an important role in this emerging sector.[1] This central role creates both an opportunity and an obligation for Texas to ensure that cryptocurrency is not just a big moneymaker for early adopters, hedge funds, and venture capitalists, but also benefits the many people attracted to its foundational ideals.

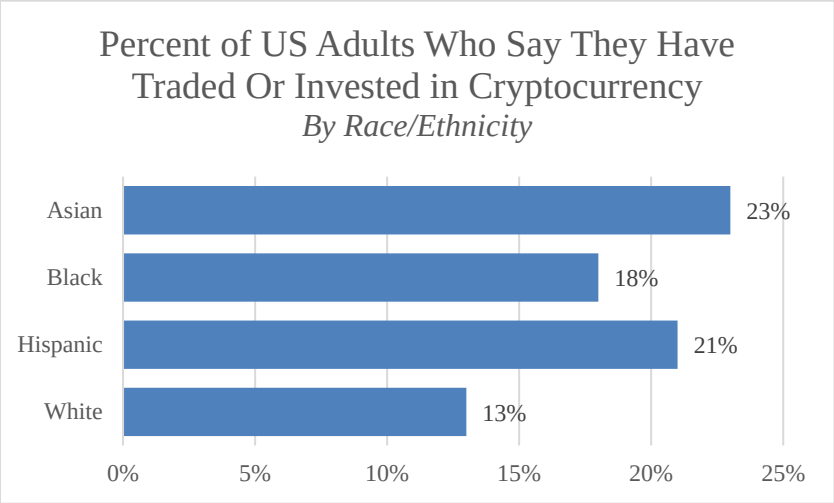
Bitcoin, the first cryptocurrency, came into being in the wake of the 2008 financial crisis and grew out of the failure of formal financial systems. It is often described as a system to replace formal banking,[2] removing intermediaries and building decentralized, permissionless, and censorship resistant systems in their place. These enticing goals, along with a spike in value and promises of high returns over the 5-year period leading up to the 2022 crash, attracted a growing base of investors.

Early adopters and large investors are the dominant force in cryptocurrency. An October, 2021

[1] Natalie Walters, "Here's why crypto companies are flocking to Texas," *The Dallas Morning News* (May 20,2022).
[2] Ian Thomas, "Crypto is not replacing the U.S. dollar, Bitfury CEO Brian Brooks says," *CNBC* (June 29, 2022).

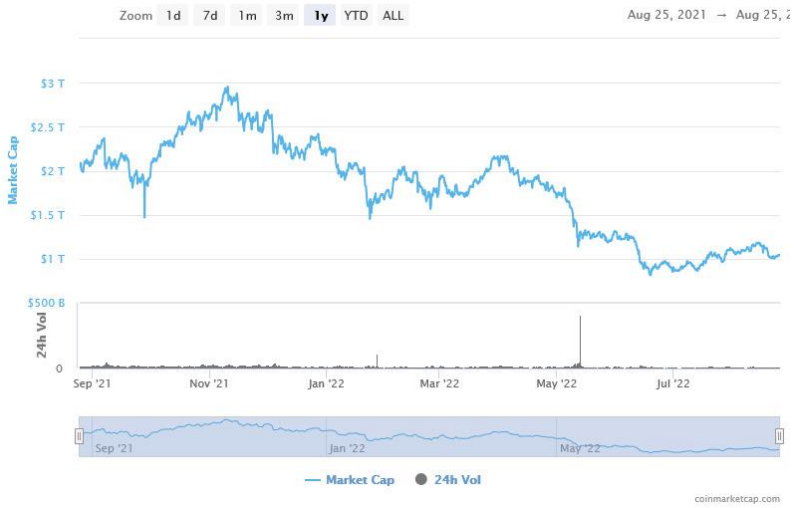
study by the National Bureau of Economic Research found that for bitcoin, the cryptocurrency with the largest market cap, the top .01% of bitcoin owners control 27% of the market.[3]

However, in terms of the number of investors, a Pew Research Center Survey from September of 2021 found that 16% of Americans said that they had invested or traded in cryptocurrency. Among lower income Americans, 15% had invested or traded in cryptocurrency. The study also found meaningful market engagement across race and ethnicity.



Source: Pew Research Center, 2021

Investment in cryptocurrency, from many US communities, grew during the pandemic period, from March of 2020 through early 2022. But, the recent crash has left many people empty-handed.[4] From a high of a nearly $3 trillion market cap, cryptocurrencies have fallen to just over $1 trillion, a nearly $2 trillion loss in value.



[3] Igor Makarov and Antoinette Schoar, "Blockchain Analysis of the Bitcoin Market," *National Bureau of Economic Research*, at 6 (October, 2021) and Khristopher J. Brooks, "Bitcoin has it's own 1% who control outsized share of wealth," *CBS News Money Watch (*December, 21, 2021).

[4] David Yaffey-Bellany, "Crypto Crash Widens a Divide: 'Those With Money Will End Up Being Fine'," *The New York Times* (June 29,2022).

The factors that drove the crypto market crash, as well as previous major losses in the crypto space, form the basis of a roadmap for user protections that are necessary in this market. Consumer protections are necessary for cryptocurrency to have potential to be a positive economic force for all Texans.

Consumer Protection Problems Undermining Benefits and Viability of the Current Market

Though not exhaustive, the list below highlights notable harmful practices in the current market. Efforts to encourage or expand blockchain and cryptocurrency in Texas should prioritize solutions to these systemic and broadly impactful issues.

1. There are Currently No Standards or Systematic Oversight for Cryptocurrency Lenders, Brokers, and Exchanges

The lack of oversight and standards are major contributors to the current market collapse. The collapse was exacerbated by the crash of the TerraUSD algorithmic stablecoin and its sister token, Luna. Once the stablecoin lost its peg to the US dollar, both Terra and the Luna coin saw a dramatic fall in value causing a loss of $40 billion in market value.[5] Cascading effects of the crash led to losses of $500 billion in the broader crypto currency markets.[6] But, the damage did not stop there. Three Arrows Capital, a major crypto hedge fund that held heavily leveraged positions in Terra and Luna then collapsed and brought down with it other crypto platforms including two major crypto lenders, Celsius and Voyager, as they could no longer pay their obligations. All parties were overleveraged, and with little to no capital reserves backing up operations, the entire system collapsed.

a. Reckless investments and deceptive promises by cryptocurrency lenders and brokers

The low interest rate environment attracted retail investors to Celsius, a cryptocurrency lender and deposit holder, promising annual rates of return near 20% and asserting that funds would be safe. Retail investors were deceived by these assertions of safety.[7] Celsius engaged in reckless investments of borrower and depositor assets, including making loans to Three Arrows Capital, among other risky ventures. In the wake of the Three Arrows Capital collapse, Celsius also collapsed, leading to a run on deposits reminiscent of 1929.

Celsius froze withdrawals and declared bankruptcy. 1.7 million customers are now forced to engage in the bankruptcy process to try to reclaim some of their funds, with the court docket full of desperate letters from depositors hoping to get at least some of their life savings back.[8] Celsius went from $25 billion in assets under management to $167 million in cash on hand.[9] People lost their life savings, because of the lack of standards and accountability in the market.[10] To add insult to injury, it appears that creditors will be paid before retail customers, likely leaving little to no assets to reimburse them for significant losses.[11]

---

[5] "South Korean founder of failed Terra Luna coin admits he was wrong," *Channel News Asia* (August 17, 2022).
[6] *Id.*
[7] Hailey Lennon, "Bankrupt Crypto Lender, Celsius Could Leave Customers Last In Line to Get Paid," *Forbes* August 1, 2022)
[8] See https://cases.stretto.com/Celsius/court-docket/#search.
[9] MacKenzie Sigalos, "From $25 billion to $167 million: How a major crypto lender collapsed and dragged many investors down with it," *CNBC* (July 18, 2022),
[10] Jacob Carpenter, "Elderly widows, paycheck-to-paycheck families, and stressed caregivers lost their life savings to Celsius' crypto collapse. Their voices deserve to be heard," *Fortune* (August 4, 2022).
[11] *Id.*

Similar to Celsius, Voyager, another creditor of Three Arrows Capital, declared bankruptcy as a result of the risky use of assets provided by depositors who understood their money to be safe. Voyager enticed customers with high returns combined with false assertions on its website and in other platforms that deposits were FDIC insured. On July 28 of this year, the Federal Reserve and FDIC issued a cease-and-desist letter.[12] However, the action came too late for the 3.5 million people holding assets at Voyager. The Dallas Mavericks, who entered into a 5-year agreement with Voyager in 2021, along with owner, Mark Cuban, are currently being sued in a class action lawsuit as part of an effort to try to recoup funds for Voyager customers.[13]

b. Insider trading and other market manipulation on cryptocurrency exchanges

In addition to major problems with crypto lenders and brokers, crypto exchanges have been plagued with numerous indications of insider trading and other anti-competitive and deceptive practices. A recent study found that between 10% and 25% of Coinbase coin listings since 2018 showed signs of insider trading.[14] The study found that, through use of decentralized exchanges without know your customer or anti-money laundering standards, insider traders could purchase new coins before the official release on Coinbase and profit from the initial boost in the coin price.[15] Insider trading was also found to be widespread on Binance, the largest cryptocurrency exchange.[16]

Pump and dump schemes and "rug pulls" are all too common on both centralized and decentralized exchanges. They can be associated with initial coin offerings or coordinated efforts to artificially boost the pricing of existing coins. Around $2.8 billion was lost to these schemes by crypto investors in 2021.[17] A well-known example is the SQUID coin, based on the popular Squid Game show, that shot up in value then was dumped by the creators, leading to a $3 million loss for those who invested.[18] A study published in July found that pump and dump schemes are common and detrimental to people participating in the exchanges. Exchanges can address these risks through creating strict rules and consequences for taking part in market manipulation.[19]

Traditional trading markets are not perfect but have laws in place to address many of these points of deception and exploitation. Without more accountability, oversight, and standards, cryptocurrency lenders, brokers, and exchanges will continue to pose a major risk for retail customers and potentially could evolve to create systemic risks for our financial system and economy.

---

[12] Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation, "FDIC and Federal Reserve Board issue letter demanding Voyager Digital cease and desist from making false or misleading representations of deposit insurance status," (July 28,2022). On August 19, 2022, the FDIC issued five additional cease and desist letters to crypto businesses falsely claiming FDIC insurance. See: https://www.fdic.gov/news/press-releases/2022/pr22060.html.

[13] Natalie Walters, "Lawsuit accuses Dallas' Mark Cuban of duping investors with crypto 'Ponzi scheme'." *The Dallas Morning News* (August 11, 2022). Though not currently facing bankruptcy, Coinbase, a major crypto wallet holder and exchange recently announced to customers that their crypto assets held by Coinbase would be at risk in the event of a bankruptcy—an unwelcome surprise for people holding crytpo assets with Coinbase.

[14] Ester Félez-Viñas, Luke Johnson, and Talis J. Putnins, "Insider Trading in Cryptocurrency Markets," (August 8, 2022)

[15] *Id.* at 5-7.

[16] Ben Foldy and Caitlin Ostroff, "Crypto Might Have and Insider Trading Problem," *The Wall Street Journal* (May 21, 2022). It is interesting to note that information regarding where Binance, the worlds' largest cryptocurrency exchange, is headquartered is not readily available making accountability for illegal actions illusive.

[17] Lisa Ferber, "How Crypto Investors Can Avoid the Scam That Captured $2.8 Billion in 2021," *Next Advisor* in partnership with *TIME* (April 19, 2022).

[18] *Id.*

[19] Tao Li, Donghwa Shin, and Baolian Wang. "Cryptocurrency Pump-and-Dump Schemes," (July 18, 2022).

2. Blockchain and Cryptocurrencies Struggle with Structural and Coding Flaws

Though blockchain and cryptocurrency, which is built on blockchains, are generally perceived to be immutable and secure, coding and structural flaws can undermine that promise. Because of the high dollar amounts associated with cryptocurrency coupled with the lack of oversight or accountability, there are plenty of incentives for hackers and unethical coin creators to exploit weak points in the technology. Once funds are stolen, it is extremely difficult to retrieve them, despite transactions being public on the blockchain. Hackers can disappear through moving funds in ways that make them difficult to track.

a. 51% Attacks

The blockchain-based consensus mechanisms for cryptocurrencies allow for self-regulation but this protection is undermined by the 51% attack problem for coins that rely on proof of work.[20] If a person or group miners control 51% or more of the computing power to mine and process transactions on a cryptocurrency blockchain, they have the ability to block certain transactions from being recorded or completely reverse transactions to "double-spend" their tokens. One of the original purposes of blockchain technology was to reduce the "double-spending" problem where the same dollar is spent twice.[21]

The concentration of mining and mining pools elevates the risk of the 51% problem. A study of bitcoin mining found that the top 10% of miners control 90% of the mining capacity and the top .1% control 50% of the capacity, making bitcoin vulnerable to 51% attacks, particularly in times of sharp price decreases, when there is less overall mining capacity.[22]

b. Faulty Coding and Hacks Exploiting Structural Weaknesses in the Blockchain

Over the years, there have been countless debacles created through faulty coding, both intentional and not. Faulty coding has allowed hackers to exploit weak points to seize virtual currency. Several of these events have caused users of cryptocurrency to lose hundreds of millions of dollars. Some of the most notorious include when amateur developer devops99 discovered a bug in a crypto wallet and, in an attempt to make it right, deleted the bug in the code.[23] The bug was removed, but the result was permanently freezing $300 million worth of Ethereum, making it inaccessible.[24] In one of the most infamous Initial Coin Offerings, on the REX platform, the REX coin was coded with the wrong Javascript hex string resulting in $1.3 million being lost. Though venture capital dollars backing the scheme allowed them to make purchasers whole, the vulnerability created a debacle.[25] Recently, hackers exploited a bug in the Aural coin, an algorithmic stablecoin associated with the

---

[20] Jake Frankenfield, *51% Attack*, Investopedia (Apr. 27, 2022), https://www.investopedia.com/terms/1/51-attack.asp#:~:text=A%2051%25%20 attack%20is%20an,other%20 miners%20from%20completing%20 blocks. Proof of work means that transactions added to the blockchain must be verified by computing power used to solve complex mathematical equations, as part of the cryptographic structure. The proof of work model enables the consensus mechanism on the blockchain. Proof of stake is another structure based on staking of value as a way to ensure transactions are legitimate.

[21] Jake Frankenfield, *Double-Spending*, Investopedia (Jan. 7, 2022) https://www.investopedia.com/terms/d/doublespending.asp#:~:text=Double%2Dspending%20is%20the%20 risk,alteration%20can%20 reclaim%20 spent%20coins.

[22] Supra note 3 at 4.

[23] Fabio Lugano, *Famous programming errors in the crypto world*, Cryptonomist (Dec. 8, 2018), https://en.cryptonomist.ch/2018/12/08/programming-errors-crypto-world/.

[24] David Hamilton, "The Biggest Crypto Programming Errors of All Time," CoinCentral (Oct. 9, 2018).

[25] *Id.*

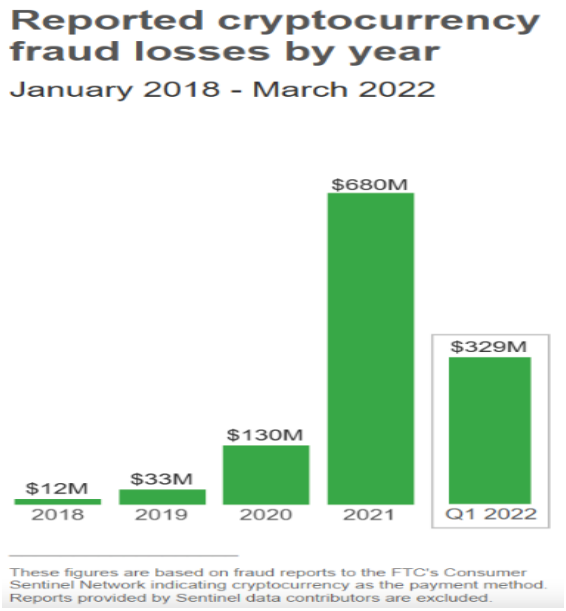
Polkadot protocol and minted $1.3 billion in new coins with no collateral backing causing the coin value to plunge by 99%.[26]

In early August, a hacker was able to obtain the personal keys of over 7,000 internet-connected wallets in the Solana ecosystem. Those impacted lost nearly $8 million.[27] In a different, but very damaging attack, a hacker used the governance protocol of Beanstalk, a decentralized finance protocol built on Etherium, to approve the execution of code to transfer $182 million of value to their wallet. The governance protocol allows a majority vote to change the code. The hacker used a flash loan to purchase a 67% share in Beanstalk, executed the code change, repaid the flash loan, and pocketed the remaining $80 million. Everything happened in a total of 13 seconds.[28] The hacker then moved the coins to a cryptocurrency mixer and so they are nearly impossible to trace.

These are just some examples to illustrate underlying security and trust risks that must be addressed or where a system of accountability must be created to mitigate these kinds of attacks that leave retail investors empty-handed.

3. Cryptocurrency Is Becoming a Common Method For Scammers to Get People's Money

In June of 2022, the Federal Trade Commission issued a bulletin noting a stark increase in fraud and complaints related to cryptocurrency. According to the bulletin, "reports to the FTC show it's an alarmingly common method for scammers to get peoples' money."[29] From 2018 to the first quarter of 2022, the FTC documented over $1 billion lost due to scams involving cryptocurrency.



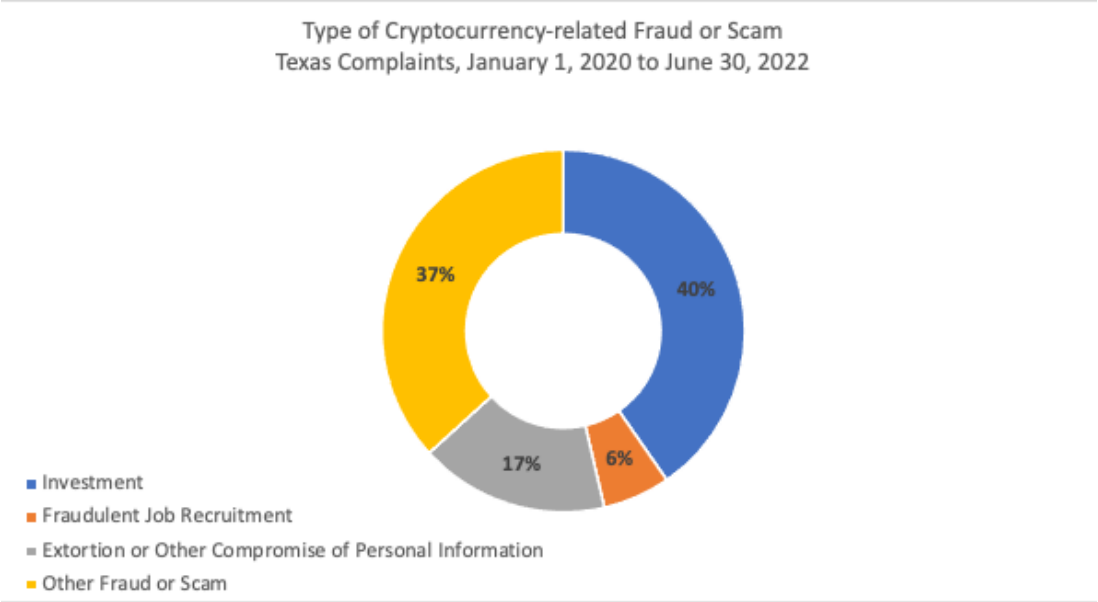
Source: Federal Trade Commission

[26] Cheyenne Ligon and Shawrya Malawa, "DeFi Platform Acala's Stablecoin Falls 99% After Hackers Issue 1.3B Tokens," *Coindesk* (August 14, 2022).

[27] MacKenzie Sigalos, "Ongoing solana attack targets thousands of crypto wallets, costing users more than $5 million so far," *CNBC* (August 3, 2022).
[28] Corin Faife, "Beanstalk cryptocurrency project robbed after hacker votes to send themself $182 million," *Verge* (April 18, 2022).
[29] Emma Fletcher, "Reports show scammers cashing in on crypto craze," *Federal Trade Commission Consumer Protection Data Spotlight* (June 3, 2022).

Data obtained from the Office of the Attorney General of Texas demonstrate similar trends, with a dramatic uptick in cryptocurrency-related complaints received from 2020 to 2021. The Office does not have a code specifically for cryptocurrency complaints, but based on complaints including the term cryptocurrency, the most common scams identified in the data are investment-related, though they manifest in numerous other ways as well.[30]

Romance scams are also common.[31] Based on the complaints, these scammers requested outrageous amounts of money for various reasons. Some reported losing a few hundred dollars, but a few reported being scammed of $200-300 thousand. There are also a concerning number of trojan horse attacks[32] and extortion using information phished about potential victims.



Seniors are also vulnerable to crypto-based scams. Though seniors are less likely than younger adults to be targeted by crypto scams, they lose substantially more money—a median of $8,000 for those 60 and over compared to $1,600 for victims in their 20's.[33]

Scams are not unique to the cryptocurrency space, but it is a concerning trend to see cryptocurrency as a growing method of choice for scammers to exploit Texans. Whereas MoneyGram,[34] Walmart,[35]

---

[30] Complaints were obtained by Texas Appleseed through an open records request to the Office of the Attorney General of Texas, for the period of January 1, 2020 to June 30, 2022. 689 complaints were received, and 332 of those complaints were categorized for this study, using word searches to verify that they were crypto-related and to categorize the complaints. The number of complaints jumped from 43 in 2020 to 197 in 2021.

[31] "Romance Scams," FBI, (last visited Aug. 5, 2022).

[32] Alison Grace Johansen, "What is a Trojan? Is it a virus or is it malware?," Norton (July 24, 2020), (explaining that "A Trojan horse…is a type of malicious software that looks legitimate but can take control of your computer. [It] is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.").

[33] Andy Markowitz, "Over $1 Billion lost to Cryptocurrency Scams in Last 15 Months," *AARP.org* (June 2022).

[34] "MoneyGram Agrees to Pay $125 Million to Settle Allegations that the Company Violated the FTC's 2009 Order and Breached a 2012 DOJ Deferred Prosecution Agreement,: *Federal Trade Commission* (November 8, 2018).

[35] "FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions," *Federal Trade Commission* (June 28, 2022).

and other intermediaries that have enabled these types of scams have been held accountable for lax practices, no such accountability measures currently exist in the cryptocurrency space.

4. Money Laundering Concerns Continue to Plague the Cryptocurrency Space

Cryptocurrency, as part of its structure, is anonymous but transparent, with every transaction in plain view on the blockchain. In the early days of bitcoin, it was used as a vehicle for money laundering and illegal enterprises, most notably, as the medium of exchange for The Silk Road.[36] It has also been a means of exchange for a large global child pornography website that included perpetrators from Texas, among other illegal enterprises.[37] For many of these cases, the trail left on the blockchain, in conjunction with cooperation from exchanges and forensic experts, has helped lead to the culprits.

However, as the efforts to follow the money trail have become more sophisticated, so have the mechanisms to hide footprints. Cryptocurrency "mixers"—a software tool where a certain amount of cryptocurrency is put in, "mixed" with other cryptocurrency and split up on the back end with the same value, but a different mix of crypto assets[38]—are being used to obfuscate cryptocurrency transactions, and they are becoming more sophisticated with time.[39] Bridges, which enable movement of cryptocurrency across different platforms, have also enabled perpetrators of fraud and other illegal activity to hide their tracks.[40]

Recently the US Department of Treasury placed sanctions on Tornado Cash, a crypto mixer, for enabling the laundering of $7 billion, including nearly $500 million stolen by North Korean hackers.[41] The statement by the Department included concerns of this money laundering undermining national security.[42]

5. Cryptocurrency Miners Profit When the Texas Electrical Grid Is Strained

It is no secret that cryptocurrency miners use large amounts of electricity to power their operations. One estimate indicated that crypto mining is expected to use 18 gigawatts in the coming years. To put that number into perspective, the current grid capacity is 80 gigawatts.[43]

Cryptomining has brought jobs to some rural communities. A representative of the City of Rockdale testified at the May public hearing of the Texas Work Group on Blockchain Matters that cryptomining had brought 300 jobs to her town, along with additional corresponding economic activity. Also striking was her comment that the mining operation uses as much electricity as downtown Dallas, which provides 135,000 jobs—450 times as many jobs for the same energy

---

[36] Charles Isidore, "Feds seize $1 billion in bitcoins they say were stolen from Silk Road," *CNN* (November 6, 2020).
[37] Andy Greenberg, "The Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site," *Wired* (April 7, 2022).
[38] Taylor Locke, "Criminals are using 'mixers' to launder millions in crypto. They're not illegal yet.," Fortune (Mar. 26, 2022).
[39] Arielle Waldman, "Cryptocurrency mixer activity reaches new heights in 2022," *TechTarg*et (July 15, 2022).
[40] Chris Gaetano, "'Cross-chain bridges' make illicit crypto harder to track," *Accounting Today* (August 10, 2022).
[41] "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," *United States Department of Treasury Press Release* (August 8, 2022).
[42] *Id,*
[43] Gretchen Morgenson, "Can the fragile Texas power grid handle a cryptomining gold rush?, NBC News (July 22, 2022).

expended based on peak numbers at the mining facility.[44]

In addition to exceedingly high power usage, these facilities appear to use large quantities of water. A mining operation looking to set up in Corsicana is expected to use 1.4 million gallons of water per day and 1 gigawatt of energy.[45] With our reservoirs strained and our electrical grid stretched, it is important to look carefully at the long-term impact of these operations on the cost of electricity and access to water for Texans.

Some assert that the power used helps the Texas grid by ceasing operations and releasing power to the grid in times of shortage. Others argue that it hurts the grid by taking up too much of the generation capacity.[46] Though this issue merits a deeper discussion, the main concern we would like to raise is its impact on the cost of electricity for Texans.

During the latest period of strain on the Texas power grid in July, a cryptomining operation made more in profits from ERCOT incentives to cease operations than they would have from mining. As the company noted in a release about the event, "By providing power back into the ERCOT grid during periods of peak demand, the Company estimates that power credits and other benefits from curtailment activities totaled an estimated $9.5 million, significantly outweighing the reduction in BTC mined."[47] While the mining operation profited from the struggling electrical grid, Texans have had to bear higher and higher costs for energy, including air conditioning during this unprecedented heat wave, paying bills that are, "50 or 60 or 70% higher."[48]

The fact that mining operations profit off of the hardship of Texans is deeply problematic and raises concerns that Texans may be subsidizing the operations of mining through higher retail charges for electricity.

6. Cryptocurrrency and Serving Underserved Markets

Cryptocurrency and other digital assets can be attractive to individuals and communities who have felt excluded from the traditional banking system or faced discrimination within that system. This appeal can particularly resonate for people of color and younger adults who have long been left out of wealth-building opportunities and are eager to participate in a new, non-traditional system.[49]

The impressive growth in value of cryptocurrency in the lead up to the 2022 crash enticed many people who felt it would be a stable and secure way to build wealth. It has not lived up to that hype for millions of investors nor has it proven to be an effective way to transact for day-to-day needs.[50]

---

[44] https://downtowndallas.com/business/market-data-reports/.
[45] *Supra*, note 43..
[46] Marcus Lu, "Visualizing the Power Consumption of Bitcoin Mining," *Visual Capitalist* (Apr. 20, 2021). See also Gretchen Morgenson, "Can the fragile Texas power grid handle a cryptomining gold rush?, NBC News (July 22, 2022).
[47] "Riot Blockchain Announces July 2022 Production and Operation Updates," (August 3, 2022).
[48] Michael Ferman, "Texans face skyrocketing home energy bills as the state exports more natural gas than ever," *The Texas Tribune* (July 5, 2022).
[49] Leda Alvim and Lulit Tadesse, "Cryptocurrency attracting Black, Latino investors and fans," *ABC News* (February 10, 2022).
[50] As one example, the nation of El Salvador has tried to embrace bitcoin as a national currency. To date the experiment is not reaping results. The sharp decline in the value of bitcoin since the experiment began has deepened the country's debt crisis and, despite multiple incentives and laws, few retail establishments accept bitcoin and just

The volatility of cryptocurrency values, unpredictable fees, lack of interoperability across cryptocurrency ecosystems, and the lack of basic consumer protections are challenges that currently undermine benefits crypto may have for unbanked and underbanked communities. The concentration of cryptocurrency wealth breeds concerns that this technology is simply building another similarly imbalanced system, just with different entities at the top. Current evidence suggests that large miners, exchanges, early adopters, and top owners of cryptocurrency are winners in the system, while small retail participants, who are likely late adopters, are taking the most harmful losses.

Conclusion

The Pensions, Investments and Financial Services Committee has an important role to play in ensuring that the interests of all Texans—interests that include access to basic necessities like affordable energy and water, as well as financial interests—are top-line priorities in Texas policy related to blockchain and cryptocurrency.

This written testimony highlights key consumer protection concerns but does not address all of them. For example, data privacy concerns are also important to consider. Data privacy concerns are relevant to multiple uses of blockchain, where the immutable ledger could make it hard for personal information people may want to put behind them and have a legitimate interest in doing so. It is also important with regard to the data of individual users who use, hold, buy, and trade cryptocurrencies, particularly if blockchain based retail transactions become a reality. Our financial lives are currently followed in multiple ways and data privacy is already a major concern. Having our financial lives documented on a public blockchain will create even more opportunities for motivated governmental entities, hackers, and fraudsters to track and potentially exploit us.

Technology is evolving and we cannot predict where things will go and what unforeseen opportunities, benefits, or pitfalls may present themselves. The ultimate guidance our organization brings as a data-driven institution is that existing evidence of problematic practices must be weighed heavily as policy options are debated. The systemic consumer protection concerns raised in this letter must be addressed if we want to see blockchain and cryptocurrency-based systems grow on a solid foundation. Under the current system, there are deep concerns, supported by evidence from the latest crypto market crash, that it is a system with many vulnerabilities.

Tax incentives and liability protections for business models that have proven rife with problematic practices that drain wealth from retail consumers may not be the best direction for Texans and our economy. We ask that there be thoughtful consideration into how the current blockchain and cryptocurrency market has impacted everyday Texans as we work to build policies that support a bright future of our state.

10% of the population is using the national wallet to transact. See: Anthony Kurmanaev and Bryan Avelar, "A Poor Country Made Bitcoin a National Currency. The Bet Isn't Paying Off," *The New York Times* (July 5, 2022).