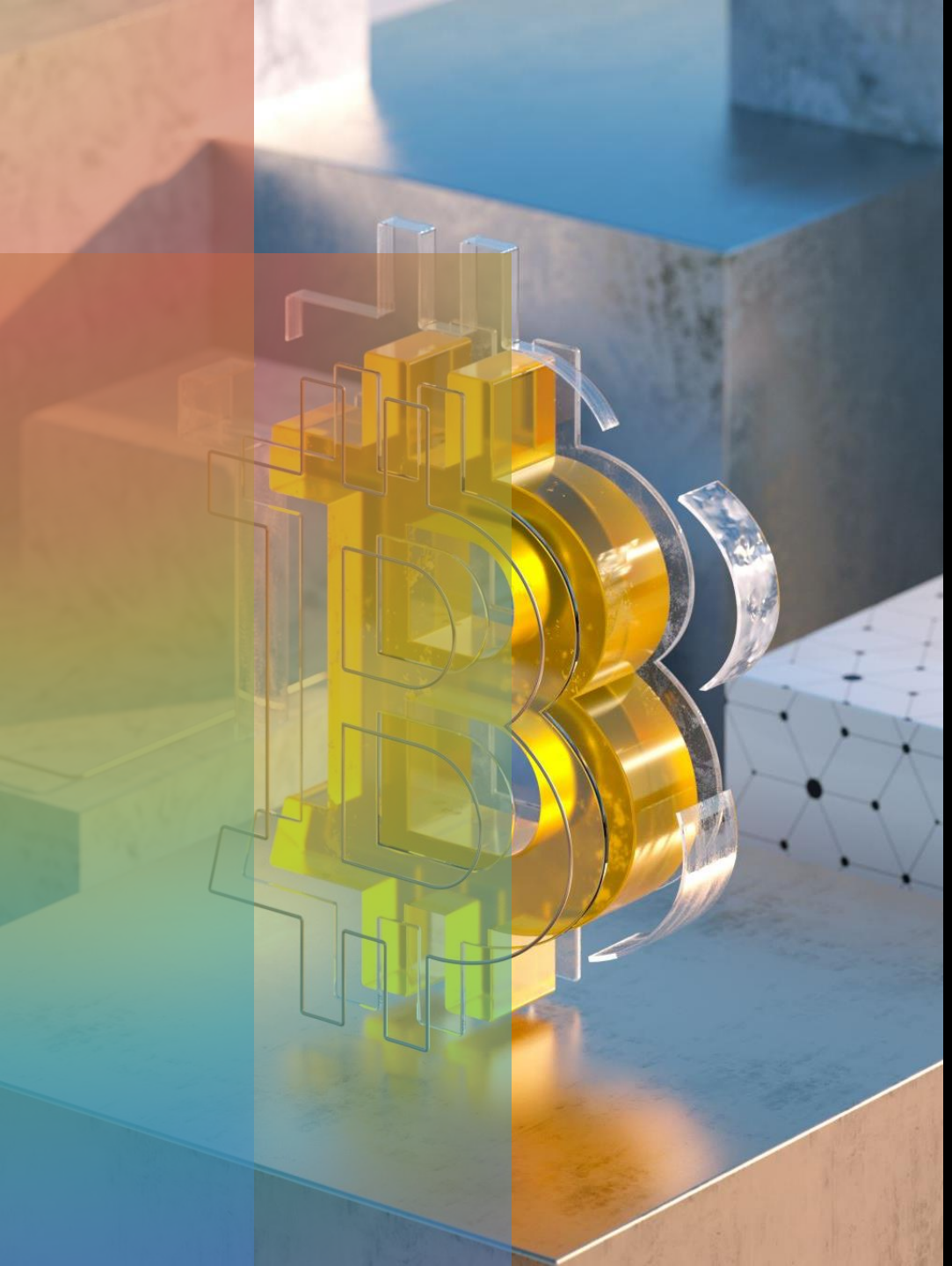


Cryptocurrency 101

A Basic Understanding and History of Cryptocurrency by David Pace

The History of Cryptocurrency

1983

- David Chaum first conceives of the idea of digital encrypted money
- He would later attempt to implement his idea in 1995 with Digicash

1996

- The NSA releases a report titled “How to Make a Mint: the Cryptography of Anonymous Electronic Cash”
- First government analysis of a potential cryptocurrency system

1997

- Adam Back proposes hashcash, a proof of work scheme to reduce spam
- The idea was to make all emails do some proof of work function to make the cost of sending spam unprofitable

1998

- Wei Dai publishes “b-money,” it is the first mention of using proof of work as a means of maintaining the digital currency system
- Digicash files for bankruptcy

History Continued

1998

- Nick Szabo designs a mechanism for his theoretical cryptocurrency called “bit gold”
- This mechanism solves the double spending problem in cryptocurrency

2008

- A person calling themself Satoshi Nakamoto publishes a paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”
- Earlier that year, the domain bitcoin.org was registered

2009

- On January 3, the bitcoin network came into existence
- Satoshi Nakamoto mines the genesis block of bitcoin and receives 50 bitcoin as his reward

2009

- The world’s first bitcoin transaction occurs on January 12 between Satoshi Nakamoto and U.S. computer programmer Hal Finney
- Nick Szabo and Wei Dai were early supporters of bitcoin

Who is Satoshi Nakamoto?

The Suspects

David Chaum

- Origin of the idea of cryptocurrency
- Attempted to implement it once

Adam Back

- First implementation of Proof of Work schemes. Active on Cypherpunk forum as well

Wei Dai

- Active on Cypherpunk forum and wrote “b-money”

Nick Szabo

- Bit gold developer and active on Cypherpunk forum.

Someone Else

- Or all of these guys

Does Anyone Know Who Satoshi is?

- Maybe, it is believed in the FBI knows who he is
- If Satoshi is a single individual, then it is likely that he owns roughly 1 million bitcoin (worth $23 billion as of August 2022) making him one of the richest people on earth.
- He is either a group of people or one of the greatest programmer who ever lived

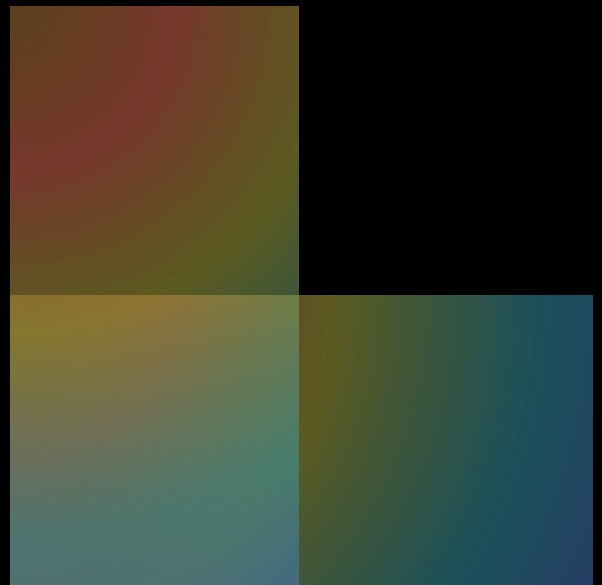
Why Bitcoin?

- Push the limits of computing
- Desire to bring back anonymity in the computing space
- Hatred of banks
  - Genesis block “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

How Does Bitcoin Work?

- Double Spending Problem: How to stop someone from copying and pasting a digital asset?
  - Proof of Work by the network solves this problem, this is what miners do.
- Miners either solve equations or verify transactions to maintain Proof of Work ecosystem.
- The bitcoin itself is a block of data
- Every time that bitcoin is transacted, the miners add another chain of data to the block
- This is the origin of “the blockchain,” also known as the distributed ledger

What Happens if There is a Problem With the Blockchain?



In August of 2010, the first, and so far only, vulnerability in bitcoin was discovered.

Bitcoin's smallest unit is the Satoshi (0.00000001 BTC)

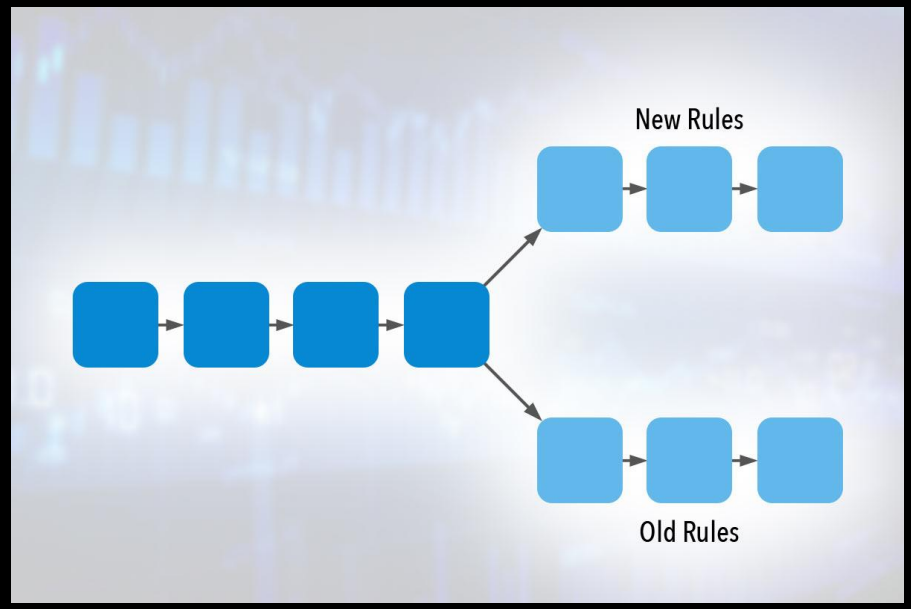
This is the base unit that mining BTC is done in

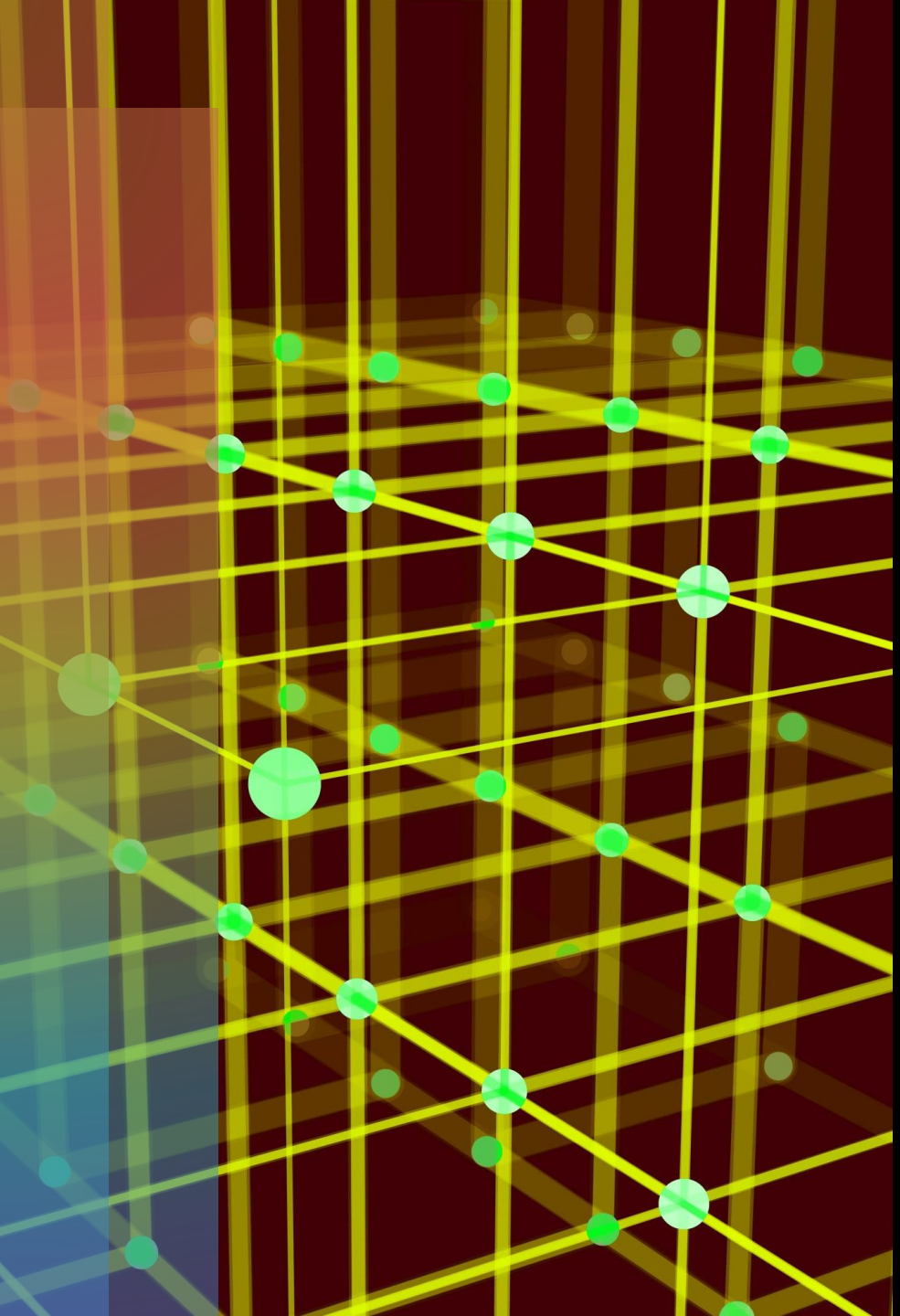
The original bitcoin code had an overflow vulnerability where a transaction that summed up to more than 2^{64} Satoshis would cause an overflow error, allowing the sender to send as many bitcoin as they wanted.

This vulnerability was exploited on August 6th, 2010, when an anonymous sender spent 0.5 BTC to send 92 billion bitcoin (2^{63} Satoshis) to 2 wallets

Forking the Blockchain

- Within hours this transaction was noticed by miners all around the world
- A patch was quickly developed and implemented into the bitcoin code.
- The blockchain was then forked by the miners to a state from before the 92 billion bitcoin was sent.
- The new forked blockchain can still trace its way back to the genesis block but the transactions from those few hours are no longer part of the bitcoin network





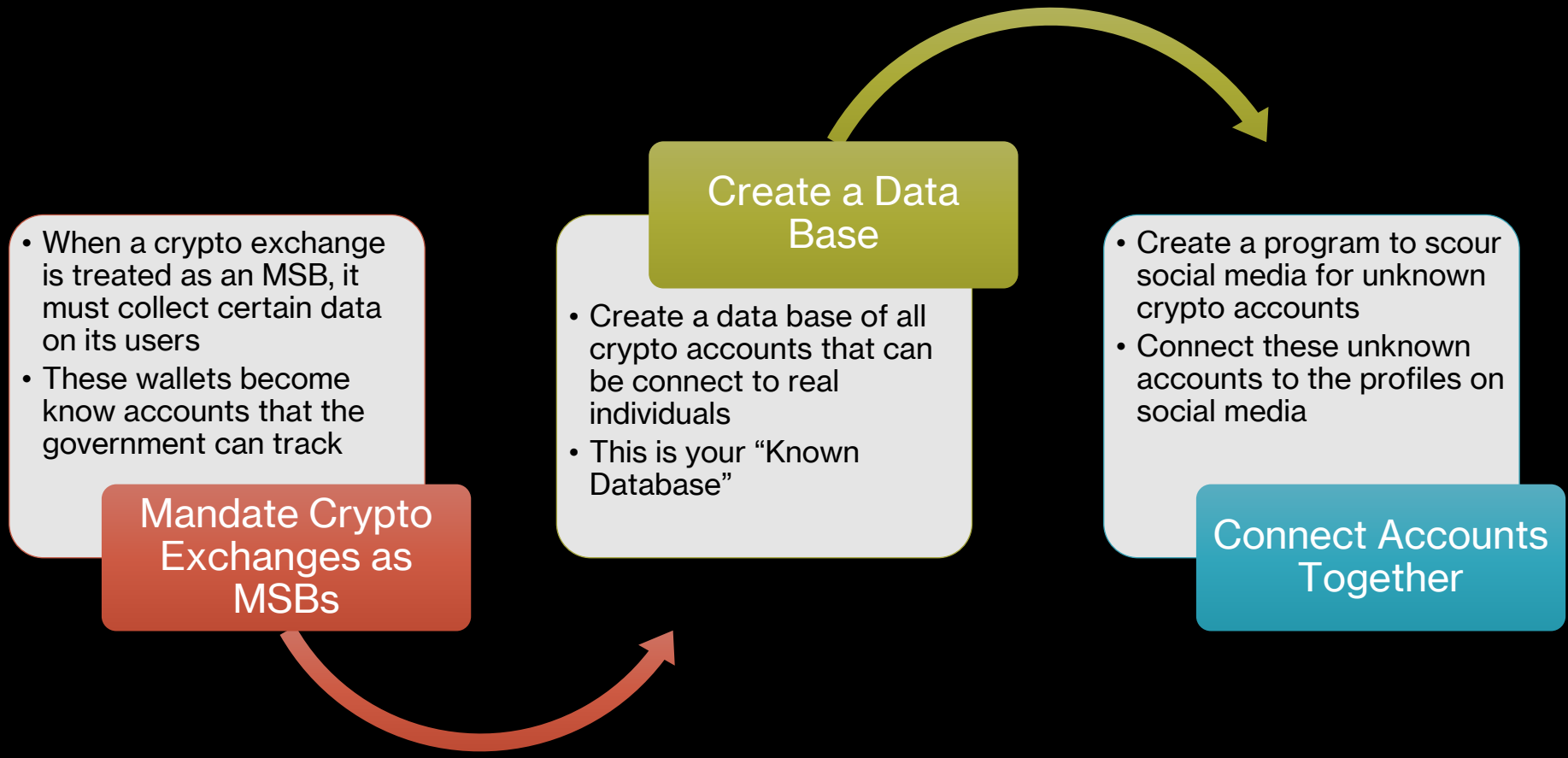
Decentralization

- Forking requires a consensus of the miners in order to happen
- This is because bitcoin is decentralized and anonymized at its very core.
- Early writing on cryptocurrency originally envisioned the central bank controlling the process due to the amount of computing power involved.
- Decentralized coins got around this by rewarding miners for their efforts.

The Government and Cryptocurrency

- The combination of anonymity and decentralization has made crypto a major headache for the government
- Unmasking crypto wallets has been an important goal of the government for years now.

How to Unmask a Crypto Wallet



How Unmasking Works

Step 1: Identify a Criminal Wallet	• Terrorists and certain criminals will publish their bitcoin wallet address to receive support • How to go to jail - Send BTC here: 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf – BTC Wallet of ISIS
Step 2: Identify Those Sending Money to Criminal Wallet	• Look for key phrases like, “I love terrorism and plan on sending ISIS $30” • Connect these phrases to transactions going to known criminal wallets
Step 3: Expand the Web	• Connect the sender to their friends and family on social media and see if their BTC wallet can be tied to any others. • Repeat steps 1 and 2 until you know as many anonymous BTC wallets as possible.

Reversing Transactions

- Bitcoin transactions were designed to be unreversible, the only time a transaction could be said to be reversed is when the code is being forked (and even then, miners strive to never reverse transactions).
- The government may have found a way to reverse these transactions though (Colonial Pipeline)
  - Worm? (like Stuxnet)
  - Supercomputer? (that we don’t know about)
  - Cut a deal? (Work with the largest mining companies to reverse the transaction)

Long Term Risks to Cryptocurrency

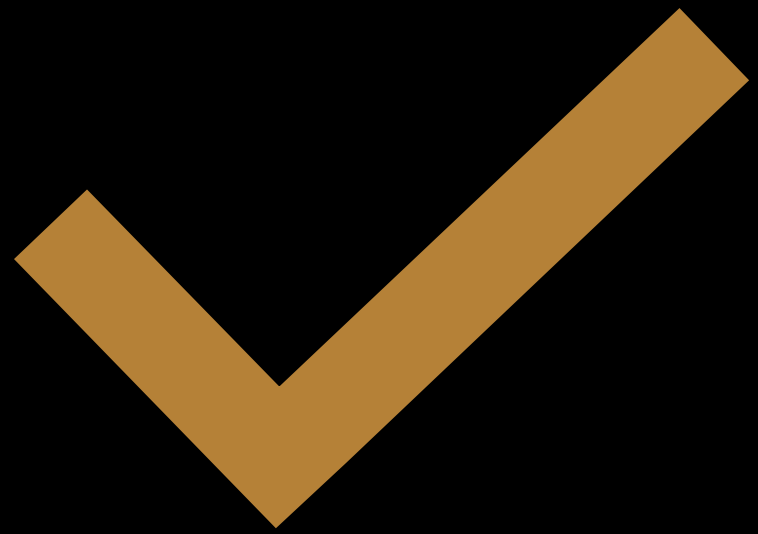
- Single miner controlling 50% of the network
- Quantum Computing
  - The Million Qubit Machine
- Loss of Anonymity
- Government Regulation
  - China

Why This Matters to You

- Cryptocurrency is not going away
- Your members are already using it in some shape or form.
- It is a major vector for fraud and money laundering
- At the very least YOU MUST BE AWARE

Actions You Can Take

- Be aware of high-risk exchanges that do not have KYC
  - Bitcoin ATMs (Atlanta Based Bitcoin Depot)
  - Anonymous Exhanges
    - ECOS (Based in Armenia)
    - CoinSmart (Based in Canada)
    - CoinGate (Based in Lithuania)
- Monitor accounts that engage in cryptocurrency
- Not all crypto transactions are suspect though
- Coinbase is a prominent American exchange that must follow BSA rules and regulations.
- If you aren’t certain about an exchange, check to see if they are registered as an MSB in your state.



Do you Want to Host Crypto Accounts?

- NCUA Letter 22-CU-7 allows for the following:
  - A credit union may use distributed ledger technology (DLT), it can be either procured from outside the credit union or developed internally
  - A credit union may partner with a third-party vendor to utilize DLT or to provide crypto services
  - It is ultimately the responsibility of the credit union to ensure that any service they or a third-party provides is in line with applicable laws and regulations
  - It is the duty of the credit union to monitor the following risks:
    - Legal and Compliance
    - Strategic and Reputational
    - Liquidity
    - Third-Party Risks

Thank you!

Questions?

How to reach me:

Email: david.pace@lscu.coop

Phone: 678-542-3419