Digital Assets = Modern Money

1. Questions, Answers

2. Woose, Woosie, Wizard

3. Speculation, Sweet Spots, Mining

4. Advisory: Be Ready, Leave a Legacy

5. Glossary, Old News, References

1.1 Start With Most Popular Digital Asset -- Bitcoin

=> **KIS**: "Bit" represents "Digital"
"coin" represents "Money," so
"Bitcoin" represents "Digital Money,"
and to be precise, Bitcoin is defined
in the Reference below:

=> **Ref**: A Peer-to-Peer
Electronic Cash System

What is Bitcoin? (continued)

=> Simple Application

=> Cool Invention

=> Secure Wallet

=> Protocol on Internet

Simple Application

Sender and Receiver have Bitcoin Wallets:

A. Sender enters:

1. Wallet address
2. Number of bitcoins e.g. 0.025 or 1.0 or 10.5 or ...
3. key: Send

B. Receiver will see:

1. After transfer time, bitcoins received
2. Status (pending or confirmed)
3. When confirmed, Receiver can save or spend (buy something, or send to another Wallet)

Cool Invention

=> It's Here To Stay

Like electricity, radio, auto, phone, TV, computer and Internet are part of our daily lives.

=> It's Revolutionary

With possible misuse and misinformation:

Expect "Red Flags" from those that don't understand it,

Expect "False Flags" from those that fear it.

Secure Wallet

=> With Public Key Cryptography

Bitcoin Address: Public address of **Wallet** to receive bitcoins, and used like a public address on a mailbox e.g. 1BzKkord11NSuGu5FjQAAL3xLQcFm3G3vH

Wallet: One or more Bitcoin Addresses, each with paired **Public Key** and **Private Key**

Public Key: Computed from a **Private Key** to verify **Digital Signature** in a **Transaction**

Private Key: Random character string, to spend (withdraw) bitcoins from a Wallet

Digital Signature: A **Hash** of Private Key and Message, to sign a **Transaction**

Hash: Fixed length character string computed from text of arbitrary length

Transaction: Bitcoin transfer between Wallets for **Confirmation** on **Blockchain**

Confirmation: Transaction validation by consensous of security service called "Miners"

Blockchain: Transaction settlement records in a distributed, global, public ledger.

Protocol on Internet: For Peer to Peer Transfer of Value*

=> **Economic Layer:** on Public Internet

=> **Transfer of Value:** Without permission from 3rd party (brokers, banks or government)

=> **Value**: Digital Asset = money, property or commodity
> *To save or spend (buy stuff, gift, donate, ...)*
> *A shared expectation*
> *Measured in Bitcoin (BTC), US Dollar (USD), ...*

**** Blockchain technology can transfer ownership of any asset -- money, house, . . .***

Bitcoin = Protocol, bitcoin = Value

=> Value designation is "BTC" (*With ISO 4217 code "XBT" in review*)

> 1 BTC value ranged from pennies in 2010 to over $19,000 in 2017

> In 2015, lows and highs were near $200 and $500, respectively

> In 2016, lows and highs were near $370 and $900, respectively

> Lows and highs in future are unknown -- it's market driven

=> Other designations: mBTC (milliBTC), bit, Satoshi, ...

> 1 BTC = 1,000 mBTC or 1,000,000 bits or 100,000,000 Satoshi

> 1 mBTC = 0.001 BTC

> 1 bit = 0.000001 BTC

> 1 Satoshi = 0.00000001 BTC

=> Bitcoin production is part of math-based Protocol

> New bitcoins paid (sent) to "Miners" for transaction confirmation

> Production requires energy (from Miners), modeled after mined commodity such as gold, and production reduces by 50% every 4 years

> Payments (to Miners) scheduled thru 2140 (next 122 years)

> Today over 17 million bitcoins, Max in 2140 will be 21 million

1.2 Why Bitcoin?

=> In a civilized society, modern money (finance) and trade (commerce) will be:

> *Digital, Fast, Economic, Peer-to-Peer, Regulated*

> *Legitimate, Worldwide, Trusted, Secure*

> *Traceable, Sustainable, Decentralized*

Why Bitcoin? (continued)

=> **Digital: Fast, low cost, peer to peer transfer of value**
vs. Snail mail, high fee wire transfers; cumbersome commodities

=> **Regulated: As 3 asset types: money (FinCEN), property (IRS), commodity (CFTC) & legitimate by worldwide consensous**
vs. Regulation and legitimacy of fiat by trust in sovereign nations.

=> **Trusted and Secure: Public Key Cryptography prevents fraud e.g. double spend (forgery) and repudiation (deny valid contract)**
vs. Forgeable money/checks, denial of credit card purchase

=> **Traceable: Value of a bitcoin is volatile, are interchangeable with other bitcoins, and transactions are recorded in a traceable, global, permanent, public Blockchain**
vs. Untraceable Fiat transactions

=> **Sustainable: Value based on trust in Math-based protocol**
vs. Fiat value based on "emotional" faith in 3rd parties (Banks, Fed, ...)

Why Bitcoin? (concluded)

=> Decentralization has historical precedents:

> ***National:*** *America split from central control by Brits,*

> ***Religion:*** *Lutherans split from central control by Catholic Church,*

> ***Business:*** *Telco's split from central control by Ma Bell,*

> ***Technical:*** *Military enhanced centralized circuit network with decentralized packet network e.g. ArpaNet*

=> Decentralization is to finance and commerce, as Internet is to communications:

> ***Internet**: Moves **packets** from A to B, without permission from central entity*

> ***Bitcoin**: Moves **value** from A to B, without permission from central entity*

1.3 How Can Bitcoin Be Used?

=> **Save --** as a long term store-of-value

=> **Spend --** buy stuff without credit/debit cards or (Fiat) cash

=> **Send --** as gifts, remittance, donations

> *Gifts -- for education, anniversaries, ...*

> *Remittance -- transfer value to worldwide family and friends*

> *Donations -- to charities: United Way, Red Cross, ...*

=> **Also**

> *Transfer value to paper wallet -- for trade or backup "cold" storage*

> *Easier to handle than mined (physical) commodities -- such as gold*

> *Diversity Future Investments with Fiat + Crypto (Bitcoin, Ethereum, ...)*

1.4 Where Can Bitcoin Be Used?

=> On any computer or smartphone with Internet access

=> Paper Wallets can be transferred between people anywhere, anytime -- without computers, phones or Internet

=> For just about Anything

(Except in places that restrict freedoms)

=> Anywhere e.g. Defacto Global Reserve Digital Money

1.5 When Can Bitcoin be Used?

Now!

=> *With historical phases:*

1. **Geek**: 2009 to ?: Creators, Early Adopters
2. **Vice**: 2011 to ?: Bad Actors - **will** get weeded out
   >e.g. Silk Road, Ponzi Schemes, . . .
3. **Speculation**: 2013 to ?: For those that love volatility
   > *If not trained and no spare cash -- **stay away**,*
   > *Otherwise -- **enjoy** the intrigue (and risk) of innovation*
4. **Wall Street**: 2015 to ?: Added security, regulation, taxation
5. **Main Street**: 2018 to ?: Added capacity and speed for prime time
   > *Store of Value -- Cash, Gold, **Crypto (Bitcoin, Ethereum, ...)***
   > *Diversify Investments -- Fiat, Propery, Commodities, **Crypto***
6. **New Street**: 2020 to ?: Contracts to transfer asset ownership