Blockchains & Distributed Ledgers

Lecture 10

Aggelos Kiayias

Slide credits: AK

Overview

Networking and Distributed Ledgers

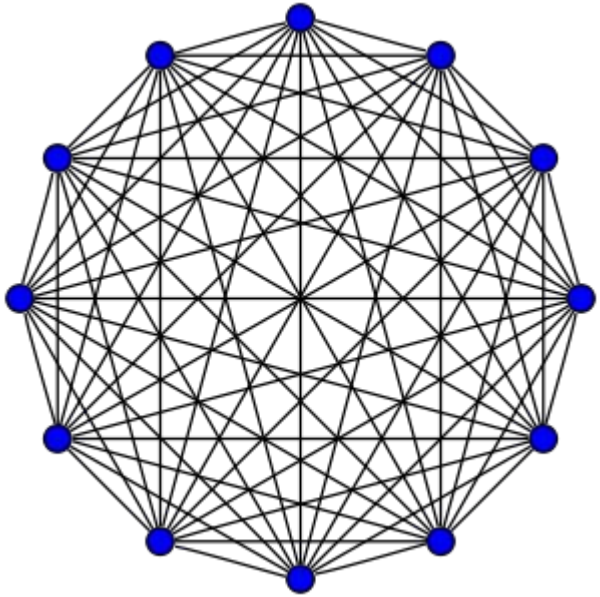
Applications and Legal aspects

Overlay Networks, I

- A reliable network is critical for blockchains and distributed ledger protocols to operate.
  - typically they utilize an overlay network.
  - An overlay network, is a network built on top of another network.
  - In an overlay network, virtual links connect the participating nodes.

Overlay Networks, II

in a network
we would like
nodes to
be fully connected



relevant operations :
1. point-to-point communication
2. broadcast.

Network Requirements

- Synchronicity.
- Reliable message transmission.
- Reliable Broadcast.

Bitcoin’s P2P Network

- A **Peer to Peer** network over TCP/IP.
- Peers are identified by their IP address.
- Peers can diffuse messages that will be propagated to the whole network.
- Peers initiate a small number of outgoing connections.
- Peers receive a limited number of incoming connections.

Public vs. Private networks

- A system with a public IP “lives” in the Internet.
- A system with a private IP “lives” in a private network and communicates with the Internet via a router that performs Network Address Translation (NAT).

Peer2Peer Networks

- (In the case of Bitcoin) The requesting node contacts a **DNS Seeder** which is a node with a public IP address that can serve a list of IP addresses for Bitcoin nodes.
  - The seeder obtains those addresses via *crawling*.
- If the connection fails the node has a hardcoded set of IP addresses.
- Peers can exchange node IP addresses via **ADDR** messages that contain a selection of a peer’s address book.

Table maintenance

- Nodes maintain tables of peers that they have learned. Typically in two categories:
  - Nodes that have proven to be operational
  - Nodes for which the node has been informed about their existence but they have not been contacted yet.
- Tables are updated on a regular basis.
- Timestamp information is stored from the last connection attempt.

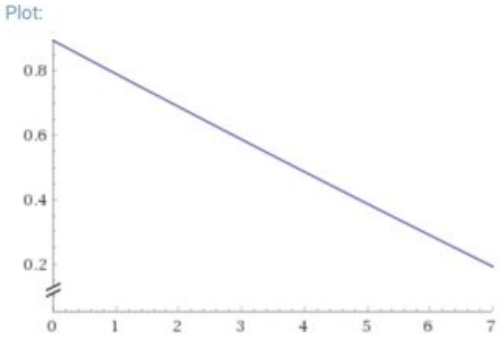
Connect to new or tried peers?

Tables “new” and “tried”

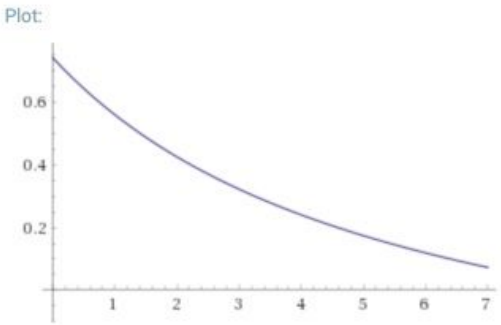
- A node with ω in {0,.., 7} outgoing connections will select the ω+1 connection from **tried** with probability:

$$: \frac{\sqrt{\rho}(9-\omega)}{(\omega+1)+\sqrt{\rho}(9-\omega)}$$

ρ=0.9



ρ=0.1



ρ = ratio between #(addresses in tried) and #(addresses in new)

choose from the selected table an address to connect,
biasing towards addresses with fresher timestamps.

Attacking the Peer2Peer layer

- Key Observations:
  - a node will add an address to the ‘tried' table if it receives an incoming connection from another node.
  - a node will accept unsolicited ADDR messages. These will be added to the ‘new’ table.
  - nodes rarely will solicit information from DNS seeders and other nodes.

Eclipse Attack, I

- In the eclipse attack the victim is a node with a public IP.
  - attacker makes outgoing connection to the node using adversarial nodes. => ‘tried’ table gets full with fresh adversarial IP’s.
  - attacker uses ADDR messages to insert “**trash**” IP’s into the ‘new’ table of the victim.
  - finally, the attacker needs to wait for the victim node to restart (as nodes themselves will maintain existing outgoing connections). Restarts can happen because of a software update or even deliberately by the attacker (via a “denial of services” (DOS) attack).

Eclipse Attack, II

- The attacker can repetitively connect to victim node to ensure timestamps of adversarial nodes are fresh.
- If a ‘new’ address is selected the injection of trash IP’s ensures that with some probability the new node will not be responsive. As a result another coin flip will be attempted for the connection which can result to an adversarial IP.

Eclipse Attack, III

- Attacker now saturates the incoming connections of the victim.
  - The protocol allows for the same IP to occupy all 117 incoming TCP/IP connections.
- In this way it is impossible for other nodes to connect to the victim.
- Given the maximum number of connections is reached the victim will deny any other incoming connections.

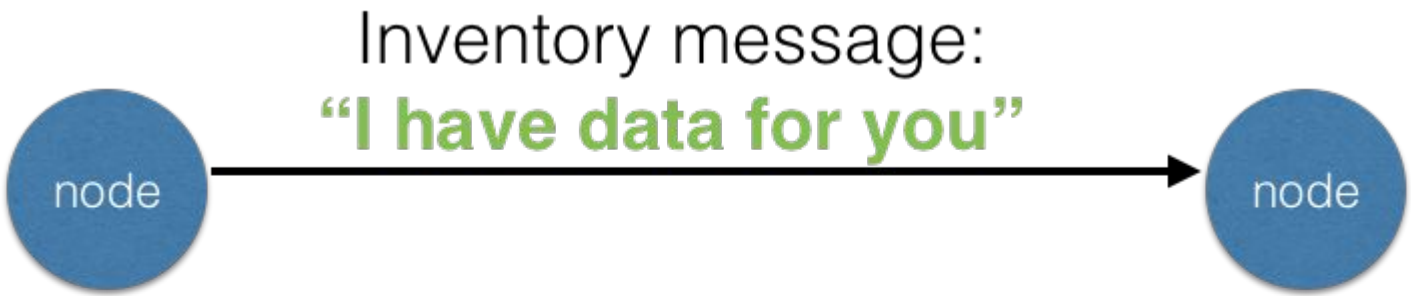
Eclipse Attack, IV

- Once the eclipse takes place, all communication of the victim (incoming/outgoing) will be routed via the attacker nodes.
  - victim’s transactions may be censored.
  - victim’s blocks can be dropped.
  - victim’s blockchain may be populated almost entirely by adversarial blocks!
- Moreover: the rest of the network will eventually completely forget about the victim node (a function **isTerrible** is executed periodically on the tables that will remove any node that has an over 30 days old timestamp and too many failed connection attempts).

Attack Countermeasures

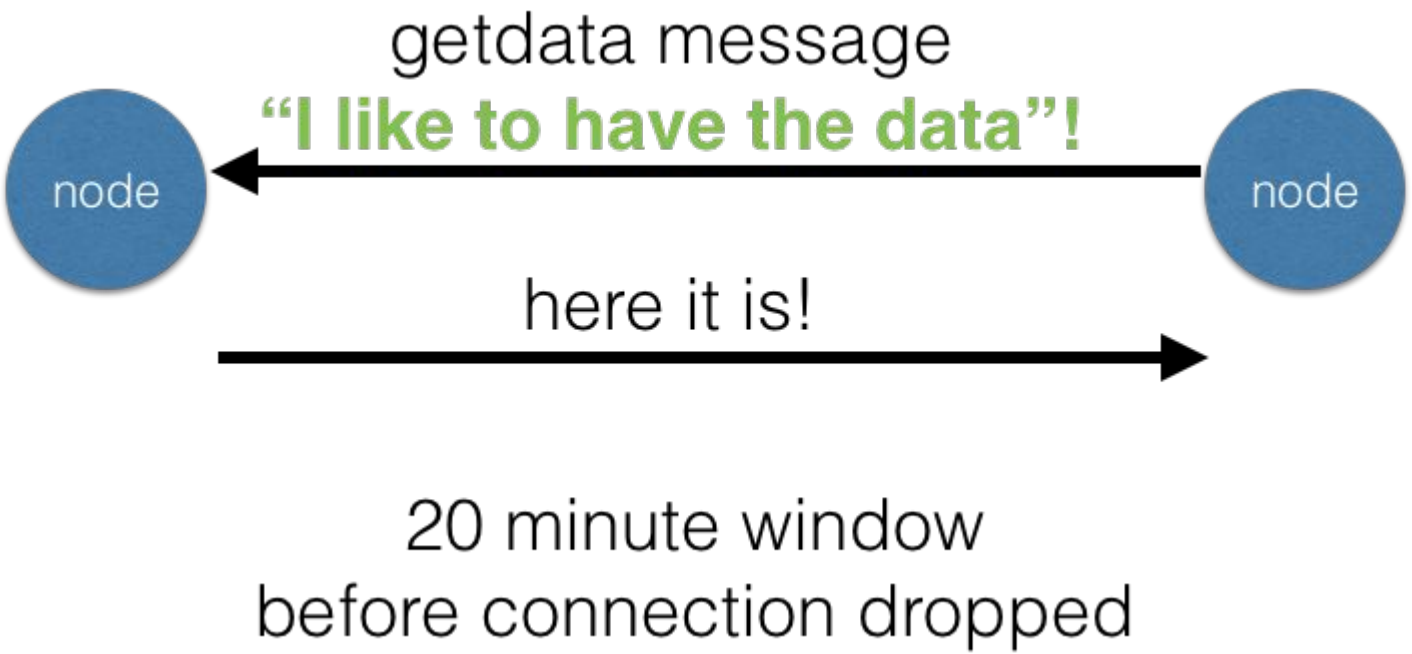
- Many mitigation techniques can be used:
  - ban unsolicited ADDR messages.
  - diversify incoming connections.
  - test before evicting addresses from the tried table.
- Nevertheless: the possibility of an attack cannot be zeroed.

Information propagation in Bitcoin

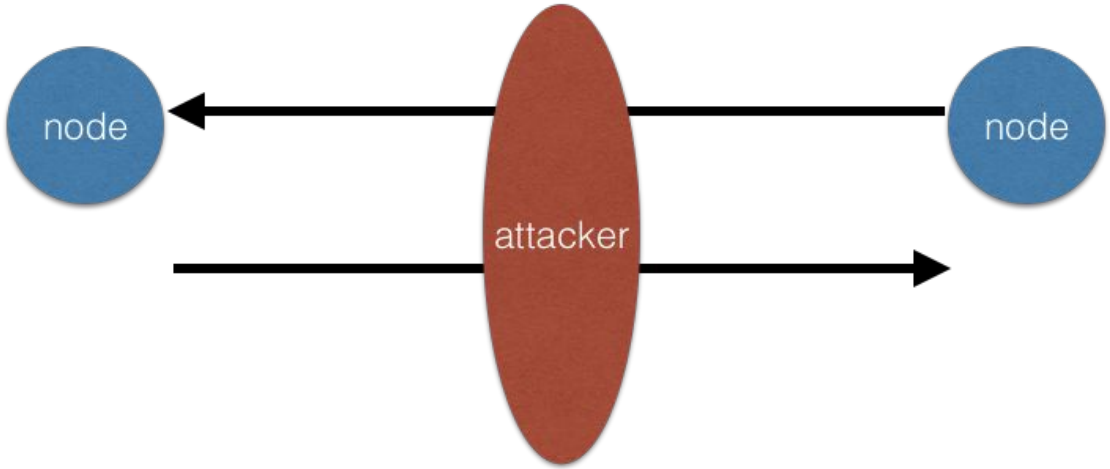


Field Size	Description	Data type	Comments
4	type	uint32_t	Identifies the object type linked to this inventory
32	hash	char[32]	Hash of the object

Information Propagation in Bitcoin, II



Possibility on Man-in-the-middle attacks



if attacker manipulates
message contents on either direction
it can delay information propagation by 20 minutes.

such delays can be extremely detrimental for security

Network Partitioning Attacks

- Internet traffic is routed via the Border Gateway Protocol (BGP).
  - BGP is the primary interdomain routing protocol.
  - Paths between networks need to be updated constantly as the Internet is an evolving infrastructure.
  - BGP is run by Internet Service Providers and other large networks that are connected. The participating nodes are called **autonomous systems** (AS).

BGP Highjacking

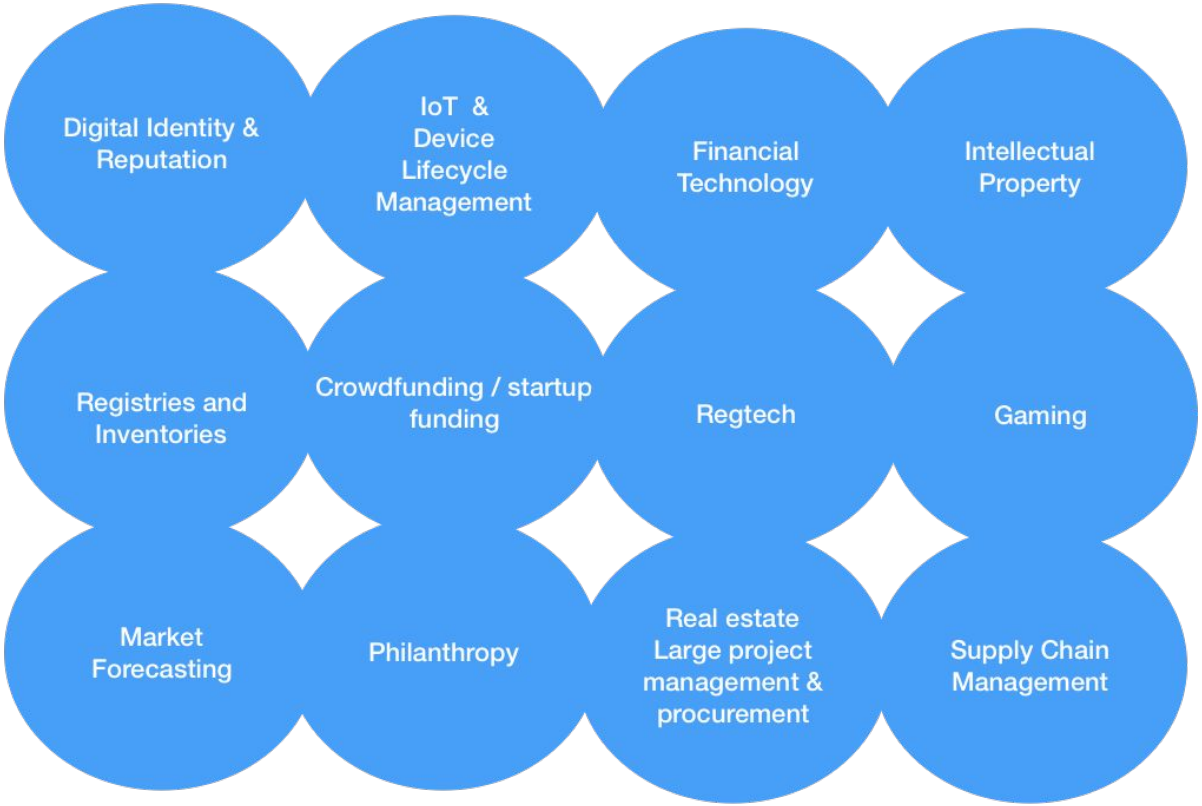
- An attacker running an AS, can announce that it can route a certain network path.
  - There is no actual validation performed of such announcements. Thus, a malicious AS can even advertise a non-existent path.
- Subsequently Bitcoin traffic can be filtered by the malicious AS.

Downside: such attack leave evidence in routing tables.
More advanced attacks exist (search e.g., for Erebus partitioning)

Network partitioning due to software error

- A software upgrade causes upgraded clients to drop old blocks and vice versa.
  - example: bitcoin version 0.8 in March 2013, older clients were forced into their own chain.

Applications of DLT

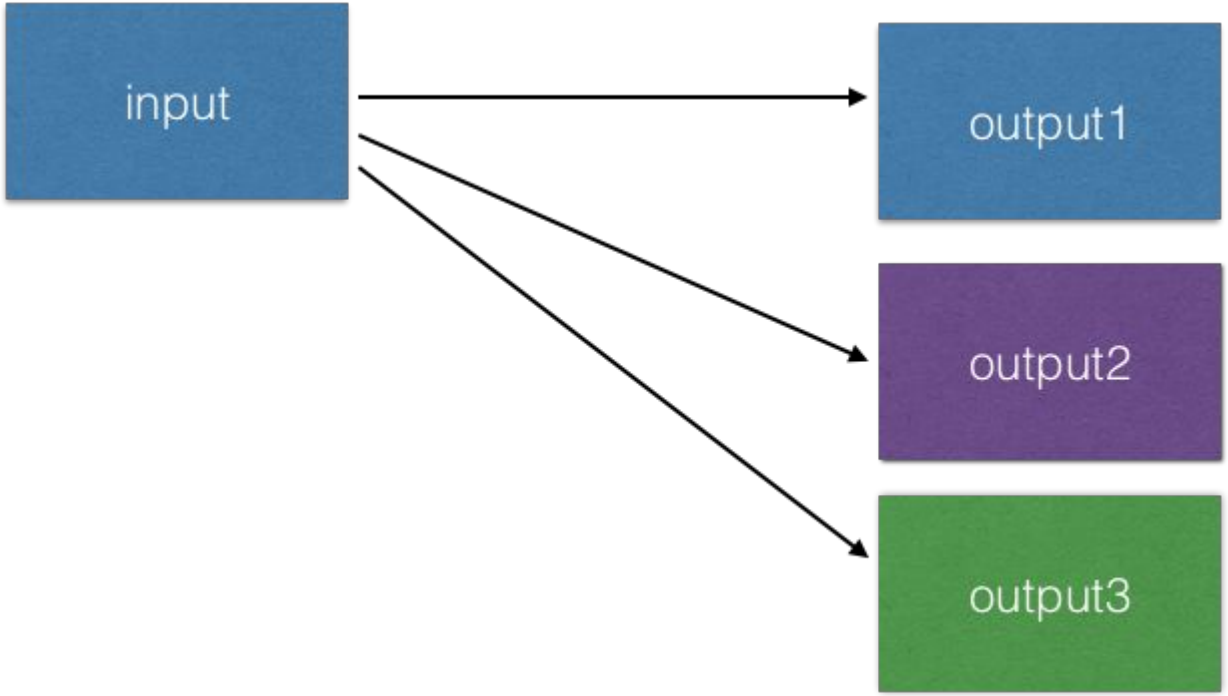


Fungibility and Bitcoin

- Even though bitcoin can be treated as being fungible, it is not:
  - the smallest denomination in the Bitcoin blockchain, “Satoshi”, can be tracked from account to account following some convention.

Colored Coins, I

- “Coloring" outputs so they represent specific assets.



Colored Coins, II

- Use of the OP_RETURN opcode (allowed to be followed by 80 bytes of data).
  - OP_RETURN signifies that a transaction output is invalid (and unspendable).
  - Paying to an OP_RETURN enables storing personal data on the blockchain.
- “sacrifice” one output to contain coloring information for the transaction.

Colored Coins, III

- Bitcoin transaction fees still apply (as transactions are necessary to be formed with OP_RETURN and the modicum of storage permitted).
  a. The secret-key of the account that is coloured controls asset ownership.
  b. Marker outputs (using OP_RETURN) can be used to further specify quantities transferred etc.
  c. Accounts should hold a balance to ensure the ability to transfer them onwards.

Coloured Coins, IV

- Bitcoin miners do not enforce proper rules of colouring (e.g., colouring should be preserved as balances move forward).
  - coloured transactions are treated as regular transactions by “colour-blind” miners.
- It is conceivable that colouring rules might not be respected by a miner acting maliciously.
- Parsing algorithms for colours should take this into account.

Example Applications

- Land Registry using coloured coins:
  - issue a new asset linked to land title.
  - store information in the asset that links to an information resource (e.g., one can insert a URL or an identifier for a **Torrent** file).
  - subsequently proof of ownership and transfer can be performed.

Example Applications, II

- Objects of value. E.g., everledger.io stores diamond certificate data in a blockchain.
- **Issue** how do you create a link between a physical object and a digital “thumbprint” ?
- Applications in **supply-chain management**.

Name Registries

- Use a blockchain to register names. Useful in the context of DNS (domain name system) and Public-key directories.
- Example **namecoin** (separate blockchain based on Bitcoin protocol), **blockstack** (piggybacking on the bitcoin blockchain as in the case of colored coins).

Use an independent DL or piggyback on existing?

Scheme	**Advantage**	**Disadvantage**
Piggybacking	Potential for higher assurance	engineer/program the protocol rules into existing protocol
Independent	Ability to customise protocol & enforce individual properties.	Might attract a small set of initial nodes. Might be less trustworthy at the onset.

Prediction Markets

- A prediction market enables trading on future events.
  - Simple example: “we will colonise Mars by 2040”.
    - participants bet in favour or against the event.
    - Market share of **YES** = α and **NO** = 1-α. Total investment = X.
    - Consider probability of event happening is *p.* Then expected Profit of YES = pX - αX.

Prediction Markets, II

- How is it possible to issue smart contracts, that control such outcomes.
- **Main challenge**: how to ensure that the blockchain can detect the outcome of an event.
  - Use an external trusted party that will vouch for the outcome.
  - Use a voting process from blockchain stakeholders that will vote that the outcome will take place.
    - (e.g., a proof-of-stake can back up that a certain event has been reached).

Financial Instruments

- Any type of financial instrument (assets that can be traded) can be tracked by a blockchain using the colored coin approach, a smart contract, or via a dedicated blockchain.
- Public Blockchains like Ethereum have been substantially used for crowd-funding: key concepts:
  a. An ERC-20 token
  b. A presale operation that enables users to buy the token for money.

ERC20 in Ethereum

ERC20 defines a set of basic functions to be implemented:

```
function totalSupply() public view returns (uint256);
function balanceOf(address tokenOwner) public view returns (uint);
function allowance(address tokenOwner, address spender)
public view returns (uint);
function transfer(address to, uint tokens) public returns (bool);
function approve(address spender, uint tokens)  public returns (bool);
function transferFrom(address from, address to, uint tokens) public returns (bool);
```

This enables building a wallet application that can handle basic ownership and transfer operation for the wallet. It also enables delegation of transfers.

An ERC20 smart contract enables issuing tokens in exchange for ether and then transferring tokens between owners as directed.

Gas has always to be spent to interact with the smart contract.

Crowdfunding via ERC20 - ICO

Initial Coin Offering (ICO) general plan

* Define an ERC20 smart contract.
* Advertise
* Accept funding
* Use funding to develop project
* Honour initial investors according to plan

What is a Security

- a fungible, negotiable, financial instrument that has some value. examples:
  - a stock (representing ownership of a public company) — **equity security**.
  - a bond (representing a creditor relationship with a government), —- **debt security**.

The Howey Test for Securities

- In the US, following, Securities and Exchange Commission (SEC) v. W.J. Howey Co, a security is
  - a contract, transaction or scheme whereby a person **invests** his money in a **common enterprise**.
  - .. and is led to **expect** profits solely from the efforts of the promoter or a third party.

Common Enterprise

- When does a venture constitute a common enterprise?
  - Horizontal commonality. Investors' assets are joined and they shared the risks and benefits of the enterprise.
  - Vertical commonality. The fortunes of the investors are linked and dependent upon the efforts of those seeking the investment.
    - **narrow** (investors' profits rise and fall together with promoter's) vs. **broad** (investors' profits depend on promoter's expertise and performance).

Securities Law

- From the financial instruments we have seen:
  - decentralised cryptocurrencies like bitcoin, ether etc. are less likely to qualify as securities (think: vertical commonality).
  - closed cryptocurrencies, ICOs, DAO tokens etc. will likely qualify as securities (e.g., the SEC has advised that this is the position).

Securities related obligations

- Become registered.
- File reports.
- Follow account and record keeping procedures.
- + more

Celebrity Endorsements

- Any promoter of a security has obligations.

> *Looking forward to participating in the new @LydianCoinLtd Token! #ThisIsNotAnAd #CryptoCurrency #BitCoin #ETH #BlockChain pic.twitter.com/a8kT9eHEko*
>
> *— Paris Hilton (@ParisHilton) September 3, 2017*

SEC: "Celebrities and others are using social media networks to encourage the public to purchase stocks and other investments. These endorsements may be unlawful if they do not disclose the nature, source, and amount of any compensation paid, directly or indirectly, by the company in exchange for the endorsement."

Criminal Activities Observed

- Ponzi schemes and securities fraud.
- Sales of prohibited items.
- Ransomware.
- Money laundering.
- Theft.
- Kidnapping.

Regulatory Technology (RegTech)

Fuse regulatory oversight with IT systems.

Examples:

* Use Machine Learning algorithms to serach for money laundering operations in transaction data recorded in a blockchain.

* Automate reports for specific transactions.

* Automate penalties

* ...