Cryptocurrencies

Arriving into reality as fast as they leave it.

Pete Horne 2021
p@horyzon.co

Overview

Crypto is arriving into reality...

- Being adopted by institutional investors
- Slowly but surely integrated into regulation systems
- Losing utility for crime

While leaving it at the same time...

- DeFi reinventing market technology
- Non Fungible Tokens (NFTs) redefining content and ownership
- DAOs revisiting governance

In this presentation I propose that we are seeing:

- Regulation creating “Integrated Crypto” while; crypto “Disintegrates Finance”

A Quick Crypto History Lesson

- Crypto was born from the cypherpunk movement which was - !PUNK
  - Anarchist
  - Argumentative
  - Disagreeable
  - Anti social
  - Collectivist
- The object was to break the apogee of control - the money system (“...” = punk tribal language)
  - Create money that could not be “debased”
  - Destroy “usurious, ticket clipping” middle men
  - Avoid “censorship” (the systems ability to void unapproved activity or people)
  - Provide “freedom” through anonymity

The Attack Plan

- Bitcoin created by “Team Satoshi Nakamoto” was designed to attack the “fiat” money systems
- Mostly built on existing techniques & knowledge:
  - Peer to peer messaging with gossip protocols and distributed hash tables
  - Message authentication codes (hashing)
  - Non repudiation (digital signatures)
  - Proof of Work (email spam filtering)
  - Merkel Trees
- BUT; the integration of the existing crypto arts into the invention of the blockchain mechanism to enable Bitcoin is objectively a world changing event.
- But while the “Rube Goldberg” money system worked technically, money get its “currency” from use - Bitcoin had to be used as money to become a form of money.

The Energy of the Nerds*

The use of cryptocurrencies was broadly energised by three phases of Nerd adoption:

1. The Libertarian Nerd Phase - cypherpunk, libertarian and technophiles play around with it (the USD 365M pizza)

2. The Drug Nerd Phase - Silk Road uses bitcoin and 1 BTC = 1 USD and fiat/crypto exchanges are born.

3. The Financial Nerd Phase - Bitcoin spawns Ethereum which makes money programmable and decentralised finance (DeFi) is born

*** Pete is a nerd and doesn't think it's a pejorative ;-)**

Ethereum - the Cyberdemon of the Bitcoin Maximalists

The Financial Nerd Phase is really the ethereum phase - what is Ethereum?

We need to take a step back:

- The blockchain invention that enabled Bitcoin is a process for adversaries to achieve consensus about the contents of a journal of messages.
- It is this consensus about the messages that have been sent since the start of the blockchain that allows a ledger of value transfer messages (transactions) to be constructed to say irrefutably who has what.
- The Bitcoin messages are actually small program fragments that when executed in blockchain-order transfer values from one wallet (public key) to another.
- The Bitcoin programming language could have been extended but the programmers who control the code said “no”
- They are known as “maximalists” - they believe Bitcoin should only be used for value transfers and any other cryptocurrency is inferior.
- So Vitalik Buterin said - I’ll make another blockchain that is programmable - Ethereum.

The Programmable Blockchain

- Ethereum created the concept of the programmable blockchain
- “ETH” is the native currency of the Ethereum blockchain, like “BTC” is the currency of the Bitcoin blockchain
- However as well as using ETH as a cryptocurrency in exactly the same way as BTC, you can also use your ETH to “buy” space on the blockchain to install programs, and run installed programs.
- Ethereum calls these programs “smart contracts”
- The invention of Ethereum also saw the invention of “Solidity” which is the preeminent smart contract language.
- Ethereum also created the concept of “Web3” which allows all Ethereum transactions to be executed from a web browser, making it “internet native” money.

DeFi - The Nerdy Bit

- While the Ethereum blockchain made the programmable blockchain possible, I would argue that Solidity makes DeFi possible
- My analogy is that Ethereum is Intel and Solidity is Windows.
  - Ethereum provides a virtual machine (VM) with an assembly language
  - The Solidity language and compiler creates the integration layer over the VM that businesses can use to share applications
- The Solidity Model means smart contracts can share method calls. This is similar to:
  - a cloud server sharing data and process using Web Services
  - Java or C# programs sharing code libraries with each other.
- Standardising and publicising Ethereum smart contract interface and method names using Solidity (technically; Solidity compiler generated ABI) allows smart contracts from one programmer to work reliably with smart contracts created by another programmer.

DeFi - The Business Bit

- The early rush to ethereum created “ICOs” - initial coin offerings. Smart contracts for tokens (“units”) in - you name it.
- The proliferation merged into a standard pattern - ERC20
    - ERC - Ethereum Request for Comment like an IETF RFC
- An ERC20 Token is a smart contract that defines divisible units of something where the units are fungible.
- An ERC20 Smart Contract will have standard method and event “signatures” so another contract can reliably use them.
- Stable Coins (coins denominated in fiat currency) are ERC20 tokens where the token represents a share of a trust or other structure that holds the fiat.
- An ERC20 contract is similar to a custody service where the owner can permit another contract to manipulate their holdings allowing the ERC20 contract to perform settlement and exchange functions.
- Other smart contracts that drive these ERC20 custody contracts call themselves “protocols”

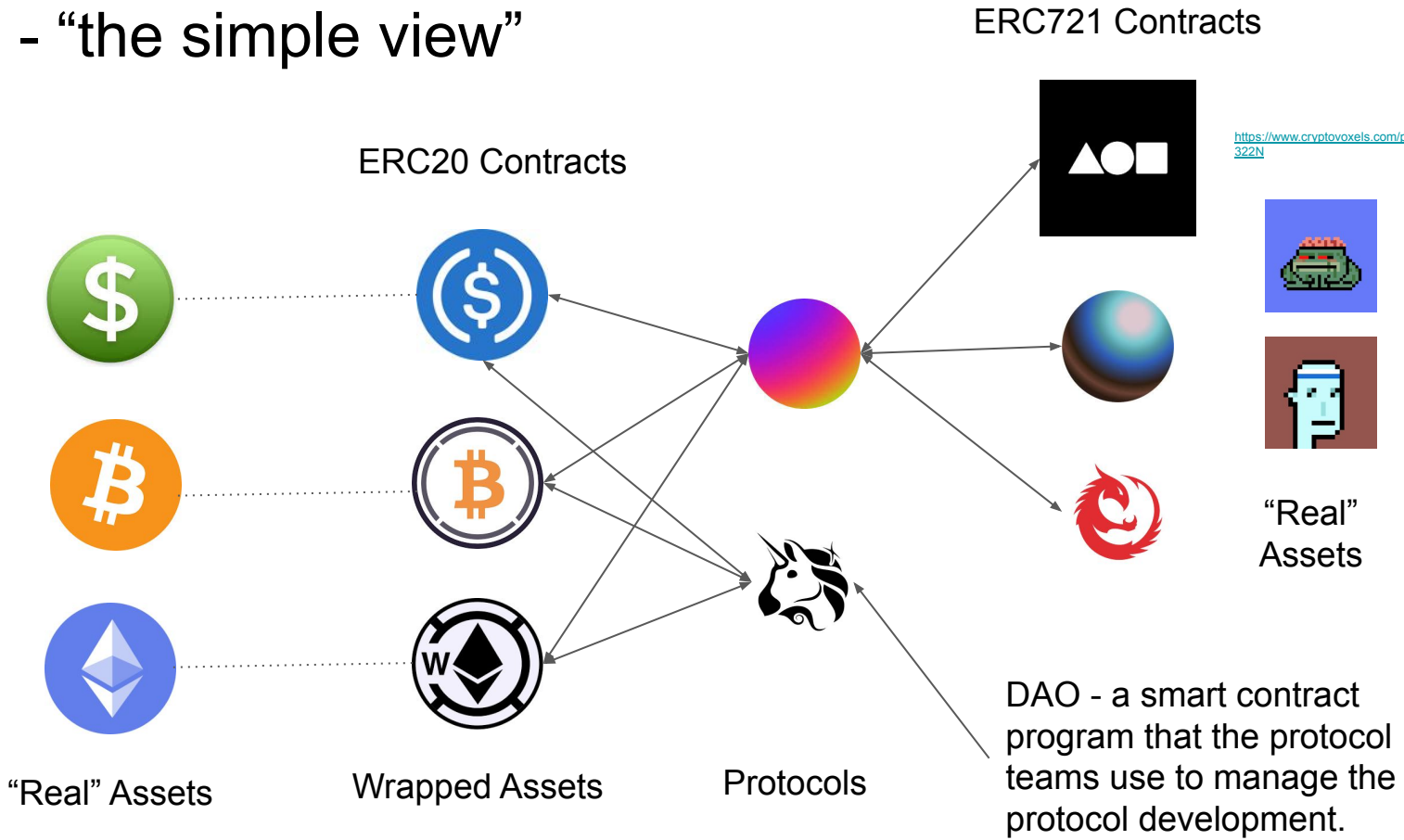
DeFi - The Disruptor bit

- Ethereum and ERC20 has proven that people can trade tokens using the decentralised blockchain and Web3 interface
- DeFi protocols are now implementing market functions at low cost and automatically “on chain”
  - Price Discovery
  - Crossing
  - DVP settlement
- Newer protocols are creating rules and incentives that automate market maker and financing/liquidity functions that used to require balance sheets
  - Uniswap market pairs
  - MakerDao stable coin pricing
- These innovations are literally disintegrating traditional finance (TradFi) functions and making them into blockchain programs

DeFi - The (slightly) unreal bit

- ERC20 standardised fungible tokens - units of interchangeable value
- ERC721 standardised non fungible tokens - units of unique value.
  - An ERC721 contract manages references to resources that are unique.
  - An ERC721 token is an instance of a reference and it can be transferred from one holder to another.
- Through the Solidity ABI, smart contracts can drive ERC721 smart contracts and ERC20 smart contracts to create markets and trades for non fungible tokens (Eg. art) paid for in fungible tokens (Eg. a USD stable coin).
- For digital art, an ERC721 smart contract is akin to a gallery that holds and transfers title for a work/deed, and the ERC20 smart contract is the payment mechanism from the purchaser to the owner.
- The ERC721 service provider (or protocol) makes the market and executes the DVP process.
- This means you can have a finance system that supports cryptopunks, cryptoadz cryptovoxel land parcels, and any other digital asset.
- The art/music innovations are real and important.

DeFi - “the simple view”



Integrated (cleaned) Crypto

While crypto has a chequered past and a weird and unknown future, it is being adopted, understood, and integrated:

- BTC: 1T (1 Tesla Corp) ETH: .5T (.5 Tesla Corp)
- Exchanges are regulated and controlled.
- “Old” cryptocurrencies are being mastered by law enforcement (they don’t work)
- Global Coordination emerging for AML/CTF frameworks (FATF)
- Securities law asserted (ICOs, Ripple case) and clarity emerging
- Stable Coins increasingly regulated
- CBDC initiatives leading to more adoption and integration

Note: Fiat/Crypto bridges are the control points; there is a growing crypto only economy.

Disintegrating Finance

- ERC*nnn* standards allows organisations to program on the blockchain what other organisations offer on the blockchain
  - Permissionless
  - No intermediaries
  - End user to smart contract
- Similar to...
  - All business rules and database systems open for public use
  - Security controlled by the client, not the enterprise
  - Frictionless transfer between service providers
- Crypto is literally attempting to disintegrate the financial services industry
  - Pull apart the processes and the control (disintegrate)
  - Remove all intermediaries (disintermediate)

Crypto - Not without considerable risks

Crypto could get cleaned away and/or become more untidy:

- Technology risks - errors, failures, quantum computing
- Lack of robustness - technology cabals control the source code
- ESG issues - electricity and resource consumption
- Government choke - CBDC competition, overregulation, lack of clarity and understanding.
- International discord - mining issues and capital controls
- A better mousetrap is invented.
- But - The Nerds weren’t asked to start and won’t stop if told to stop.

What’s next

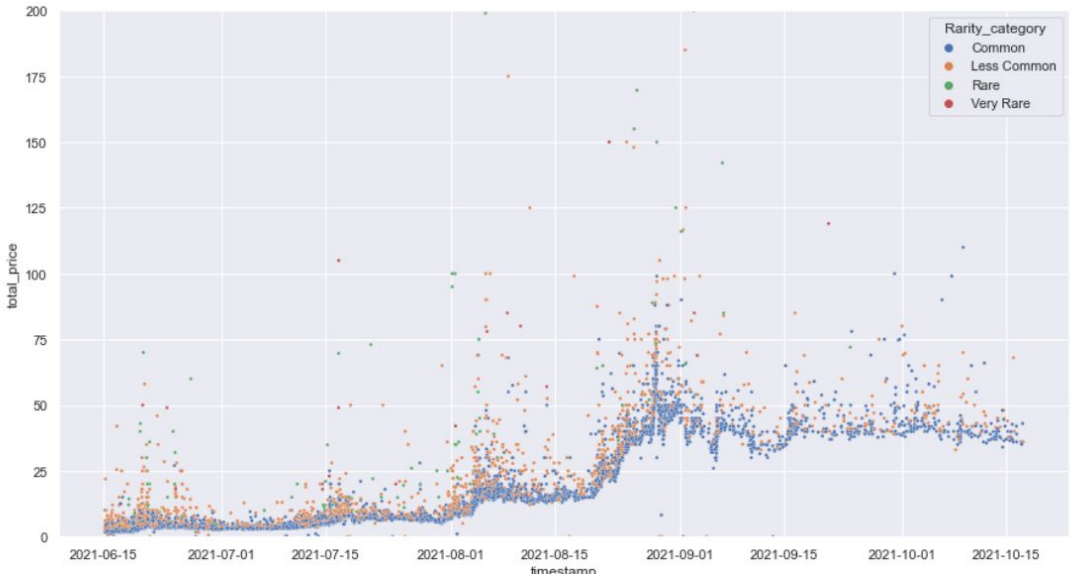
- More innovation, disintegration and integration...

Innovation	**Crypto Narrative**	**Reality**	**Progress**
Cryptocurrencies	Disintegrate Money	Becomes Money without intermediaries	Done
ERC20 Smart Contracts	Disintegrate Securities	Becomes securities without exchange/registries.	Done
ERC721/NFT Tokens	Disintegrate Property Ownership (NFTs)	Creators manage and distribute digital property without agents/platforms	Underway
DAOs	Disintegrate Governance	Adopted into governance processes.	Coming

Finally - what's a crypto worth

ETH/BTC: "I'll tell you why it went down if you can tell me why it went up"

NFTs: Cryptoadz Analysis



Horyzon/CARS rarity score/price over time - patterns emerge (dare we say the market is rational?)

Snoop Dogg's ½M cryptoadz NFT

Is this Origin City parcel worth 180K?

https://www.cryptovoxels.com/map

Summary

- Crypto started weird, continues to be weird, and will only get weirder; but there’s something important going on.
- Culture will embrace it as it grows and learns about it.
- So will regulation.
- There is still considerable risk and uncertainty
- It’s fascinating and won’t go away