Lesson 3 - - Blockchain Intro

The advent of the Ethereum platform has spawned thousands of startup companies in the blockchain space. The failure rate has always been high for high-tech startups and blockchain is no different. But there is a twist in that a blockchain app can try to create a new cryptocurrency. Startups have been issuing and selling their own currency tokens in exchange for Bitcoin and Ether. Like selling shares of stock, it's a way to raise capital bypassing the scrutiny of banks, venture capitalists, and government regulations and controls. The process is called an Initial Coin Offering (ICO) and it's a new way to raise funds necessary for development and expansion. An ICO is similar to crowd funding in that a startup company promotes its idea for a product and its currency tokens, and if it raises enough money in the time allotted, work begins. If not, the ICO fails and the money is returned. Eventually successful privately-owned companies go public, selling shares of stock through an Initial Public Offering (IPO). The Initial Coin Offering (ICO) in the cryptocurrency space's is far easier than an IPO in the mainstream investment world. Startups connect with interested investors who buy into the offering, either with fiat currency or with preexisting digital tokens like Bitcoin or Ether, and in return investors receive equivalent cryptocurrency tokens specific to the ICO. Naturally investors are speculating that the their newly acquired tokens' value will grow over time. The startup then launches its product, and/or its new digital currency and many don't last more than a year. An article from Fortune (http://fortune.com/2018/02/25/cryptocurrency-ico-collapse/)

reported some lasted only a few months. This is an excerpt from the same article:

We here at Fortune have cast a curious but frequently skeptical eye on ICOs, which from the get-go were ripe for scams. It turns out that skepticism was well warranted: cryptocurrency news site Bitcoin.com has surveyed last year's ICOs and found that of 902 tracked by TokenData, 142 failed before raising funding, and another 276 failed after fundraising.

That's a 46% failure rate — but wait, there's more. Bitcoin.com found another 113 projects that it calls "semi-failed," because their teams have gone off the radar or their community has withered away. Add those, and the failure rate jumps to 59%. Bitcoin.com says the total funding of failed projects from 2017 was $233 million.

==========

Nonetheless, since literally thousands of blockchain startups have embraced Ethereum and Ether, the founders are dreaming of the day when Ethereum becomes the world's "decentralized computer," as explained below in a video by Dr. Gavin Woods.

The complexity of blockchain applications like Bitcoin, and those built with cryptocurrency options using Ethereum, can become confusing very quickly by examining in greater detail the workings of the underlying cryptography and consensus mechanisms. The higher level concepts regarding decentralized design, security benefits, scalability challenges, trust, and immutability are easier to digest. This is important because new ways to use blockchain continue to be discovered at a rapid pace. That's because a digital asset can be almost anything of interest between two or more parties. Therefore, blockchain technology has created quite a stir among innovators and investors world-wide who predict it will ultimately change how the economy works when intermediaries in any given market are no longer needed to handle payment, clearing, and settlement.

Watch this video:

1. Watch *"DEVCON1: Ethereum for Dummies" from Dec of 2015 by Ethereum's CTO Dr. Gavin Wood. He explains how his appreciation for the technology changed over time, and in this 23 minute presentation explains his vision for Ethereum to become the first global computer, and how that will impact the world.* click here

Staying at a high level and considering risks surrounding the use of a blockchain application, here are a few excerpts from a very long legal agreement pulled from the ethereum.org website, requiring anyone downloading its platform to

acknowledge the risks. Interesting that what isn't mentioned below is that the majority of blockchain attacks have been designed to steal cryptographic keys rather than attack the actual blockchain:

"Risk of Weaknesses or Exploitable Breakthroughs in the Field of Cryptography

Cryptography is an art, not a science. And the state of the art can advance over time. Advances in code cracking, or technical advances such as the development of quantum computers, could present risks to cryptocurrencies and the Ethereum Platform, which could result in the theft or loss of ETH. To the extent possible, Stiftung Ethereum intends to update the protocol underlying the Ethereum Platform to account for any advances in cryptography and to incorporate additional security measures, but it cannot predict the future of cryptography or guarantee that any security updates will be made in a timely or successful manner.

Risk of Ether Mining Attacks

As with other cryptocurrencies, the blockchain used for the Ethereum Platform is susceptible to mining attacks, including but not limited to:

- Double-spend attacks
- Majority mining power attacks,
- "Selfish-mining" attacks
- Race condition attacks.

Any successful attacks present a risk to the Ethereum Platform, expected proper execution and sequencing of ETH transactions, and expected proper execution and sequencing

of contract computations. Despite the efforts of the Ethereum Stiftung and Team, known or novel mining attacks may be successful.

Risk of Rapid Adoption and Increased Demand

If the Ethereum Platform is rapidly adopted, the demand for ETH could rise dramatically and at a pace that exceeds the rate with which ETH miners can create new ETH tokens. Under such a scenario, the entire Ethereum Platform could become destabilized, due to the increased cost of running distributed applications. In turn, this could dampen interest in the Ethereum Platform and ETH. Instability in the demand of for ETH may lead to a negative change of the economical parameters of an Ethereum based business which could result in the business being unable to continue to operate economically or to cease operation.

Risk of Rapid Adoption and Insufficiency of Computational Application Processing Power on the Ethereum Platform

If the Ethereum Platform is rapidly adopted, the demand for transaction processing and distributed application computations could rise dramatically and at a pace that exceeds the rate with which ETH miners can bring online additional mining power. Under such a scenario, the entire Ethereum Platform could become destabilized, due to the increased cost of running distributed applications. In turn, this could dampen interest in the Ethereum Platform and ETH. Insufficiency of computational resources and an associated rise in the price of ETH could result in businesses being unable to acquire scarce computational resources to run their

distributed applications. This would represent revenue losses to businesses or worst case, cause businesses to cease operations because such operations have become uneconomical due to distortions in the crypto-economy."

Please navigate to the quiz questions for this lesson.

****