**Cipriani Family Law Inn of Court**

**February 5, 2025**

**Divorce: digital assets in divorce including locating, valuing, and distributing &**

**Regulations including cryptocurrency news, Bitcoin Reserve and Legisltion;**

1. DIGITAL Assets:
   What it is and how to find it?
   How do cryptocurrencies enable asset hiding?
   What are Crypto Exchanges?
   What are Digital Wallets and where does Crypto Reside?
   How to ID signs of Hidden Crypto Assets?

2. How to Value Crypto During Divorce (Valuation Methods, Approaches to address Valuation Challenges) and Divide Cryptocurrency in Divorce? (transfer, cash-out?)
   Discovery; Where to Look for cryptocurrency – strategy? Forensic Experts, tech specialists

   - Bank and credit statements; Exchange names; Check descriptions; Revealing Crypto Clues look for Exchange apps, Payment apps, price tracking apps, wallet apps, News info apps, Twitter reddit feeds; App – Sleuthing – Apps, installed on phones, tablets, other devises; Tax returns: IRS Form 8949; Loan applications

3. Cryptocurrency holdings in divorce: Lack of regulation, Privacy concerns and tax implications

   Crypto News and currency

   Bitcoin Reserve, PA Bill 2481, Bitcoin Rights Bill

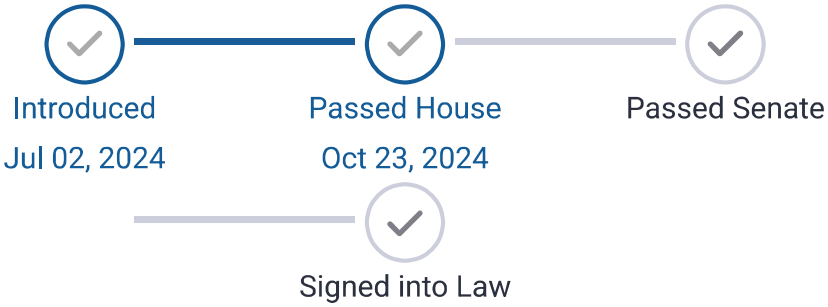
**February 2/5/25 Inn team**:

a. MK Feeney, Esq.
b. Gregory Hyde, Esq.
c. Carol Krawitz Verlin, Esq.
d. Patrick Cooper, Esq.
e. Elizabeth Klaproth, Esq.
f. Heidi Anderson, Esq.

FastDemocracy

# HB 2481

Overview
Bill Summary
Tweets
Similar Bills
Sponsors
News
Votes
Actions
Bill Texts
Documents
Sources




## HB 2481

Pennsylvania House Bill



An Act providing for restriction on use and custody of digital assets prohibited and for use of nodes authorized.



**Last Action** **See all actions**

Senate • Nov 07, 2024: Referred to COMMUNICATIONS AND TECHNOLOGY

**Latest Bill Text** **See all bill texts**

Printer's No. 3791

# HB 2481

Overview
Bill Summary
Tweets
Similar Bills
Sponsors
News
Votes
Actions
Bill Texts
Documents
Sources

## Summary/Bill Text

PRIOR PRINTER'S NOS. 3475, 3747 PRINTER'S NO. 3791

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 2481

Session of

2024

INTRODUCED BY CABELL, KAUFER, FLICK, RYNCAVAGE, ECKER AND KUTZ,

JULY 2, 2024

AS AMENDED ON SECOND CONSIDERATION, HOUSE OF REPRESENTATIVES,

OCTOBER 22, 2024

AN ACT

### Sponsors

**Mike Cabell**
primary
( - )

**Aaron D. Kaufer**
cosponsor
( - )

**Jamie L. Flick**
cosponsor
(R - 83)

**Ryncavage**
cosponsor

**Ecker**
cosponsor

**Kutz**
cosponsor

### Votes

# HB 2481

Overview
Bill Summary
Tweets
Similar Bills
Sponsors
News
Votes
Actions
Bill Texts
Documents
Sources

Oct 22, 2024, House
HB 2481 PN 3747, 2023 A5982

YES: 202 NO: 0 OTHER: 1

Oct 23, 2024, House
FINAL PASSAGE

YES: 176 NO: 26 OTHER: 1

## Actions

**Nov 07, 2024 | Senate**
- Referred to COMMUNICATIONS AND TECHNOLOGY

**Oct 23, 2024 | House**
- Re-reported as committed
- Third consideration and final passage

**Oct 22, 2024 | House**
- PN 3791 Second consideration, with amendments
- Re-committed to APPROPRIATIONS

**Oct 09, 2024 | House**
- PN 3747 Reported as amended
- First consideration
- Laid on the table
- Removed from table

**Jul 02, 2024 | House**
- PN 3475 Referred to COMMERCE

# HB 2481

Overview
Bill Summary
Tweets
Similar Bills
Sponsors
News
Votes
Actions
Bill Texts
Documents
Sources

## Bill Texts

- Printer's No. 3475 HTML
- Printer's No. 3475 PDF
- Printer's No. 3475 MSWORD
- Printer's No. 3747 HTML
- Printer's No. 3747 PDF
- Printer's No. 3747 MSWORD
- Printer's No. 3791 HTML
- Printer's No. 3791 PDF
- Printer's No. 3791 MSWORD

## Documents

- House Fiscal Note PDF

## Sources

- http://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?syear=2023&sind=0&body=H&type=B&BN=2481
- http://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2023&sind=0&body=H&type=B&BN=2481

# Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

**Abstract.** A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

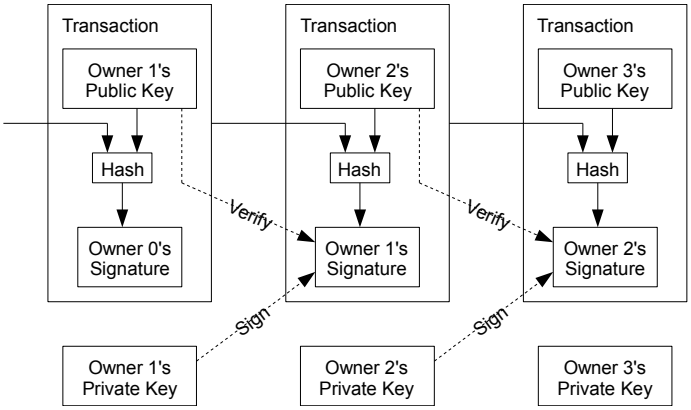
## 1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

## 2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

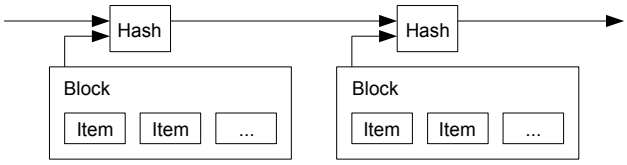



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

## 3. Timestamp Server

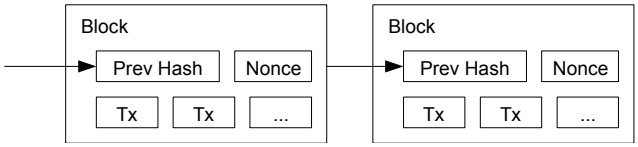
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



## 4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.




The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

## 5. Network

The steps to run the network are as follows:

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

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

## 6. Incentive

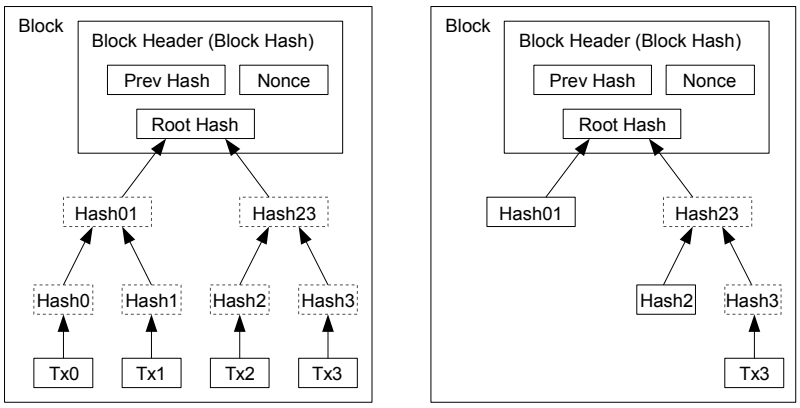
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

## 7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



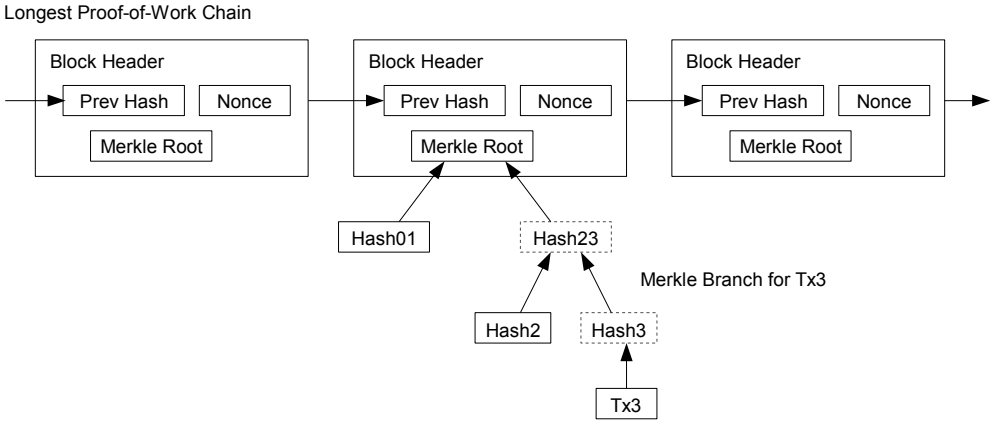

Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

## 8. Simplified Payment Verification

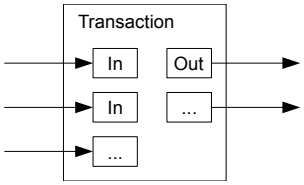
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.




As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

## 9. Combining and Splitting Value

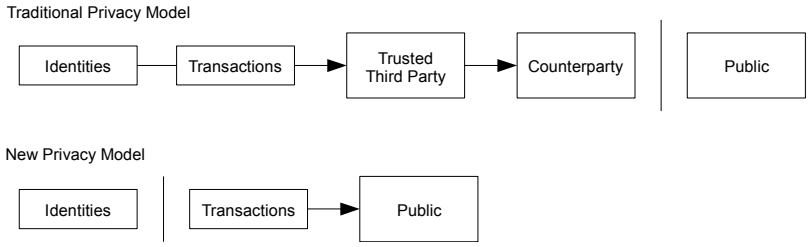
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.




It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

## 10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.




As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

## 11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

$p$ = probability an honest node finds the next block
$q$ = probability the attacker finds the next block
$q_z$ = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and $z$ blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

## 12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

## References


[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

# CRACKING THE CODE: A GUIDE TO DISCOVERING, VALUING, AND DIVIDING DIGITAL ASSETS IN DIVORCE

Posted by **John Millard** | Aug 09, 2023 | 0 Comments

In today's rapidly evolving financial landscape, the emergence and adoption of digital assets like Bitcoin and Ethereum have added a layer of complexity to divorce proceedings. Cryptocurrencies and other digital assets present unique challenges in divorce cases, especially when these assets are undisclosed or hidden. In this guide, we will delve into the world of cryptocurrencies, explore their potential for asset hiding, and discuss steps to uncover and equitably distribute digital assets. Get ready to crack the code and learn how to locate and divide digital assets!

## WHAT ***ARE*** CRYPTO ASSETS?

Cryptocurrencies, often called “crypto,” encompass a wide range of digi
Bitcoin is the most well-known, “crypto” also includes other digital valu

such as utility and non-fungible tokens (NFTs). Utility tokens grant access to specific platforms or services, while NFTs represent unique digital items, like digital art, collectibles, or virtual real estate. Unlike traditional assets such as real estate or stocks, cryptocurrencies exist only in digital form. This distinction makes them particularly challenging to identify, assess and divide during divorce proceedings.

## HOW DO CRYPTOCURRENCIES ENABLE ASSET HIDING?

Cryptocurrencies provide an appealing avenue for asset hiding during divorce due to their unique characteristics. Instant and seamless transferability without traditional intermediaries like banks enables parties to securely transfer and hold digital assets on a computer or smartphone. Moreover, cryptocurrencies operate on decentralized computer networks based on blockchain technology, resulting in a lack of central oversight and making it challenging to monitor financial activities. Additionally, cryptocurrency transactions are pseudonymous, meaning the real identity behind each transaction is often obscured, adding a layer of privacy and confidentiality.

## CRYPTO EXCHANGES

Like traditional brokerages, “exchanges” serve as digital platforms that enable individuals to trade, buy, and sell cryptocurrencies. Users can deposit funds, usually in fiat currency or other cryptocurrencies, into accounts on the exchange platform and use those funds to purchase or sell different cryptocurrencies at prevailing market prices. Exchanges provide user-friendly interfaces, order books displaying current buy and sell orders, and often offer additional features such as advanced trading options, secure storage of funds, and access to market data.

Fortunately, transactions on exchanges can leave traces crucial in uncovering hidden cryptocurrency assets. Family law attorneys can request transaction records from these exchanges as part of the discovery process to unveil the existence and location of potential hidden assets.

Several well-established cryptocurrency exchanges have gained prominence in the crypto industry. Notable examples include Binance, Coinbase, Kraken, Gemini, Bitfinex, and KuCoin. However, it's important to note that the cryptocurrency exchange landscape is dynamic, with new and existing exchanges evolving.

## DIGITAL WALLETS: WHERE CRYPTO ASSETS RESIDE

Digital wallets are tools that store, send, and receive cryptocurrencies. They come in various forms, including software wallets (online or mobile apps), hardware wallets

(physical devices), and paper wallets (printed or written codes). Cryptocurrency holdings can be stored off exchanges in digital wallets, protected by complex cryptographic keys, making it difficult to link these assets to an individual.

A digital wallet typically consists of a pair of cryptographic keys. The public key, also known as the address, is used for sending and receiving funds, while the private key, acting as a password, is utilized for authorizing transactions and accessing the stored assets. Safeguarding and protecting the private key is crucial to ensure the security of cryptocurrency holdings.

## IDENTIFYING SIGNS OF HIDDEN CRYPTOCURRENCY ASSETS

Recognizing indicators of hidden cryptocurrency assets is crucial for family law attorneys. Unusual financial behavior, such as unexplained transfers or discrepancies in reported income, may signal attempts to hide assets using cryptocurrencies. There are indicators, or signs individuals should be aware of if they suspect their spouse is hiding cryptocurrency assets during a divorce. Here are some examples:

- *Cryptocurrency Wallets*: Look for evidence of cryptocurrency wallets on electronic devices or statements related to wallet services. Wallets may be stored on computers, smartphones as an app, or hardware devices. Unexplained transfers of funds to or from cryptocurrency wallets can be a strong indication of hidden assets.
- *Unfamiliar Financial Accounts*: Monitor bank statements and financial records for unusual transactions or transfers to cryptocurrency exchanges or platforms. These transactions can suggest the conversion of funds into cryptocurrencies or moving assets to different exchanges.
- *Increased Online Security Measures*: A sudden increase in security measures, such as using encrypted messaging apps, password managers, or virtual private networks (VPNs), may signify attempts to conceal cryptocurrency-related activities.
- *Minimal Financial Footprint*: If your spouse's financial records or bank statements show a lack of transactions or a significant decrease in traditional financial activity or spending, it may indicate the presence of hidden cryptocurrency assets. However, this can also suggest that a spouse has other undisclosed traditional accounts like checking accounts.
- *Unreported Income or Investments*: Look for discrepancies between reported income and actual spending patterns. If your spouse is living beyond their reported means or making substantial purchases without a clear source of income, it could suggest

hidden cryptocurrency assets.

- *Unexplained Tech Expertise*: If your spouse suddenly exhibits a high level of technical knowledge or is interested in computer programming, cryptography, or blockchain technology, it could indicate involvement with cryptocurrencies.

## WHERE TO LOOK

Uncovering hidden cryptocurrency assets requires a strategic approach. Family law attorneys should collaborate with forensic experts and technology specialists who can analyze financial records, trace transactions, and identify digital breadcrumbs left behind by cryptocurrency transactions. In-depth investigations can shed light on concealed assets and contribute to achieving an equitable distribution. If you suspect a spouse is hiding assets, you must actively search for proof of your suspicions. Places to start include:

### ***Bank and Credit Statements***

Cryptocurrency is usually purchased with fiat (currency), so at some point, money must move from a bank account into a cryptocurrency exchange account. It is, therefore, essential to check bank and credit card statements for popular crypto exchange names such as Coinbase, Binance, Kraken, Bitfinex, Gemini, KuCoin, Etoro, and Bitstamp. In addition, look for purchases or transfers with descriptions such as “crypto”, “coin”, “digital asset”, or ticker symbols like BTC (Bitcoin), ETH (Ethereum), LTC (Litecoin), ADA (Cardano), XLM (Stellar), and DOGE (Dogecoin). If you see evidence of any crypto activity, however insignificant, it's worth investigating further — especially if a spouse omitted these assets from their initial disclosures.

### ***App-Sleuthing: Revealing Crypto Clues!***

Evidence of crypto use may be hiding in plain sight. Look for crypto-related apps installed on phones, tablets, and other electronic devices, such as:

- *Exchange Apps*: These apps enable users to trade cryptocurrencies and access market data. Popular exchange apps include Coinbase, Binance, and Kraken.
- *Payment Apps*: These apps facilitate cryptocurrency payments and transactions. Notable examples are Strike, BitPay, Crypto.com, and Venmo (which supports cryptocurrency transactions).
- *Price Tracking Apps*: These apps provide real-time price updates and market information for various cryptocurrencies. Examples include CoinMarketCap, CoinGecko, and Blockfolio.

- *Wallet Apps*: These apps allow users to manage their cryptocurrency holdings, send and receive funds, and view transaction history. Examples include Ledger, Trezor, Coinbase Wallet, Trust Wallet, and Exodus.
- *News and Information Apps*: These apps offer news, articles, and educational resources related to cryptocurrencies and blockchain technology. Examples include CoinDesk, Cointelegraph, and CryptoSlate.
- *Twitter & Reddit Feeds*: Check who your spouse follows on Twitter and Reddit. Check hashtag searches for cryptocurrency. An interest in hashtags like #Bitcoin, #BTC, #ETH, or #Crypto shows at least an interest in these assets.

### *Tax Returns*

Checking if your spouse has reported crypto on a tax return is vital. Income from cryptocurrency transactions is taxable by law, just like income or gains from other property. Starting in tax year 2019, the IRS began to include a question on the front page of the federal tax return 1040 form asking if "you received, sold, sent, exchanged, or otherwise acquired any financial interest in any virtual currency." IRS introduced this question to improve tax compliance and ensure taxpayers accurately report their cryptocurrency-related income and gains. If this box is checked on a tax return, the details of each transaction must be reported on Form 8949 (Sales and Other Dispositions of Capital Assets).

### *Loan Applications*

Other places to look for evidence of crypto assets include loan applications. Even if a spouse is trying to hide crypto assets, they might still list them on a loan or line of credit application. After all, you want your balance sheet to look good if you're trying to secure a loan!

## WHAT SHOULD YOU DO IF YOU SUSPECT YOUR SPOUSE IS HIDING CRYPTOCURRENCY ASSETS?

If you suspect your spouse is hiding cryptocurrency assets during divorce, taking proactive steps to protect your financial interests is crucial. Here are some actions to consider:

- *Consult with an Experienced Divorce Attorney*: Seek the guidance of a divorce attorney with knowledge and experience handling cases involving cryptocurrency assets. They can provide legal advice, guide you through the process, and assist in effectively uncovering and addressing hidden assets.

- *Gather Evidence*: Document any suspicious behavior or financial activities that raise concerns about hidden cryptocurrency assets. Keep records of unexplained expenses, withdrawals, or transfers. Take screenshots or save relevant digital communications or financial statements that may serve as evidence.
- *Pursue Extensive Discovery*: Obtaining complete financial disclosure from the spouse is critical. Work with your attorney to utilize legal tools such as subpoenas, formal discovery requests, or court orders to compel your spouse to disclose information about their financial holdings, including cryptocurrency assets.
- *Consult Financial and Cryptocurrency Experts*: Engage the services of forensic accountants or cryptocurrency experts who can help identify and evaluate hidden cryptocurrency assets. They can analyze blockchain transactions, trace digital wallets, and provide expert opinions on the value of the assets.
- *Consider Mediation or Arbitration*: If you and your spouse are open to alternative dispute resolution methods, such as mediation or arbitration, consider working with a mediator who understands cryptocurrencies and can facilitate discussions on the division of assets. A knowledgeable mediator can help the parties reach a fair and equitable resolution.

## VALUING CRYPTOCURRENCY DURING DIVORCE

Divorcing couples often face the challenge of fairly dividing their assets, but the complexity is magnified when cryptocurrency enters the equation. Cryptocurrencies are highly volatile and can experience significant price fluctuations quickly. Determining an accurate and fair valuation is essential to ensure an equitable distribution of marital property.

Crypto assets are property. Like other assets, crypto may be deemed community property subject to division in a divorce action. Dividing cryptocurrency or its equivalent worth can be difficult, as it is not only easy for parties to hide cryptocurrency transactions, but it can also be challenging to determine the actual value of cryptocurrency.

### *Challenges of Valuing Cryptocurrency*

Market Volatility: Cryptocurrency markets are known for their extreme volatility. The value of cryptocurrencies can skyrocket or plummet within hours, making it challenging to pinpoint a precise valuation at any given moment.

Lack of Regulation: The lack of regulatory oversight in the cryptocurrency space further

complicates valuation. Unlike traditional assets that adhere to established valuation standards, cryptocurrencies operate in a relatively unregulated environment.

Multiple Exchanges: Cryptocurrencies are traded on numerous exchanges, each with potentially varying prices for the same digital asset. This divergence can lead to discrepancies in valuation if not carefully addressed.

### *Valuation Methods for Cryptocurrency*

Market Value: This method involves valuing cryptocurrency assets based on current market prices. While it provides a real-time snapshot of value, it may not accurately reflect the long-term worth of the assets due to market fluctuations.

Cost Basis: Calculating the cost basis involves determining the original purchase price of the cryptocurrency. While it offers a historical perspective, it may not consider the current market conditions.

Expert Appraisal: Engaging a cryptocurrency valuation expert may be necessary for complex cryptocurrency portfolios. These professionals analyze various factors, including historical data, market trends, and the specific cryptocurrencies held.

### *Approaches to Addressing the Valuation Challenge*

Evaluating the average value: Instead of considering the peak value or the current reduced value of the crypto asset, the parties can agree to use an average value over a specific period of time. This approach aims to provide a more balanced representation of the asset's worth, considering both the peak and lower market values.

Offsetting other assets: If one spouse incurred significant losses due to the decreased value of the crypto asset, the parties may consider offsetting losses by adjusting the division of other assets. This can help balance the impact of the volatile cryptocurrency market on the overall distribution of marital property.

Deferred settlements: In some cases, deferring the sale or transfer of cryptocurrency assets may be beneficial until the market stabilizes or recovers. This approach allows both parties to hold onto their respective shares of the assets without realizing immediate losses. It provides an opportunity to benefit from potential future market improvements.

In-Kind Division: In-kind division refers to directly transferring specific cryptocurrencies from one spouse to another rather than selling the assets and splitting the proceeds. Like issues with an in-kind division of other securities such as stocks or bonds, when dealing

with a cryptocurrency, which is subject to significant price fluctuations, determining an equitable division becomes more complex. Both parties must agree on the valuation date and method to assess the asset's value accurately. Additionally, considering the tax implications of such transfers is crucial, as the recipient may inherit the tax basis and potential capital gains or losses associated with the cryptocurrency.

## DIVIDING CRYPTOCURRENCY IN A DIVORCE

Husband and Wife are going through a divorce. It is discovered that Husband has significant Bitcoin holdings held in an electronic wallet in Husband's name. Husband and Wife need to decide how to divide the community Bitcoin holdings. They have three main options: transfer, cash-out, or valuing for offset. Let's look at all three.

### *Transfer*

If a portion (or all) of the Bitcoin holdings will be transferred to Wife, she must open an electronic wallet to receive the transfer. Husband will need Wife's new wallet address for the Bitcoin to make the transfer. Husband can then send the Bitcoin to Wife based on a dollar value or by selecting the number of coins to send.

Important Considerations About Crypto Transfers

- Is the spouse comfortable with the complexity and risks associated with the custody and potential volatility of crypto?
- Who will cover transaction fees related to the transfer?
- What is the impact of potential capital gains or losses on the digital assets received?

One thing to remember is Internal Revenue Code **Section 1041**, which states that property transfers between spouses or incident to divorce are treated as a gift and are not taxable at the time of transfer. Under this rule, the transferee acquires the transferor's tax basis in the property. The effect is to *defer* tax consequences (recognition of any gain or loss) until the transferee disposes of the property. Consulting a competent tax advisor on these issues is always wise!

### *Cash-out*

Wife decides she doesn't want to deal with the volatile nature of their marital cryptocurrency holdings and would prefer to sell her portion of the Bitcoin and receive cash instead. There are two ways to do this.

Option 1: Husband sells Wife's portion and sends Wife the cash.

Option 2: Husband sends Wife her portion of the cryptocurrency, and Wife sells it immediately and receives the cash.

Things to consider if you go the cash-out route. The main difference between options one and two is in whose name the capital gains must be reported. And, in the case of a crypto transfer, there will likely be transaction fees that should be considered.

### *Valuing for offset*

Wife decides she would prefer an offset for the value of her portion of the cryptocurrency. This means a value needs to be placed on the Bitcoin that Husband is keeping, and Wife will receive another asset instead. Things to consider if you go the "Value for Offset" route include:

- What value will be used? Due to the wide fluctuations in the market value of some cryptocurrencies, it may make sense to not determine the offset value until the date the divorce is finalized or close to it. Another option would be to use a 52-week moving average as the value.
- Are tax consequences considered when determining a value for offset? For example, $10,000 in cash is different from $10,000 in cryptocurrency purchased for $3,000. The cryptocurrency in this example would have a $7,000 taxable capital gain if sold or transferred for goods or services. The spouse who keeps the cryptocurrency should consider asking for a full or partial tax discount to help cover future taxes.

## CONCLUSION

Every divorce involving cryptocurrency assets is unique, requiring tailored strategies based on individual circumstances. Working closely with a knowledgeable divorce attorney experienced in complex financial matters is crucial to protecting one's interests. When it's time to mediate, leveraging the expertise of a mediator who understands cryptocurrencies, trading exchanges, and blockchain technology becomes even more critical.

At Armatys Millard, we understand the intricacies of divorce cases involving hidden assets, including cryptocurrencies. With our expertise in family law and judicial insight, we can guide you through mediation or arbitration toward a successful resolution. **Schedule your mediation session** today and take the first step toward a fair and equitable divorce settlement.

## READY TO TAKE A DEEPER DIVE?

As you have probably gleaned, the topic of digital assets is complex and evolving. One thing is certain – digital assets are here to stay, and their importance in the division of the marital estate will continue to escalate. As family law practitioners, we must become educated about these assets. This article provides only a brief overview of this complicated subject. If you're ready to learn more, I suggest that you consider reading the following excellent articles:

**A Divorce Practitioner's Bitcoin Primer**, by Richard West and Jonathan Fields.

**Cryptocurrency, NTFs, and the "Metaverse": Addressing the Expanding World of Virtual Assets in Divorce Proceedings**, by Stephanie L. Tang.

---

## SHARE



## ABOUT THE AUTHOR

### JOHN MILLARD

John Millard recently served as Associate Judge of the 328th District Family Court, Fort Bend County. This experience gave John a keen insight into how Judges think, what persuades them, what annoys them, and, importantly, what information Judges need to make an appropriate ruling. John provides mediation and arbitration services for family law cases pending in Fort Bend, Harris, and surrounding counties. You can count on John's extensive family law experience and judicial wisdom to help successfully resolve your case.

## COMMENTS

There are no comments for this post. Be the first and **Add your Comment** below.

### LEAVE A COMMENT

**NAME**

**EMAIL**

WOODRUFF
FAMILY LAW GROUP

# Cryptocurrency and Divorce Cases

**Cryptocurrency and Divorce Cases**

Divorce cases with cryptocurrencies have undoubtably been adjudicated by now. However, written appellate opinions are still sparse at this time in Guilford County and beyond. But more and more Americans are investing in crypto, and we should begin seeing more complex cases being published shortly. Below are two cases, one from California the other from Washington, both community property jurisdictions. One case involves a spouse hiding cryptocurrency during a divorce and the other case involves dividing Bitcoins in a divorce.

Chao Liu v. Junhuia Chang (Wash. App. 2020):

Plaintiff wife and Defendant Husband were in a proceeding for division of their property in 2017. Mother introduced a screenshot of Husband's Bitcoin wallet showed that Husband owned 53.21 Bitcoins valued at $504,766. Husband testified that he had sold all those Bitcoins in 2015 to support himself. But he also produced account information a month before trial that evidenced his ownership of the 53+ Bitcoins.

The trial court ultimately did not find Husband's testimony credible; notably, even allowing Husband to bring his computer to court to show the current wallet balance, which Husband did not do. The court valued the Bitcoin and distributed that value to Husband, and he appealed. This was reviewed under an abuse of discretion standard, and given the trial court record, no abuse was found.

The interesting part of this was that the trial court had written in their order that due to the nature of cryptocurrency, it was difficult for anyone but the owner of Bitcoin to establish how many Bitcoins were owned and at what time and what value.

This case's result was only because Husband was unable to prove that he did not have Bitcoin. It perhaps signaled that more extensive discovery may be needed to determine ownership. Bitcoin itself is only pseudo-anonymous, through some forensic investigations, it is possible to determine the owner of Bitcoins. As referenced in the previous segment, if you suspect or find evidence that your spouse has secret cryptos, it may be worthwhile to delve deeper to determine the extent of ownership and an accurate value.

Desouza v. Desouza (In re Desouza), 54 Cal.App.5th 25, 266 Cal.Rptr.3d 890 (Cal. App. 2020)

In January of 2013, Plaintiff wife initiates the divorce proceedings, and is granted an "automatic temporary restraining order that . . . prohibited him from transferring, encumbering, hypothecating, concealing, or in any way disposing of any property, real or personal, whether community, quasi-community, or separate, without the written consent of the other party or an order of the court, except in the usual course of business or for the necessities of life."

However, Husband then goes on to make multiple purchases of Bitcoin through his friends. They are held in the Mt. Gox account. In total, he purchased 1062.21 Bitcoins for $144,391. In 2017, the party's property trial was held, and a judgment was entered that ordered Husband to divide his Bitcoins evenly. Between 2013 and 2017, Mt. Gox

suffered a hack, legal issues, and was forced to declare bankruptcy. Thus, Husband had only had possession of 613.53 of his total Bitcoins. However, this only came to light after the entry of the judgment. Wife then moved for post-judgment relief seeking immediate transfer of her interest in the Bitcoin, and for further remedies available by California law. The trial court eventually also ordered Husband to transfer a further 249.445 Bitcoins, and $22,500 in cash to Wife, and awarded attorney's fees. Husband appealed.

On appeal, the Court held that in concealing these Bitcoin transactions had violated a fiduciary duty that California imposes of married couples, continuing even through separation. The fact that Wife did not know that a portion of the Bitcoin was tied up by Mt. Gox's bankruptcy and legal woes was a material omission. If Wife had known, she may have objected to an in-kind division of the Bitcoin. Had she known about Husband's decision to purchase in the first place, she could have motioned to enjoin Husband from the initial purchase. The fact that Wife benefitted from his unilateral decision to purchase Bitcoin (the value had skyrocketed, and the investment was worth millions), would not be an excuse for Husband's actions. The trial court's order was affirmed.

The cases both illustrate some of the difficulties associated with crypto in divorce. Namely, identification of existence, ownership, and value. It also brings up a practical consideration for distribution of property: in-kind distribution, or distributive award? The need for accurate accounting of crypto is apparent, but thankfully it seems like discovery tools are catching up with the technology. Our divorce lawyers in Greensboro have expertise in the emerging field of cryptocurrency and can advise you in this process.

---

## Practice Areas

**High Net Worth** | **Divorce** | **Child Custody and Support** | **Property Division – Equitable Distribution** | **Spousal Support** | **Family Law Appeals** | **Alienation and Other Civil Actions** | **Business Planning / Financial Planning for Divorce** | **Trials / Mediation / Collaborative** | **International Family Law**

---

420 W Market St
Greensboro, NC 27401

**Phone:** 336.272.9122

We serve the following localities: Guilford County, including Greensboro and High Point; Alamance County, including Burlington and Graham; Caswell County, including Yanceyville; Chatham County, including Siler City and Pittsboro; Davidson County, including Lexington and Thomasville;
Durham County, including Durham; Forsyth County, including Winston-Salem; Orange County, including Chapel Hill and Hillsborough; Person County, including Roxboro; Randolph County, including Asheboro and Randleman; Rockingham County, including Reidsville and Wentworth; Rowan County, including Salisbury; Stokes County, including Danbury; Wake County, including Raleigh and Cary.

We do high net worth, complex custody, and high-income cases statewide on a case-by-case evaluation. Ms. Woodruff will consider cases outside the Piedmont Triad on a case-by-case basis.

Cryptocurrency and Divorce Cases | Greensboro Family Law Lawyers

# Cryptocurrency Becomes a Real Threat

Pennsylvania Bar News · July 12, 2021

This article was originally published in the PBA Family Law Section *Pennsylvania Family Lawyer* summer 2021 issue. It is reprinted here with the author's permission.

By Mark R. Ashton

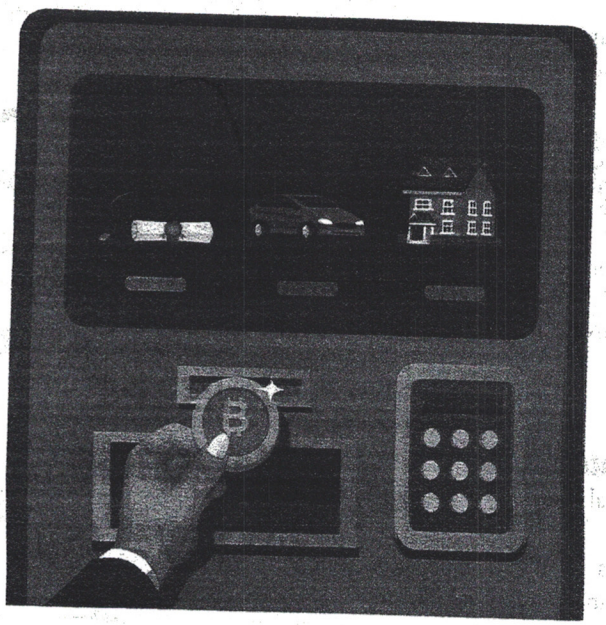
In many cases, we deal with parties hiding assets the old-fashioned way. For much of this writer's career, the game was "cash." The pizzeria, the auto body shop, the produce vendor. They lived in 3,500 square foot houses and drove luxury cars. Nevertheless, the tax returns showed a mere $30,000 in income, a remarkable achievement.

In the last 20 years, the cash world has measurably changed. I have worked alongside fellow lawyers who told me that I could turn them upside down and empty their wallets without finding more than $20 in cash. When I stand in line at the convenience store today, people in front of me are buying cigarettes and a sandwich with a debit or credit card. The dry cleaner, and yes, even my local pizzeria, will take plastic for any transaction over $5. So cash is dead, right?

Well, not so fast. When bitcoin and cryptocurrency originated, it appeared that these would be assets accessible to the rich. In January 2017, a bitcoin commanded $900 and there were very few places to trade or exchange it. A year later, it had catapulted to $17,000. Then it collapsed. In January 2019, it was worth $3,800. The beginning of 2020 brought it back up to $7,400, still half of the value two years earlier. So, bitcoin had two problems. It was not easily accessible to trade and it was highly volatile; two sound reasons to stay away even if your goal was to hide assets from a spouse. After all, if you had $17,000 you wanted to hide in January 2018, you could buy a bitcoin and hope no one figured it out. However, a year later, your crummy coin had lost 75% of its value, worse than disclosing and sharing the asset with your unworthy spouse.

The year 2020 changed everything. If you bought a "coin" early in 2020, you paid $7,400. A year later, your coin was worth $32,000. Last week it was commanding $63,000. Your dollar investment was now worth $9. Then there was mid-April 2021, when your bitcoin lost 10% of its value while you were in bed sleeping.

A few months ago, I engaged a contractor to fix some things around my house. As I signed his proposal, he asked if I had any bitcoin. I confessed that I was wary. His response was his whole family had investments in bitcoin. As he left, I mused where his family would have access to acquire virtual coins at $18,000 a pop.



A week ago, I found my answer. I was in the supermarket and as I departed, I saw a currency machine at the front of the store where you bring your change or buy ice or umbrellas. "Bitcoin sold here." So now I can hit the grocery store account for $20 in groceries and take $100 cash back. I

then wander over and put my $100 in the bitcoin machine. That will get me 0.00159 of a bitcoin assuming no one is going to ding me for a 10% commission to buy. My spouse will never know because my bitcoin machine and I have a confidential relationship, right?

My grocery store visit prompted me to wonder whether this was an aberration. So, I looked at a site to search for places that sold cryptocurrencies. It is https://coinatmradar.com/bitcoin-atm-near-me/. My office is 35 miles northwest of Philadelphia in an affluent Chester County suburb. My search turned up 20 cryptocurrency vending machines within 15 miles. All but one was in a gas station or a convenience store. Perhaps American investors have shifted from brokerages to petrol stations. My suspicion is that these investors are in fact lottery ticket buyers who decided that at least all is not lost when the winning ticket is drawn.

So, I smell a cryptocurrency bubble emerging. However, this is not an investment article. What concerns me is the temptation to use a vending machine to hide assets when it's right there in the grocery store or gas station. Unhappy spouses who don't want to share their marital assets may be "parking" wealth at the bitcoin machine.

What's the solution in a divorce setting? It can be dubbed "Forensics at home." Gather a year of bank statements. Prepare a chart of cash withdrawals. If you see a regular pattern of large cash withdrawals from particular places,

Mark R. Ashton

go look at the location and see if there are cryptocurrency machines. We have just asked a client to do this and to his surprise, his spouse had $32,000 in cash withdrawals over 18 months. Certainly, we all need cash but when was the last time you spent an average of $60 a day in actual Federal Reserve currency every single day for 545 consecutive days? That was in addition to $9,000 in groceries, $9,000 in clothing and $9,000 in personal care expenses that showed as withdrawals for those purchases. The clear message is that money is being palmed. It used to be in the cigar box or a shoebox in the closet. Now the shoebox is at the gas station and the grocery store.

Mark R. Ashton is a partner in the Exton office of Fox Rothschild LLP, past chair of the PBA Family Law Section, editorial board of *Pennsylvania Family Lawyer*, member, Chester County Bar Association (former chair, Domestic Relations Section), Montgomery Bar Association (former director) and member, Board of Directors, Historic Yellow Springs (president, 2009-11). mashton@foxrothschild.com. 610-458-4942

The Family Law Section focuses on the development and practical working of the law relating to marriage, divorce, support, custody, property and economic matters, and domestic relations generally, as well as the law relating to adoption and to juvenile dependency. For more information, go to https://www.pabar.org/site/For-Lawyers/Sections/Family-Law-Section.

# DIVIDING DIGITAL ASSETS IN DIVORCE

A Divorce Practitioner's Bitcoin Primer

The first step is to identify all marital assets, which for example are: accounts, account balances, investments, trusts, dividends, CD's etc.

## I. General Information

Financial Discovery and Enforcement in Pennsylvania

**The Pennsylvania Rules for Discovery in Domestic Relations Matters** allow for discovery in cases, which is the process of identifying, qualifying, and determining the value of all marital assets that are then subject to equitable distribution among the parties. The court has the power to investigate and enforce non-compliance among parties (such as non-disclosure of assets) throughout the discovery process.

A Divorce Practitioner's Bitcoin Primer

## II. Discovery

Practitioners should question clients at the outset of a matter to determine whether Bitcoin may play a role in the divorce. Inquiries might include whether the client or their spouse: (a) is tech savvy; (b) has ever bought and sold bitcoins; and (c) has ever received bitcoins in exchange for goods and services.

If there is a history of Bitcoin ownership, further inquiries should include: (a) How did the client or spouse store or transact in bitcoins? (b) Where are important records kept and does the client have access to them? (c) What electronic devices does the client or spouse own? (d) Does the client have physical access to such electronic devices?

If the practitioner determines Bitcoin discovery is warranted, the first step in a sound discovery plan is to send a "preservation letter" to the spouse's attorney reminding that spouse to preserve evidence on phones and computers. If evidence is not preserved, the letter helps to establish a claim for spoliation, an element of which is bad faith and a conscious disregard of the duty to preserve relevant evidence. If a court finds spoliation, it may preclude evidence or make an adverse inference should the matter go to trial. Because every time a person continues to use a computer or phone, there is the potential

that relevant data is overwritten, the letter should remind the opponent to "image" (copy/ghost) their drives immediately so there is a record of them at or about the point in time the preservation letter was received.

While seemingly perplexing, Bitcoin discovery is no different from tracing more traditional assets and may even provide more information. Blockchain transactions are not strictly anonymous, but rather pseudonymous, since they can be linked to a public address. Because of the immutable nature of the blockchain, information on every transaction remains available forever, unlike conventional financial institutions which may only keep records for seven years. Interrogatories, document requests, and depositions simply need to be tailored to use the new terminology of Bitcoin.

Examination of bank or credit card statements might reveal payments to Bitcoin exchanges (e.g., Coinbase). If they do, records can be obtained from the exchanges showing the history of all transactions. In United States v. Coinbase, Inc.,24 the IRS successfully enforced a summons (subpoena) to obtain the records of Coinbase customers. These records included transac tion logs, records of payments processed, correspondence be tween the exchange and the other spouse, amongst others.

The most direct method of obtaining the complete history of Bitcoin transactions is to obtain the private address. If a court has personal jurisdiction over the other spouse, the court can or der that spouse to provide the private address, just as a court could order them to provide account logins and passwords.

A forensic examination (with or without the private address) of the other spouse's computer, smartphone, or tablet may yield evidence of past or present use of wallet apps (e.g., Mycelium) or exchange apps (e.g., Coinbase). If the attorney is fortunate and obtains the private keys associated with the bitcoins, a forensic expert will be able to examine the blockchain and trace the movement and amount of every transaction the other spouse has made.

Once a court orders the examination of the contents of a hard drive, several considerations come into play since a party is not going to simply hand over a hard drive to the other side. Therefore, it is critical to work with a computer forensic expert to draft pleadings or stipulate to a protocol. The protocol must have search parameters such as keywords (e.g., "Bitcoin," "Mycelium") and a date range, as well as a procedure to deal with privileged communications and irrelevant data. The protocol must require the device owner to provide his or her password. Al though the world of Bitcoin is cutting-edge, as noted above, the fundamental discovery rules about breadth and scope and the use of protective orders still apply.

The shrewdest of spouses may well evade even the ablest forensic investigator by a process known as "bitcoin mixing." By using a mixing service or tumbler, such as UltraMixer or CoinMixer, the user can break the link between addresses by either creating temporary addresses or by swapping coins with other addresses of the same value. Another way people are maintaining the secrecy of cryptocurrencies is "private coins" such as Monero and Zcash. Mixers and private coins make the trail hard to follow on the blockchain.

Regarding the examination of computer devices, many clients are tempted to resort to self-help. They might search their spouse's cell phone or computer, or install key-stroking software and, in so doing, depending on the circumstances, violate state or federal privacy laws.28 Practitioners, therefore, must consider these statutes, and other applicable laws, before counselling cli ents regarding self-help.

**Discovery to the opposing party either by interrogatories or deposition should include:**

1. Do you own any form of cryptocurrency?
2. Have you ever owned any form of cryptocurrency?
3. Does anyone now, or in the past, hold any cryptocur rency for you?
4. Are any held by overseas exchanges? If yes;
5. Do you have any form of E-wallet? (generic term)
6. Have you ever had an E-wallet?
7. If you have a crypto account what exchange or ex changes do you use?
8. Which have you used in the past?
9. What is your private key?
10. What is your public key?
11. Have you reported/intend to report capital gains?
12. If not, will you be filing an amended return?

**Additionally, looking at the Order in the Coinbase case, at a minimum, document requests to Coinbase or other exchanges should include:**

1. Complete user profiles;
2. Know-your-customer due diligence;
3. Documents regarding third-party access;
4. Transaction logs;
5. Records of payments processed;
6. Correspondence between the exchange and the other spouse;
7. Account or invoice statements;
8. Records of payments.

The address for Coinbase is: Coinbase, Inc.
548 Market Street #23008
San Francisco, CA 94104

**Documents To Be Produced:**

1. All account statements solely or jointly in the name of _____.

2. All documents regarding detailed account activity for Coinbase accounts solely or jointly in the name of _____.

3. All documents regarding deposits of currency or money in Coinbase accounts solely or jointly in the name of _____.

4. All documents regarding deposits of bitcoins or cryptocur rencies in Coinbase accounts solely or jointly in the name of _____.

5. All documents regarding withdrawals of currency or money from Coinbase accounts solely or jointly in the name of _____.

6. All documents regarding withdrawals of bitcoins or cryptocurrencies from Coinbase accounts solely or jointly in the name of _____.

7. All documents regarding storing, buying, selling, trading, ex changing, sending, receiving, or using bitcoins or cryptocur rencies in Coinbase accounts solely or jointly in the name of _____.

8. All documents regarding converting or exchanging bitcoins or cryptocurrencies into currency, products, services or oth erwise in Coinbase accounts solely or jointly in the name of _____.

9. All documents regarding converting currency, products, ser vices or otherwise into bitcoins or cryptocurrencies in Coin base accounts solely or jointly in the name of _____.

10. All account opening documents for all Coinbase accounts solely or jointly in the name of _____.

11. All documents regarding the codes or identification of bitcoins or cryptocurrencies in Coinbase accounts solely or jointly in the name of _____.

12. All documents regarding wallets, blockchains, transaction I.D.' s, inputs of transactions and input keys in Coinbase ac counts solely or jointly in the name of . All documents in Coinbase's file on _____

23 Erica Driskell, Comment, Dissipation of Marital Assets and Prelimi nary Injunctions: A Preventive Approach to Safeguarding Marital Assets, 20 J. AM. ACAD. MATRIM. LAW. 135, 137 (2006). See also Segall v. Segall, 708 So.2d 983, 986 (Fla. Dist. Ct. App. 1998).

24 See United States v. Coinbase, Inc., No. 17-cv-01431-JSC, 2017-2 U.S. Tax Cas. (CCH) P50,423, 120 A.F.T.R.2d (RIA) 2017-6671, 2017 WL 5890052 (N.D. Cal. Nov. 28, 2017).

29 Bitcoin.org, https://bitcoin.org/en/vocabulary (last visited Aug. 29, 2020). 30 Id. 31 What Are Bitcoin Mixers, BITCOIN MAG. https://bitcoinmagazine.com/ guides/what-are-bitcoin-mixers (last visited July 29, 2020).

32 Bitcoinexchnageguide.com, Blockchain Glossary & Cryptocurrency Vocabulary Terms, https: //bi tcoinex changeguide .com/bl ockchain- glossa ry cryptocurrency-vocabulary-terms/#g (last visited Aug. 29, 2020); Montclair Uni versity, Course Hero, ACCT510 Class_Bitcoin and Blockchain Exercise (1).docx https://www.coursehero.com/file/52177964/ACCT510 (last visited Aug. 29, 2020). 33 Id. 34 https://coinira.com/cryptocurrency-glossary/ (last visited Aug. 29, 2020)

36 https://dash-docs.github.io/en/vocabulary (last visited Aug. 29, 2020).

37 WAYNE WALKER, THE DEFINITIVE GUIDE TO MASTERING BITCOIN & CRYPTOCURRENCIES (2018).

38 Jason Hall, Fiat Currency: What It Is and Why It's Better Than a Gold Standard, MOTLEY FOOL (Dec. 6, 2015), https://www.fool.com/investing/gen eral/2015/12/06/fiat-currency-what-it-is-and-why-its-better-than-a.aspx.

39 Bitcoins Terms/Vocabulary, BITBUY https://bitbuy.at/about-bitcoin/ terms/ (last visited Aug. 29, 2020).

40 U.S. Sentencing Commission, Bitcoin Glossary: 2018 National Seminar, https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training seminar/2018-materials/emerging-tech_glossary-crypto.pdf.

41 Id.

Janice L. Boback & Stephanie L. Tang, Cryptocurrency in Divorce Proceedings, http//i illnoislawforyou.com/property-division/cryptocurrency- divorce-proceedings/, (last visited Aug. 29, 2020).

DuaneMorris

# The Blueprint For A National Bitcoin Reserve

By Stefanie Wayco, Matthew Catania and Gregory Bailey

January 21, 2025
*Law360*

President Donald Trump is moving toward implementing a crypto-friendly administration. A clear indicator of this direction is the appointment of David Sacks as the White House artificial intelligence and crypto czar.

This appointment has fueled speculation about what the so-called crypto czar role will look like and what, if any, meaningful policymaking power it will have. Will the role lead to clearer regulation? Will Sacks serve merely as an adviser without a formal government title or authority? Will the role lead to a new reserve where the government holds and secures crypto-assets?

A U.S.-backed crypto reserve could pave the way for some desperately needed clarity in this digital space — such as which governmental body will regulate cryptocurrencies — that could chart the path for the full and complete integration of crypto into our daily spending and investment, and the adoption of blockchain technology in larger government initiatives.

Bitcoin, the most widely recognized digital asset, has been seen as the industry standard, and Trump has endorsed calls for a strategic bitcoin reserve.

The new administration has the opportunity to lead what could mark the beginning of an era defined by innovation, digital credit and the global acceptance of not just bitcoin, but also cryptocurrencies generally, whether as a security or commodity.

## *The Federal Reserve's Role*

The Federal Reserve serves as the nation's central bank, managing monetary policy, controlling inflation, regulating financial institutions, ensuring efficient payment systems and promoting consumer protection.

The hallmark of the Fed is its political independence, which allows it to focus on long-term economic stability. Part of its role requires it to work closely with other federal agencies, including the U.S. Department of the Treasury, U.S. Securities and Exchange Commission, and Federal Deposit Insurance Corp. to provide comprehensive oversight and stability.

For example, the Fed collaborates with the Treasury to manage government debt issuance and liquidity in bond markets. It works alongside the SEC to enhance financial market stability, and coordinates with the FDIC to secure deposits and maintain banking system integrity.

To achieve its goals, the Fed utilizes a range of tools, including adjusting interest rates to influence borrowing costs, conducting open market operations through the buying and selling of Treasury securities, and setting reserve requirements to ensure banks maintain sufficient liquidity.

Additionally, the Fed oversees key components of the nation's payment and settlement systems, including processing electronic payments and maintaining the currency supply.

### *A Vision for Cryptocurrency Reserves*

Trump's proposal for a crypto reserve — whether aimed at enhancing financial stability, curbing inflation, managing the national debt or fostering innovation — would require strategic collaboration, with the Fed being the most appropriate agency to pave the path forward.

Much like its role in managing traditional assets, the Fed's involvement in potential cryptocurrency reserves could shape its success, ensuring alignment with broader fiscal and monetary objectives.

In addition, the upcoming administration's embrace of crypto demonstrates its confidence in the Fed's capability to manage cryptocurrency reserves effectively.

A national crypto reserve could conceptually function as a strategic asset akin to traditional reserves like gold. Proponents argue that cryptocurrency reserves would reduce the national debt, free up U.S. dollars for other uses and position cryptocurrencies as long-term financial assets.

Such a reserve could also act as a stabilizing factor, regardless of whether the digital assets are classified as securities, commodities or currencies, and foster reliability and credibility to full faith in crypto.

### *Historical Context and Standards*

Financial standards play a pivotal role in economic stability and consumer trust. Historically, systems like the gold standard offered a fixed framework for currency valuation, tying national currencies to a specific quantity of gold.

Under this system, currencies were convertible into gold at a fixed rate, providing stability and predictability in financial markets and trade. Central banks maintained gold reserves and limited the money supply in proportion to these reserves, promoting fiscal discipline.

Today, the U.S. government guarantees various securities through its so-called full faith and credit system, guaranteeing reliability even without physical backing. This principle refers to the government's unconditional guarantee to honor its debts, bolstering confidence in government-issued securities.

For consumers, full faith and credit provides investments in instruments like Treasury bonds are backed by the government's ability to levy taxes or issue currency, offering a secure and stable form of credit and investing.

From a policy perspective, full faith and credit facilitates economic management by enabling the government to raise funds efficiently through debt issuance.

This system supports critical initiatives, such as infrastructure development and emergency relief programs, by ensuring access to capital markets. Moreover, it underpins trust in the broader financial system, providing a foundation for policies aimed at fostering economic growth and resilience.

*Project Crypto: A Plan for Regulatory Clarity*

Sen. Cynthia Lummis, R-Wyo., has championed the idea of a national bitcoin reserve.[1] Her plan envisions accumulating 1 million bitcoin over 20 years to hedge against inflation and complement the U.S. dollar.

The proposal involves converting Fed gold certificates into bitcoin and establishing a strategic reserve with a 20-year minimum hold period.

Future cryptocurrency frameworks must address property rights, ownership protection, secure custody solutions, and most importantly, which agency regulates cryptocurrencies, as well as when, and how, it is categorized as a security under SEC v. Howey[2] — decided in 1946 by the U.S. Supreme Court — or a commodity.

The Lummis bill addresses these regulatory challenges, proposing clearer distinctions between securities and commodities to simplify compliance for crypto businesses. The bill includes specific funding mechanisms and regulatory frameworks, shifting oversight from the SEC to the U.S. Commodity Futures Trading Commission for certain crypto-assets.

With the surge of cryptocurrency, courts have grappled with whether certain digital assets qualify as a security or a commodity.[3] The blurred line here has drawn various distinctions and confusing standards for the industry to follow.[4] A clearer regulatory framework for digital assets as a whole, and one that embraces cryptocurrencies in a defined manner, is essential.

The Howey test will continue to apply, but the 1946 test has become antiquated when it comes to cryptocurrencies — something the courts back then could not have envisioned.

Although a digital asset is not in and of itself a security, the new administration's voice for acceptance of the crypto industry at large, and an embrace of cryptocurrency reserves, could push for a new regulatory framework that clarifies the blurred lines of securities and commodities.

Clearer legal standards and frameworks would make companies more equipped to operate their exchanges to offer cryptocurrencies; allow institutions to invest; allow consumers to be able to buy, sell and use digital assets without uncertainty; and continue the acceptance of the full faith in crypto.

*Strategic Petroleum Reserve as a Model*

The U.S. Department of Energy demonstrates how government-maintained commodity reserves can influence markets and policy through its management of the Strategic Petroleum Reserve.

Although the SPR is relevant to energy companies maintaining reserves and indirectly to broader consumers, which differs from the crypto industry, it serves as a foundational model to begin framing cryptocurrency reserves.

The SPR is used to stabilize oil prices, offset budget deficits and generate revenue, and provides leverage in global markets. Similar to how the SPR affects energy markets and inflation, cryptocurrency reserves could affect digital asset markets and monetary policy.

While the DOE manages day-to-day operations, the president may order directives for releases of the reserves. Congress may authorize the sale of oil from the SPR to fund government spending or to respond to emergencies and legislative mandates, such as periodic sales, and influence reserve levels.

Therefore, the SPR affects financial and monetary policy, including stabilizing oil prices, as well as energy commodities and inflation expectations.

Similarly, cryptocurrency reserves could stabilize crypto markets, hedge against economic instability and influence global crypto adoption. Just as Congress authorizes SPR sales to fund government initiatives, legislative mandates could dictate crypto reserve usage.

With a bitcoin reserve, the Fed would act similar to the SPR, and the CFTC could manage the underlying assets like the DOE, being the regulatory enforcement and governing body.

The Fed would strategically influence crypto-related policies, as well as manage and stabilize government crypto funds. It could also ensure an excess is available to offset budgets and generate revenue, and protect consumers' underlying interest.

The Fed would also continue its ability to set rates, borrow and fund government projects, all while collateralizing cryptocurrencies.

Lummis' bill addresses that the Treasury would play a role in managing and securing a bitcoin reserve, just as the Treasury collaborates now with the Fed.

Proposals for decentralized vault systems managed by the Treasury could provide secure storage for national cryptocurrency reserves, which could address ownership and custody issues while ensuring transparency and accountability, in line with the public's growing acceptance of full faith in crypto.

The prospect of a national crypto reserve reflects a transformative vision for the U.S. economy, blending traditional financial principles with emerging digital technologies.

However, the evolution in cryptocurrency policy represents a significant shift from bitcoin's original decentralized vision, for example, to a more regulated, government-integrated future.

The challenges lie in maintaining consumer efficiency to use, invest and innovate digital assets while balancing the decentralized historical concept.

Even with a decentralized focus, the growth of the industry has reached a point where there are calls for oversight and limited government intervention to provide regulatory guidance, which has become necessary given the vague legal standards and the need for consumer protection mechanisms. A full faith in crypto under the new administration sees the value in setting the stage.

Development is needed to set rules for everyone to play the game.

By embracing cryptocurrency, the new administration has the potential to develop a future defined by innovation, stability and global leadership in the digital asset space. Whether through federal initiatives, state-level efforts or regulatory reforms, the U.S. is poised to navigate this new frontier with strategic foresight and adaptability.

Congressional approval faces calls from lawmakers concerned about economic stability and inflation, while ongoing regulatory uncertainty and public skepticism could impede progress. The new administration's ability to balance efficiency and innovation with appropriate oversight will determine the success of any national cryptocurrency reserves and the crypto industry at large in the U.S.

Notably, as other nations adopt cryptocurrency policies, the U.S. risks falling behind without proactive measures. Establishing cryptocurrency reserves and implementing supportive regulations could solidify the U.S.' leadership in the global crypto economy, driving innovation and investment.

The U.S. has consistently held itself to high standards for consumer protection, data security and financial trading, and as the leader in capital markets.

Thus, if other countries progress ahead, there are risks of less stable policies protecting digital assets, and the U.S. should set forth its full faith in crypto as the crypto capital of the world.

Stefanie Wayco is a partner, Matthew Catania is a senior associate and Gregory Bailey is an associate at Duane Morris LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Full text of the previously proposed bill is available here: https://www.congress.gov/bill/118th-congress/senate-bill/4912/text. Sen. Lummis is expected to reintroduce the bill during the new administration. See Zach Halaschak, Lummis plans renewed push for strategic bitcoin reserve after Trump win, Wash. Examiner, Nov. 22, 2024, https://www.washingtonexaminer.com/policy/finance-and-economy/3237933/lummis-renewed-push-strategic-bitcoin-reserve/#google_vignette.

[2] SEC v. W.J. Howey Co. , 328 U.S. 293 (1946). The United States Supreme Court defined an investment contract, or a security, in Howey as an investment of money, in a common enterprise, with an expectation of profits or losses from the efforts of others. Id.

[3] See, e.g., SEC v. Ripple Labs Inc. , 682 F.Supp.3d 308 (S.D.N.Y. 2023); SEC v. Terraform Labs Pte. Ltd. , 684 F.Supp.3d 170 (S.D.N.Y. 2023); SEC v. Payward Inc. , 2024 WL 4511499 (N.D. Cal. Aug. 23, 2024).

[4] See, e.g., Terraform Labs Pte. Ltd., 684 F. Supp. 3d at 191 (noting SEC's view "that some cryptocurrencies may fall within the regulatory ambit of federal securities laws.") (emphasis added); Ripple Labs, 682 F. Supp. 3d at 324 (a digital asset "is not in and of itself" an investment contract under Howey).

*Reprinted with permission of Law360.*

Stefanie Wayco
+1 404 253 6914
SMWayco@duanemorris.com

Matthew A. Catania
+1 215 979 1954
MACatania@duanemorris.com

Gregory Bailey
+1 215 979 1213
GBailey@duanemorris.com

# Glossary

**Address**

A Bitcoin address, or key (see private key below) refers to either public or private addresses. Public addresses are used to send and receive bitcoins. A crucial difference, however, is that each address should only be used for a single transaction

**Bit**

A bit is one one-millionth of 1 bitcoin, or 1,000,000 bits equals 1 bitcoin. A bitcoin can also be divided to 8 decimal places or 0.00000001 bitcoin, is called a satoshi. This is important because, for a currency to be useful it must be easily divisible.

**Bitcoin**

When capitalized "Bitcoin" refers to open source software used to create the bitcoin virtual currency and the peer-to-peer net work formed as a result. The individual units of the bitcoin vir tual currency (when lowercase). e.g., "I sent ten bitcoins today"; it is also often abbreviated BTC or XBT.

**Bitcoin mixing**

Bitcoin mixers are solutions (software or services) that let users mix their coins with other users, in order to preserve their privacy.

**Block**

These are where all the details of transactions are stored. All transactions recorded in the block are considered immutable they cannot be altered – and transparent. This way, users can see where they were recorded, and which transactions took place. Once a block is full, all new transactions are automatically moved to a new block and so on.

**Blockchain**

The block chain is a "public record of Bitcoin transactions in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending.

**BTC**

"BTC is a common unit used to designate one bitcoin."

**Confirmation**

"Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like $1,000, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a re versed transaction."

**Convertible Virtual Currency**

Virtual currency that has an equivalent value in real currency or that acts as a substitute for real currency.

**Cryptography**

Cryptography is the branch of mathematics that lets us cre ate mathematical proofs that provide high levels of security. On- line commerce and banking already use cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

**Double Spend**

"If a malicious user tries to spend their bitcoins to two different recipients at the same time, this is double spending. Bitcoin min ing and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid."

**Fiat Currency**

Fiat currency is "legal tender whose value is backed by the gov ernment that issued it. The U.S. dollar is fiat money, as are the euro and many other major world currencies. This approach dif fers from money whose value is underpinned by some physical good such as gold or silver, called commodity money."38

**Mining**

Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a spe cialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an effortless way to make money.

**P2P**

"Peer-to-peer refers to systems that work like an organized collective by allowing everyone to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party."

**Private Key**

A private key is "a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic sig nature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

**Signature**

A cryptographic signature "is a mathematical mechanism that al lows someone to prove ownership. In the case of bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathe matical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard earned bitcoins."

**Wallet**

A Bitcoin wallet is "loosely the equivalent of a physical wallet on the Bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in the blockchain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where the merchant charges you.

# Pennsylvania House of Representatives

https://www.legis.state.pa.us/cfdocs/legis/RC/Public/rc_view_action2.cfm?sess_yr=2023&sess_ind=0&rc_body=H&rc_nbr=1609

**02/03/2025 12:40 PM**



# House Roll Calls

RSS Available

## House of Representatives
## Session of 2023-2024 Regular Session

**Details for RCS No. 1609**

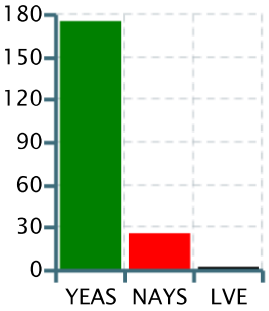
Wednesday Oct. 23, 2024

12:16PM

House Bill 2481 PN 3791
FINAL PASSAGE

**Summary**

| | | |
|---|---|---|
| Y | YEAS | 176 |
| N | NAYS | 26 |
| E | LVE | 1 |
| X | N/V | 0 |
| | TOTAL | 203 |




**Prime Sponsor**

CABELL

**Short Title**

An Act providing for restriction on use and custody of digital assets prohibited and for use of nodes authorized.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Y | ARMANINI | Y | LEADBETER | Y | BELLMON | Y | KRAJEWSKI |
| Y | BANTA | Y | MACKENZIE, M. | N | BENHAM | Y | KRUEGER |
| Y | BARTON | Y | MACKENZIE, R. | Y | BIZZARRO | Y | KULIK |
| Y | BENNINGHOFF | Y | MAJOR | Y | BOROWSKI | Y | MADDEN |
| Y | BERNSTINE | Y | MAKO | Y | BOYD | Y | MADSEN |
| Y | BONNER | Y | MALONEY | Y | BOYLE | Y | MALAGARI |
| Y | BOROWICZ | Y | MARCELL | Y | BRADFORD | Y | MARKOSEK |
| Y | BROWN, M. | Y | MARSHALL | N | BRENNAN | Y | MATZIE |
| Y | CABELL | Y | MEHAFFIE | Y | BRIGGS | N | MAYES |
| Y | CAUSER | Y | MENTZER | Y | BROWN, A. | Y | MCANDREW |
| Y | COOK | Y | MERCURI | N | BURGOS | Y | MCNEILL |
| Y | COOPER | Y | METZGAR | Y | BURNS | Y | MERSKI |
| Y | CUTLER | Y | MIHALEK | Y | C FREYTIZ | Y | MILLER, D. |
| Y | D'ORSIE | Y | MILLER, B. | Y | CARROLL | Y | MULLINS |
| Y | DAVANZO | Y | MOUL | Y | CEPHAS | Y | MUNROE |
| Y | DELOZIER | Y | MUSTELLO | Y | CERRATO | Y | NEILSON |
| Y | DIAMOND | Y | NELSON, E. | Y | CIRESI | Y | NELSON, N. |
| Y | DUNBAR | Y | O'NEAL | Y | CONKLIN | Y | O'MARA |
| Y | ECKER | Y | OBERLANDER | Y | CURRY | N | OTTEN |
| Y | EMRICK | Y | OLSOMMER | N | DALEY | Y | PARKER |
| Y | FEE | Y | ORTITAY | Y | DAVIS | Y | PASHINSKI |
| Y | FINK | Y | OWLETT | Y | DAWKINS | Y | PIELLI |
| Y | FLICK | Y | PICKETT | Y | DEASY | Y | PISCIOTTANO |
| Y | FLOOD | Y | RADER | Y | DELLOSO | Y | POWELL |
| Y | FRITZ | Y | RAPP | Y | DONAHUE | Y | PROBST |
| Y | GAYDOS | Y | RIGBY | Y | EVANS | Y | PROKOPIAK |
| Y | GILLEN | Y | ROAE | N | FIEDLER | Y | RABB |
| Y | GLEIM | Y | ROSSI | Y | FLEMING | Y | ROZZI |
| Y | GREGORY | Y | ROWE | Y | FRANKEL | Y | SALISBURY |
| Y | GREINER | Y | RYNCAVAGE | N | FREEMAN | N | SAMUELSON |
| Y | GROVE | Y | SCHEMEL | Y | FRIEL | Y | SANCHEZ |
| Y | HAMM | Y | SCHEUREN | Y | GALLAGHER | N | SAPPEY |
| Y | HEFFLEY | Y | SCHLEGEL | Y | GERGELY | Y | SCHLOSSBERG |
| Y | HOGAN | Y | SCHMITT | Y | GIRAL | Y | SCHWEYER |
| Y | IRVIN | Y | SCIALABBA | N | GREEN | Y | SCOTT |
| Y | JAMES | Y | SMITH | Y | GUENST | N | SHUSTERMAN |
| Y | JONES, M. | Y | STAATS | Y | GUZMAN | Y | SIEGEL |
| Y | JONES, T. | Y | STAMBAUGH | Y | HADDOCK | Y | SMITH-WADE-EL |
| Y | JOZWIAK | Y | STEHR | Y | HANBIDGE | Y | SOLOMON |
| Y | KAIL | Y | STENDER | Y | HARKINS | N | STEELE |
| Y | KAUFER | Y | STRUZZI | Y | HARRIS, J. | N | STURLA |
| Y | KAUFFMAN | Y | TOMLINSON | Y | HARRIS, K. | N | TAKAC |
| Y | KEEFER | Y | TOPPER | N | HOHENSTEIN | N | VENKAT |
| Y | KEPHART | Y | TWARDZIK | N | HOWARD | N | VITALI |
| E | KERWIN | Y | WARNER | N | ISAACSON | N | WARREN |
| Y | KLUNK | Y | WATRO | Y | KAZEEM | N | WAXMAN |
| Y | KRUPA | Y | WENTLING | Y | KENYATTA | Y | WEBSTER |
| Y | KUTZ | Y | WHITE | N | KHAN | N | WILLIAMS, D. |
| Y | KUZMA | Y | WILLIAMS, C. | Y | KIM | Y | YOUNG |
| Y | LABS | Y | ZIMMERMAN | N | KINKEAD | | |
| Y | LAWRENCE | N | ABNEY | Y | KOSIEROWSKI | Y | MCCLINTON |

# Pennsylvania introduces bill to implement strategic bitcoin reserve

By Micah Zimmerman November 14, 2024 at 6:14 pm Edited by Jayson Derrick



Pennsylvania's legislature has introduced a bill allowing the state to invest in Bitcoin.

Led by Representative Mike Cabell, this bill would permit Penns three state funds — the General Fund, Rainy Day Fund, and Sta BTC 1.53% .

Cabell argues that Bitcoin could act as a hedge against inflatior economy amid economic volatility.

You might also like:
DOJ investigates Polymarket over alleged U.S. user participation

## Pro-Bitcoin sentiment across the United States

This proposed legislation comes amid a nationwide pro-Bitcoin sentiment, with discussions about creating a national Bitcoin reserve should President-elect Donald Trump take office.

Trump's campaign has advocated for making the U.S. the "crypto capital of the planet," leading to speculation about Bitcoin's potential role in the federal government.

Cabell cited the moves of major firms like BlackRock and Fidelity as examples, highlighting Bitcoin's appeal for its potential to add stability to investment portfolios.

This legislation follows Pennsylvania's recent Bitcoin Rights bill, which passed the House. If signed into law, that bill would ensure residents' rights to hold digital assets securely.

You might also like:
Crypto whales eye PEPE at $2, but experts predict WallitIQ will hit $15 by 2024's end

## related news


**MicroStrategy halts Bitcoin buying spree after 12 straight weeks**

BTC

53 minutes ago


**Bybit CEO estimates crypto wipeout crossed $8b, more than $2b reported**

3 hours ago


**Russian gang ta platform spear-**

3 hours ago

## sign up for crypto news and market insights

Get crypto market analysis and curated news delivered right to your inbox every week.

Enter your email address subscribe

# SAMPLE

THE COUNSEL, ESQUIRE
Attorney ID No.
THE FIRM
123 Sesame Street, St.456
Philadelphia, PA 19107
(000) 000-0000

*Attorney for Plaintiff*

| | | |
|---|---|---|
| PLAINTIFF<br>789 Summer Drive<br>Somewhere , PA 19426 | : | COURT OF COMMON PLEAS<br>MONTGOMERY COUNTY |
| | : | FAMILY DIVISION |
| *Plaintiff* | : | |
| vs. | : | |
| DEFENDANT<br>1011 Fall Drive<br>Somewhere Else , PA 12345 | : | NO.<br><br>IN DIVORCE |
| *Defendant* | : | |

PLAINTIFF'S FIRST SET OF INTERROGATORIES FOR DEFENDANT

**TO:**

C/O …….., Esquire

Please take notice that demand is hereby made upon you for answers under oath or certification to the following Interrogatories within the time and in the manner prescribed by the rules of this Court. You are required to answer the following Interrogatories within thirty (30) days after service upon you pursuant to the Rules of Civil Procedure.

## Definitions and Instructions

Unless negated by the context of the Interrogatory, the following definitions are to be considered to be applicable to all Interrogatories contained herein:

(A) "Documents" is an all-inclusive term referring to any writing and/or recorded or graphic matter, however produced or reproduced. The term "documents" includes, without limitation, correspondence, memoranda, inter-office communications, minutes, reports, notices, schedules, analyses, drawings, diagrams, tables, graphs, charts, maps, surveys, books of account, ledgers, invoices, purchase orders, pleadings, questionnaires, contracts, bills, checks, drafts, diaries, logs, proposals, print-outs, recordings, telegrams, films, tax returns, and financial statements, computer discs, electronic data processing records and all other such materials tangible or retrievable, of any kind. "Documents" also include any preliminary notes and drafts of all the foregoing, in whatever form, for example, printed, typed, longhand or shorthand, on paper, paper tape, tabulating cards, ribbon blueprints, magnetic tape, microfilm, film, motion picture film, phonograph records, or other form.

(B) The term "identify" means, with respect to documents:

(1) To give the date, title, author and addressee;

(2) To describe a document sufficiently well to enable the interrogator to know what the document is and to retrieve it from a file or wherever it may be located;

(3) To describe it in a manner suitable for use as a description in a subpoena; and

(4) To give the name, address, position or title of the person(s) who has custody of the document and/or copies thereof.

(C) "Identify" when used in reference to an individual means:

(1) To state his or her full name;

(2) Present residence address or last known address;

(3) Present or last known business address;

(4) Present employer or last known employer; and

(5) Whether ever employed by any party to this action, and if so, the dates he or she was employed by that party, the name of the party, and the last position held as an employee of the party.

(D) Whenever the expression "and/or" is used in these Interrogatories, the information called for should be set out in both conjunctive and disjunctive, and whenever the information is set out in the disjunctive, it is to be given separately for each and every element sought.

(E) Whenever a date, amount, or other computation or figure is requested, the exact date, amount or other computation or figure is to be given unless it is not known; and then, the approximate date, amount or other computation or figure should be given or the best estimate thereof; and the answer shall state that the date, amount or other computation or figure is an estimate or approximation.

(F) No answer is to be left blank. If the answer to an Interrogatory or subparagraph of an Interrogatory is "none" or "unknown," such statement must be written in the answer. If the question is inapplicable, "N/A" must be written in the answer. If an answer is omitted because of the claim of privilege, the basis of privilege is to be stated.

(G) These Interrogatories are continuing and any information secured subsequent to the filing of your answers which would have been includable in the answers had it been known or available, is to be supplied by supplemental answers.

(H) Attach such additional sheets as are necessary to completely answer each interrogatory.

INTERROGATORY NO. 1. Do you or have you had in the past ten (10) years, whether held by you or for your benefit, any of the following:

A. Balances on any money transfer software applications including but not limited to Paypal, Dwolla, Venmo, Cashapp, held in your name or for your benefit.

B. Virtual Currencies including but not limited to blockchain based currencies, airline miles, mileage points or online game currency held in your name or for your benefit.

C. Digital Currencies including but not limited to Bitcoin, Ethereum, Dogecoin, and Ripple, held in your name or for your benefit.

D. Hardware or software purchased or constructed for the purpose, of or that was ultimately used for the purpose of, "mining" or earning, electronic currency including but not limited to Bitcoin, Ethereum, Dogecoin, etc.

E. Accounts with Coinbase, Coinbase Pro, Kraken, Binance, or any other online currency exchange.

ANSWER NO. 1.

INTERROGATORY NO. 2. If you answered “yes” to any of the questions in the preceding interrogatory, please provide the following information for each of said balances or currencies:
A. Type of Account/Software Currency

B. Name and Address of Institution/Account Manager/Software/Exchange

C. Account Number/Wallet Address

D. Present Balance

E. Present Value in USD ($)

F. When Obtained

G. Username, Password, Private Key

ANSWER NO. 2.

INTERROGATORY NO. 3. Identify any people or business with whom you have transacted in the past ten (10) years to send or receive any money or monetary value through payment applications, virtual currencies or digital currencies, including but not limited to purchases, online exchanges, automated teller machines, online services or local businesses.

ANSWER NO. 3.

INTERROGATORY NO. 4. For each person or business listed in the preceding interrogatory, please provide the following information:

A. When the transaction(s) took place.

B. What was obtained by your in the transaction.

C. What payment application or currency was used.

D. What number of units of the currency were involved.

ANSWER NO. 4.

INTERROGATORY NO. 5. Do you or have you in the past ten (10) years stored any virtual currencies, digital currencies, payment applications or any related information (including items such as Bitcoin, Software or hardware Wallets, or Venmo software) on any computer, phone or portable storage devices you possess?

ANSWER NO. 5.

REQUEST NO. 1: Please provide all electronically stored information regarding any payment application, virtual currency or digital currency, in your possession or held by someone else for your benefit including, but not limited to, Bitcoin software or hardware wallets, Venmo software or frequent flyer miles.

RESPONSE NO. 1:

REQUEST NO. 2: Please provide all documents or electronically stored information with account transaction histories regarding any application, virtual currency or digital currency, including, but not limited to, any lists of transactions with any online exchanges or phone software.

RESPONSE NO. 2:

REQUEST NO. 3: Please provide any documents you provided to the IRS or any state tax authority regarding virtual currencies or digital currencies, including, but not limited to, reporting of foreign accounts and reporting of capital gains.

RESPONSE NO. 3:

REQUEST NO. 4: Please list the details of and physical location of any servers which you own, lease, or control.

RESPONSE NO. 4:

**Verification**

I,……., hereby verify that the answers to the foregoing Interrogatories are true, correct, and complete. I understand that false statements therein are made subject to the penalties of 18 Pa. C. S. §4904, relating to unsworn falsification to authorities.

_____ _____

Date ……., Defendant