INTRODUCTION TO CRYPTOCURRENCY

Presented by Mike Gallagher CRCM, CCAS, CAMS, CAFP
Chief BSA Officer – VersaBank USA

AGENDA

Intro to the Blockchain

Miners, Validators, and Nodes

Cryptocurrencies (Coins, Tokens, Stablecoins, Altcoins, and Tokenization)

Wallets – Keys (Private/Public), Digital, Seed Phrases, Wallet types (Hot v Cold)

VASPs – e.g., Coinbase/Crypto.com, Applications (PayPal/Venmo), Decentralized Exchanges (Uniswaps, Pancakeswap, Hyperliquid, ORCA)

Decentralized vs. Centralized blockchain

Smart Contracts

Blockchain Tools

Meme Coins and Trading

Crypto ATMS

INTRO TO THE BLOCKCHAIN

WHO KEEPS A BLOCKCHAIN RUNNING?

Three kinds of participants check the transactions and keep the shared record honest.

Miners

The workers. Powerful computers race to solve a puzzle. The winner adds the next batch of transactions and earns new coins.

Example: Bitcoin

Validators

The stakers. Instead of racing, they lock up their own crypto as a deposit to earn the right to approve transactions. Cheat, and they lose it.

Example: Ethereum

Nodes

The record keepers. Thousands of computers each hold a full copy of the ledger and check every transaction, so no one party is in control.

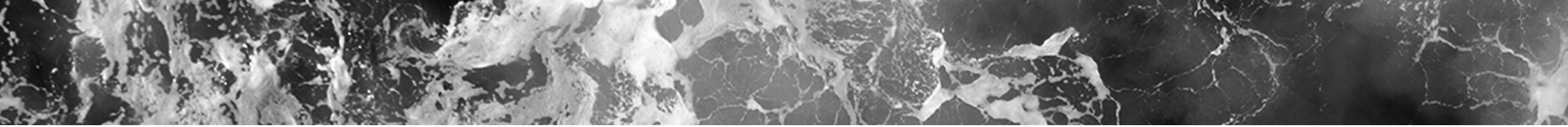
The backbone of the network

MINERS, VALIDATORS, AND NODES

Miners – A crypto miner is a participant in a blockchain network who uses specialized computing power to verify transactions, add new blocks to the blockchain, and earn cryptocurrency rewards. (PoW – Bitcoin)

Validators – A crypto validator is a participant in a Proof-of-Stake blockchain responsible for verifying transactions, proposing new blocks, and maintaining network security by staking cryptocurrency. (PoS – Ethereum)

Nodes - A **blockchain node** is any device running the blockchain's protocol software, connected to the network, and participating in maintaining the ledger. Nodes validate transactions, store blockchain data, and ensure consensus across the decentralized system, making them the backbone of blockchain infrastructure.



CRYPTOCURRENCIES

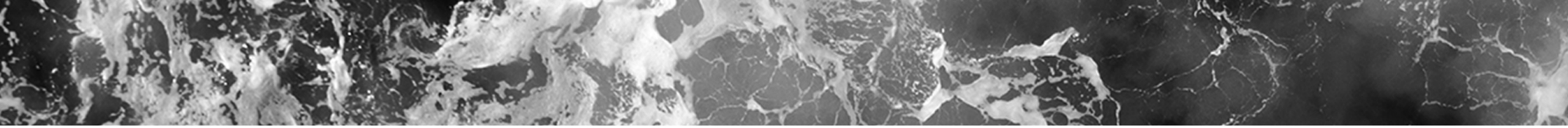
Coins - A cryptocurrency coin is a digital asset that exists on a blockchain and represents ownership of a unit of a decentralized currency, used for transactions or as a store of value.

Tokens – A cryptocurrency token is a digital asset created on an existing blockchain that represents value, rights, or access and can be used for transactions, governance, or ownership of digital and real-world assets.

Stablecoins – Stablecoins are cryptocurrencies designed to maintain a stable value, typically pegged to a fiat currency like the U.S. dollar, combining blockchain benefits with price stability.

Altcoins – An **altcoin** is short for **alternative coin** — any cryptocurrency other than Bitcoin.

Tokenization - Tokenization in cryptocurrency is the process of converting ownership or rights to an asset into a digital token on a blockchain, enabling secure, transparent, and programmable management of that asset.



WALLETS

Keys – Private / Public

A **cryptocurrency wallet key** refers to the secret cryptographic information that proves ownership of cryptocurrency assets on a blockchain. In most cases, this means the **private key**, which is an alphanumeric code (often in hexadecimal form) that authorizes transactions and allows you to spend funds from a specific wallet address.

> Private key: A unique, randomly generated number (typically 256 bits long) that you must never share. It is the "password" to your crypto account — whoever controls it can sign transactions and move the associated funds.

> Public key: Derived from the private key, it is used to generate a **wallet address** (the shorter, public-facing destination where others can send you crypto). You can share your public key or address, but it does not give anyone the ability to spend your funds

Digital –A digital wallet in cryptocurrency is a tool that allows you to access, manage, and transact your digital assets using cryptographic keys, without storing the coins themselves.

Seed Phrases – A cryptocurrency seed phrase is a human-readable sequence of 12 to 24 words that serves as the master key to access and recover a crypto wallet.

Cold Wallets – A cryptocurrency cold wallet is a secure storage method that keeps your private keys completely offline, protecting your digital assets from online threats.

Hot Wallets - A crypto hot wallet is an internet-connected cryptocurrency wallet that allows users to store, send, and receive digital assets quickly and conveniently.

Warm Wallets - A warm wallet is a cryptocurrency storage solution that balances security and accessibility, sitting between hot wallets (online) and cold wallets (offline). Unlike hot wallets, which are always connected to the internet, warm wallets use advanced security protocols to reduce exposure while still allowing relatively quick access to funds.

VASP

A VASP (Virtual Asset Service Provider) is an entity that facilitates the exchange, transfer, safekeeping, or administration of virtual assets on behalf of others, subject to regulatory compliance.

VASP Examples -Coinbase / Crypto.com or applications – Paypal/venmo

Decentralized Exchange – A decentralized exchange (DEX) is a blockchain-based, peer-to-peer marketplace where users trade cryptocurrencies directly from their own wallets using smart contracts, without a central intermediary such as Binance or Coinbase.

Centralized Exchange - A **centralized exchange** is a crypto trading platform managed by a single company that acts as an intermediary between buyers and sellers. Users create accounts, deposit funds (fiat or crypto), and place orders, which the exchange matches internally through a central order book

SMART CONTRACTS

Smart Contract Basics

A **smart contract** is a digital agreement stored on a blockchain that executes automatically when certain conditions are satisfied. Unlike traditional contracts that rely on legal enforcement or intermediaries, smart contracts operate using code, ensuring transparency, immutability, and trustless execution.

ZKPs

A **zero-knowledge proof (ZKP)** is a cryptographic protocol in which one party (the **prover**) can convince another party (the **verifier**) that a statement is true **without revealing any information beyond the truth of that statement**

Travel Rule

The **crypto Travel Rule** is the application of the Financial Action Task Force (FATF) Recommendation 16 to virtual assets, such as cryptocurrencies. Originally designed for traditional wire transfers, it mandates that **information about the sender and recipient "travels" with the transaction**, ensuring regulators can trace funds and detect illicit activity.

BLOCKCHAIN TOOLS

Wallet scanning and risk assignment

Transactional review

Connectivity (Other wallets / higher risk sites / connected to dark web markets, foreign VASPs, etc.)

Due diligence and risk rating

MEME COINS AND TRADING

Meme coins are cryptocurrencies that have been produced as a lighthearted joke. Nevertheless, some meme coins have ballooned in value, gained multibillion-dollar market caps and garnered celebrity endorsements.

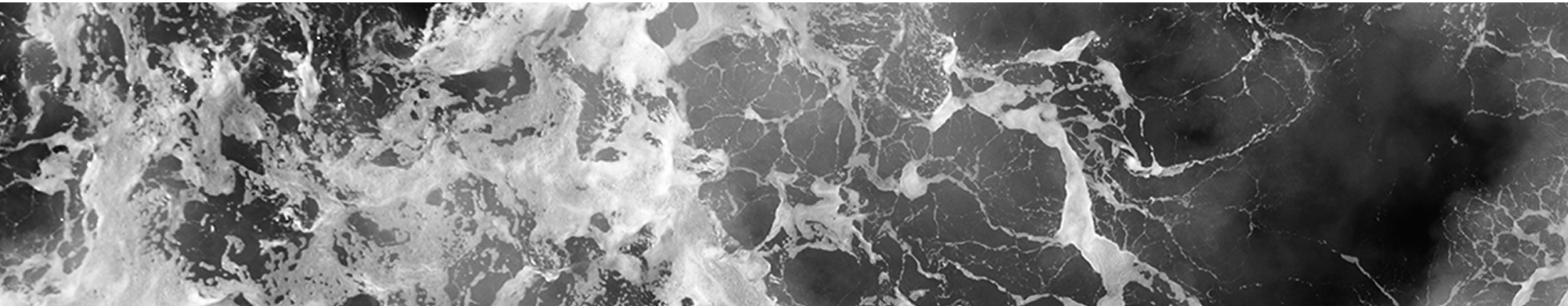
While these characteristics suggest that meme coins offer some underlying utility or value, the truth is that nearly all of them lack anything like fundamental value or unique use cases.

MOVING FORWARD WITH CRYPTOCURRENCY

New Products

New Opportunities for Compliance, Risk, and AML/CFT applications.

Time for control management, risk assessment, and risk management.



GLOSSARY OF TERMS

Address (Wallet Address)
A unique alphanumeric identifier used to send or receive digital assets. Similar to an account number, but visible on a blockchain.

Atomic Settlement
A transaction where the asset transfer and payment transfer occur simultaneously, eliminating settlement risk.

Attribution
The process of identifying the person, business, exchange, or organization controlling a blockchain wallet.

Blockchain
A distributed digital ledger that records transactions across a network of computers.

Blockchain Analytics
Technology used to trace, monitor, and assess blockchain transactions for AML, sanctions, fraud, and investigative purposes.

Burn / Burning
The permanent destruction of digital tokens, typically when a stablecoin holder redeems tokens for fiat currency.

Beneficial Wallet Ownership
The determination of who owns or controls a cryptocurrency wallet.

GLOSSARY OF TERMS

Chain Hopping
The movement of assets across multiple blockchain networks to facilitate transfers, access new services, or obscure transaction origins

Cold Storage
Offline storage of digital assets designed to reduce cybersecurity risk.

Consensus Mechanism
The process used by a blockchain network to validate transactions and maintain integrity.

Custodian
The entity with control over cryptographic private keys and the ability to move digital assets.

Custodial Wallet
A wallet where a third party controls the private keys on behalf of the customer.

Decentralized Finance (DeFi)
Blockchain-based financial services operating without traditional financial intermediaries.

Digital Asset
An asset that exists electronically and uses blockchain or distributed ledger technology.

Distributed Ledger Technology (DLT)
Technology that allows transaction records to be maintained across multiple participants.

GLOSSARY OF TERMS

Darknet Market
An online marketplace accessible through anonymizing technologies that may facilitate illicit activity.

Fiat Currency
Government-issued currency, such as U.S. dollars.

Gas Fee
A fee paid to blockchain validators for processing transactions.

Governance Token
A token that allows holders to vote on protocol changes within a decentralized network.

Hosted Wallet
A wallet maintained by a regulated financial institution, exchange, or service provider.

Hot Wallet
A wallet connected to the internet and actively used for transactions.

Hash
A cryptographic fingerprint used to verify data integrity on a blockchain

Layer 1 Blockchain
The foundational blockchain network itself, such as Bitcoin, Ethereum, or Solana.

Liquidity Provider
A market participant that supplies assets to facilitate trading and settlement.

GLOSSARY OF TERMS

Miner
A participant that validates transactions on proof-of-work blockchains such as Bitcoin.

Mixer (Tumbler)
A service designed to obscure the origin and destination of digital assets. Often viewed as high-risk by regulators and compliance departments.

Mint / Minting
The creation of new blockchain tokens.

Multi-Party Computation (MPC)
A custody technology that distributes control of private keys across multiple parties or devices

Node
A computer participating in a blockchain network by maintaining transaction records and validating activity.

Non-Custodial Wallet
A wallet where the user retains sole control over the private keys.

On-Chain
Activity that occurs directly on a blockchain and is recorded in the ledger

Peel Chain
A money laundering typology where funds move through numerous wallets while small amounts are repeatedly transferred away at each step.

Permissioned Blockchain
A blockchain network that restricts participation to approved organizations

GLOSSARY OF TERMS

Public Blockchain
A blockchain network open to participation by the public.

Reserve Account
The account holding funds or assets that back a stablecoin.

Self-Custody
A structure where an individual directly controls his or her own private keys.

Smart Contract
Computer code that automatically executes predefined business rules on a blockchain.

Stablecoin
A digital asset designed to maintain a stable value, typically pegged to a fiat currency such as the U.S. dollar.

Token
A digital representation of value or rights recorded on a blockchain.

Tokenized Deposit
A traditional bank deposit represented as a blockchain token while remaining a liability of the issuing bank.

Travel Rule
A regulatory requirement that originator and beneficiary information accompany certain virtual asset transfers, like requirements applicable to wire transfers.

Unhosted Wallet
A wallet controlled by an individual rather than a regulated intermediary. Also referred to as a self-custodied wallet

GLOSSARY OF TERMS

Validator
A participant responsible for confirming transactions and securing a blockchain network.

Virtual Asset
A digital representation of value that can be transferred or traded electronically.

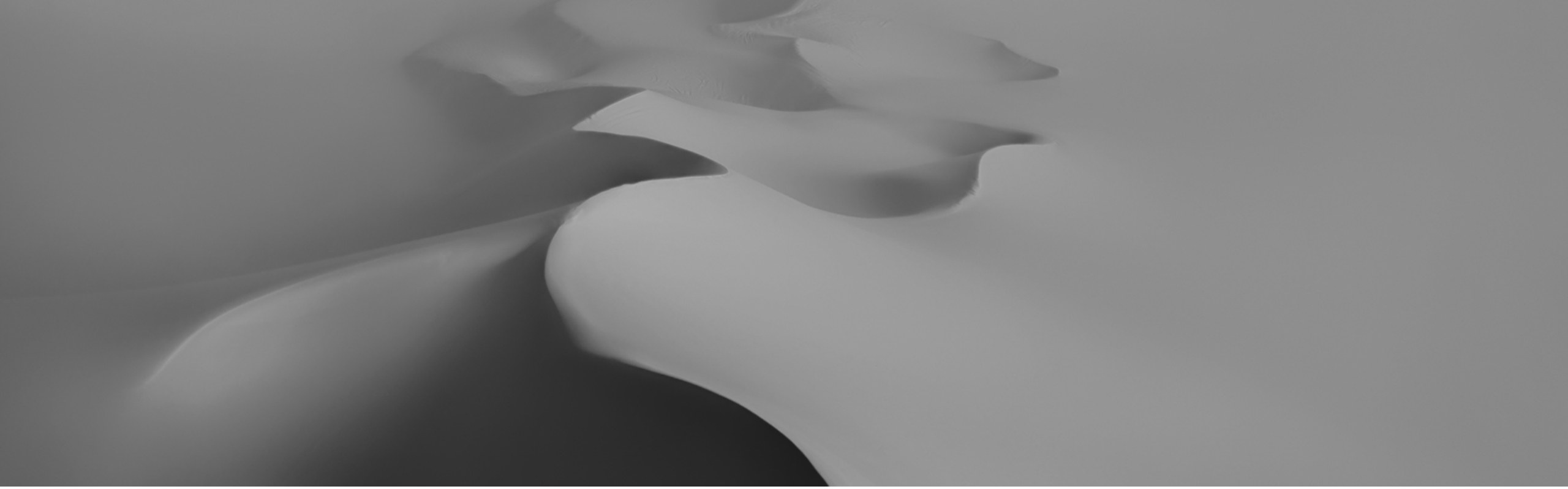
Virtual Asset Service Provider (VASP)
A business engaged in activities involving virtual assets, such as exchanges, custodians, brokers, or wallet providers.

Wallet
A software application, hardware device, or service used to store and transfer digital assets.

Wallet Screening
The process of evaluating a blockchain address for sanctions exposure, illicit finance risk, fraud indicators, or other compliance concerns.

Five Terms Every BSA Officer Should Master
1. **Travel Rule**
2. **VASP**
3. **Unhosted Wallet**
4. **Blockchain Analytics**
5. **Mixer**

Five Terms Every Banker Should Master
1. **Stablecoin**
2. **Tokenized Deposit**
3. **Custody**
4. **Private Key**
5. **Smart Contract**



THANK YOU

Presented by Mike Gallagher CRCM, CCAS, CAMS, CAFP
Chief BSA Officer – VersaBank USA