| 01 | CRYPTOCURRENCY BASICS | 5 MIN | Overview of cryptocurrencies and related products and services |
| 02 | EXCHANGE AND TRADING PLATFORMS | 10 MIN | How exchanges and trading platforms work |
| 03 | DECENTRALIZED EXCHANGES | 10 MIN | Differences between centralized and decentralized exchanges |
| 04 | LIGHTNING NETWORK | 10 MIN | Understanding the purpose and operation of Bitcoin’s lightning network |
| 05 | CUSTODY | 10 MIN | Centralized and decentralized custodial solutions |
| 06 | STABLECOINS | 10 MIN | How stablecoins differ from other cryptocurrencies |
| 07 | CLOSING REMARKS | 5 MIN | Products and services on the horizon |
**TERMINOLOGY**

**CRYPTOCURRENCY**
A digital token that is designed to function as a medium of exchange, and that enters into circulation via a decentralized process, such as thorough “mining”

**TOKENIZED SECURITY**
Digital representations of traditional securities such as equities, bonds and options

**UTILITY TOKEN**
Tokens that function as a medium of exchange within a particular platform. Utility tokens sold via an ICO are generally considered to be securities

**DIGITAL ASSET**
Digital representations of other types of assets such as gold

**STABLECOIN**
A digital representation of a payment instrument that contains certain characteristics of cryptocurrencies such that it can operate within a blockchain ecosystem
01 TERMINOLOGY

EXCHANGES
Platforms that enable peer-to-peer trading of cryptocurrencies and other digital assets

WALLET PROVIDERS
Services that allow users to securely storing their private keys in either a custodial or non-custodial manner

CUSTODIANS
Services that store private keys on behalf of customers

OTC TRADING
Trading that is conducted directly between two parties, rather than on an exchange

DECENTRALIZED EXCHANGES
Platforms that enable investors to find one another for the purpose of trading, but that do not take possession of customer funds or act as an escrow

02 CRYPTOCURRENCY EXCHANGES AND TRADING PLATFORMS
WHAT MAKES CRYPTOCURRENCY EXCHANGES UNIQUE FROM STOCK EXCHANGES?
- Coins are listed on multiple exchanges
- Customers must register with the Exchange directly
- Exchanges operate isolated from one another
Securities exchanges are carefully regulated to ensure that the exchange does not engage in market manipulation or fraud.

Exchanges must have enough supply of each of the cryptocurrencies they support to ensure that users can buy and sell at a stable and transparent price.

How does a regulatory agency verify that the licensee actually maintains 1:1 cryptocurrency holdings?

Inbound and outbound transfers of cryptocurrency introduce AML and other risks.

03 DECENTRALIZED EXCHANGES
03 DECENTRALIZED EXCHANGES

Source: https://radarrelay.com/
The primary distinction between centralized and decentralized exchanges is that decentralized exchanges do not take custody of customer funds at any point in the transaction.
REGULATORY CONSIDERATIONS
OF THE LIGHTNING NETWORK

SMART CONTRACT INTEGRITY
Who is responsible for the smart contract software code?

CONSUMER EXPECTATIONS
Transparency and disclosure is necessary to ensure that consumers understand that these platforms may not be regulated.

AML RISK
Greater decentralization correlates with greater AML and terrorist financing risk.

IS AUTOMATION SAFER?
The blockchain community believes that trust increases when humans are removed from the transaction. But humans are still responsible for coding and deploying the technology.
01 THE PROBLEM WITH BITCOIN

VISA NETWORK

VISA AND MASTERCARD NETWORKS

- 4,000 to 65,000 Transactions Per Second (TPS)
- Transaction fees based on transaction value

BITCOIN

BITCOIN PROTOCOL

- 7 Transactions Per Second
- Maximum block size = 1MB
- Average time between blocks = 10 minutes
- Transaction fees based on how busy the network is
  - Mining fees in December 2017 reached as high as $24 per transaction

04 THE SCALABILITY TRILEMMA

DECENTRALIZATION

SCALABILITY

SECURITY
LIGHTNING NETWORK

HOW PAYMENT CHANNELS WORK

Large nodes will likely be exchanges and other financial services platforms.

Medium nodes will likely be smaller exchanges and retail merchants.

Small nodes will likely be individuals and local merchants.

Transactions travel across the network via nodes and channels.
**FUNDING CHANNELS**
- Channels are opened by sending bitcoin to a smart contract written on the public blockchain.
- Both sides to the channel must sign the transaction.
- Users can open channels with other users or nodes.
- Channels are akin to multi-signature wallets.

**LINKING CHANNELS**
- Larger nodes serve to connect users through central hubs.
- Larger nodes can collect transaction fees by allowing transactions to flow through them.

**MULTISIGNATURE**
Channels operate like multi-signature wallets—each party to a channel must sign to withdraw funds from the channel.

**TRANSACTING ACROSS CHANNELS**
- Transactions can route through a channel only if there are enough funds in the channel.
- Nodes cannot control whether a transaction flows through its channels.

---

**REGULATORY CONSIDERATIONS OF THE LIGHTNING NETWORK**

**SMART CONTRACT INTEGRITY**
Who is responsible for the smart contract software code?
Risk of loss increases if a user doesn’t connect to the network for more than 30 days.

**CONSUMER EXPECTATIONS**
Transparency and disclosure is necessary to ensure that consumers understand how their channels will be used and whether there are any protections in the event of a loss.

**AML RISK**
Greater decentralization correlates with greater AML and terrorist financing risk risk.

**IS AUTOMATION SAFER?**
The blockchain community believes that trust increases when humans are removed from the transaction. But humans are still responsible for coding and deploying the technology.
05 ONE HUNDRED YEARS OF CUSTODY

INSTITUTIONAL CUSTODY

MARKET CRASH OF 1929
Cash exited institutions post-crash, but after the FDIC formed in 1933, re-entered
Paper securities were primarily self-custodied but, post-crash, moved to central custodians

RISE OF CUSTODIANSHIP
Cash is easily lost or stolen – banks provide fortress-level security and insurance
Paper securities can be lost or hard to sell or transfer; securities intermediaries provide liquidity access and administrative ease of transfer

FORK IN THE ROAD
Digital assets can be custodied securely along a spectrum of options, via institutional custodians or as self-custody methods

SELF CUSTODY

FIAT

STOCK

DIGITAL ASSETS

1919 1929-1933 2014-2019
**05 WALLET-BASED CUSTODY**

**WHY WALLETS?**
- Anyone can interact with a blockchain using a command-line prompt, but most need a simple interface
- Wallet software gives a common user access to complicated technology

---

**INSTITUTIONAL CUSTODY**
- **MULTISIGNATURE**
  Company stores one key, user stores other keys, third party may store more keys
- **HOSTED**
  Company generates and stores the sole key (may use hot or cold storage methods)

**SELF CUSTODY**
- **SOFTWARE**
  Simple interface downloaded from a third party, stores file with encrypted key locally on personal computer
- **HARDWARE**
  User buys a third party-built specialized physical device to store file with encrypted key
- **PAPER**
  User prints a key or seed phase, often using wallet software, and stores offline

---

**LEGAL LEGEND**
- **HOT WALLETS ARE INTERNET-CONNECTED**
- **COLD WALLET ARE COMPLETELY OFFLINE**

---

**05 REGULATORY CONSIDERATIONS**

**IS IT A SECURITY?**
- A stablecoin that contains a mechanism designed to maintain price parity may constitute an "investment contract" under the Howey test

**KNOW THE ISSUER**
- The issuer of a fiat or asset-backed stablecoin is akin to an issuer of a payment instrument

**VERIFYING COLLATERAL**
- Collateral may be held in a trust account and verified by state regulatory agencies

**SECONDARY MARKET SALES**
- Cryptocurrency exchanges trade stablecoins on the secondary market. This activity is more akin to "money transmission" in that the collateral is already accounted for.
06

STABLECOINS

COINS AND CURRENCY
- Precious Metals
- Coins
- Currency
- Bank notes

PAPER INSTRUMENTS
- Promissory notes
- Bills of exchange
- Traveler’s cheques
- Paper gift certificates

FINANCIAL TECHNOLOGY
- Credit and debit cards
- Stored value / prepaid access cards
- Digital wallets
- **Stablecoins**
PAYMENT INSTRUMENT
Any electronic or written check, draft, money order, traveler's check or other ELECTRONIC or written INSTRUMENT or order FOR THE TRANSMISSION OR PAYMENT OF MONEY, sold or issued to one or more persons, WHETHER OR NOT THE INSTRUMENT IS NEGOTIABLE. "Payment instrument" DOES NOT INCLUDE any credit card voucher, any letter of credit or ANY INSTRUMENT THAT IS REDEEMABLE BY THE ISSUER IN GOODS OR SERVICES.

PRICE VOLATILITY
At its highest, the price of BTC was nearly $20,000
06 THE ROLE OF STABLECOINS

MEDIUM OF EXCHANGE
An intermediary instrument or system used to facilitate the sale, purchase or trade of goods between parties.

STORE OF VALUE
An asset that maintains its value without depreciating.

UNIT OF ACCOUNT
A unit of measurement for defining, recording and comparing value.

06 TYPES OF STABLECOINS

FIAT/ASSET-BACKED STABLECOINS
- Tokens represent a claim on the underlying deposits
- Involves an issuer, custodian and initial seller
- May be fully or only partially collateralized
- Examples: Gemini Dollar (fully-collateralized) and Tether (partially-collateralized)

CRYPTO-COLLATERALIZED STABLECOINS
- Price stability mechanism aims to achieve parity with fiat currency
- Relies on an algorithm that works autonomously to achieve price stability
- Collateral is often locked in a smart contract
- Example: Dai

ALGORITHMIC (NON-COLLATERALIZED) STABLECOINS
- Money supply is governed by an autonomous algorithm that buys and sells the stablecoin to create price stability
- Not backed by any collateral
A stablecoin that contains a mechanism designed to maintain price parity may constitute an "investment contract" under the Howey test.

The issuer of a fiat or asset-backed stablecoin is akin to an issuer of a payment instrument.

Collateral may be held in a trust account and verified by state regulatory agencies.

Cryptocurrency exchanges trade stablecoins on the secondary market. This activity is more akin to "money transmission" in that the collateral is already accounted for.
Motivated by a desire for "decentralization," the industry continues to create new methods of payments and capital formation. But aren't these just digital forms of traditional payment instruments?

When you do not need to trust others with your valuable assets, you still need to trust yourself.

Despite the desire to move towards a decentralized environment, the efficacy of centralized networks continues to pull the industry towards centralized applications.