# Security Analysis of Large-Scale Computer Systems

Dairon Andrés Benites Aldaz
**daba2@kth.se**

November 3, 2022


Project Area: **IT Security**
Project Supervisor
**Ashish Kumar Dwivedi, Mathias Ekstedt & Zeeshan Afzal**

In submitting this work I am indicating that I have read the KTH's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

# 1 Security Analysis of one of the largest Bitcoin Exchange Platform

## 1.1 Background

> "Security isn't something you buy, it's something you do, and it takes talented people to do it right"

### 1.1.1 Coinbase Global, Inc.

Being an all American publicly traded firm, *Coinbase®* works mainly as a bitcoin exchange platform. Most of their employees work remotely, and the business has no physical headquarters. By trading volume, it is the biggest cryptocurrency exchange in the US. Brian Armstrong and Fred Ehrsam launched the business in 2012. As part of a wave of numerous significant tech businesses closing headquarters in San Francisco following the COVID-19 epidemic, Coinbase announced in May 2020 that it would close its San Francisco, California headquarters and transition to a **remote-first model**.

### 1.1.2 The good

Coinbase has been know to implement quite a number of interesting security features. They pride on calling themselves **"The most trusted crypto exchange"** as of the time of this writing they have more than 103 million users trusting their services. They offer 2-Step Verification on all accounts, password management and even machine learning models that evaluate crypto-transactions in order to cancel a transaction before it is submitted if it does not look quite right.

### 1.1.3 The bad

There have been several attacks that have raised concern among some users, to mention a few: in January 2019, they stopped all trading on **Ethereum** since there have been some signs of an attack on the network. After this incident, it has been known that they have acquired via absortion an Italian startup called *Neutrino*. They offered a *"blockchain intelligence platform"* even though their founders where actually related to the **Hacking Team** who have several claims of providing advanced internet surveillance technology to dictatorial governments.

### 1.1.4 The ugly

Coinbase revealed in August that a **sophisticated hacking attack attempt** had been made against them in mid-June.
This alleged attack made use of two Firefox browser zero-day vulnerabilities as well as :

- Spear-phishing and Social engineering techniques [1]

One of the Firefox flaws (CVE-2019-11707) could let an attacker increase their level of JavaScript access on a browser page, and the other could let them get out of the browser sandbox and run code on the host PC (CVE-2019–11708). The network was not breached, and no cryptocurrency was stolen thanks to the security team at Coinbase's detection and blocking of the attempt.

# 2 Main technical components

The main technical components of the "Coinbase environment" can be described as the elements needed to provide a certain level of service that gives user the capability to **buy, store and trade** different cryptocurrencies. (Mainly Bitcoin, Ethereum and Litecoin)

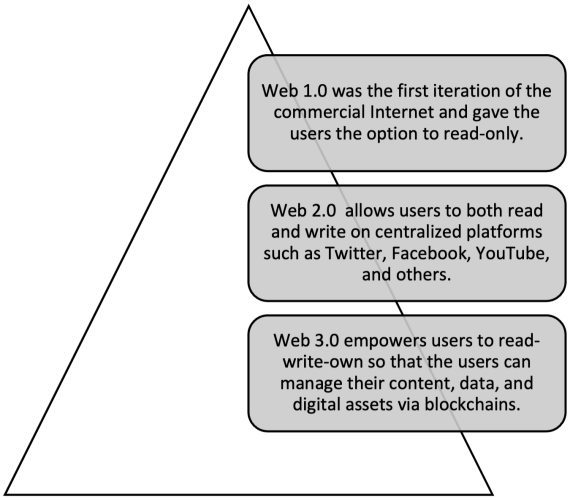
### 2.0.1 Products

For most of the products shown in Figure 1 Coinbase offers an API( Application Programming Interface) for other developers and merchants to accept payments.


[1] Such as sending bogus emails from hijacked email accounts and building a fake landing page from the University of Cambridge

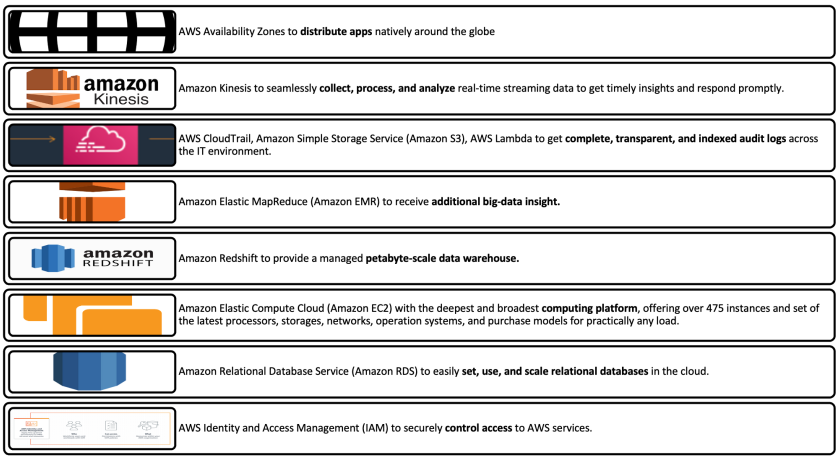
### 2.0.2 Web

Some of the elements mentioned above (and specially the ones that concern Coinbase Wallet®) are based on **Web 3.0**. This is a concept for public-blockchain based decentralised Internet. We can make some distintions with prior *popular* "standards":




### 2.0.3 Infrastructure

Most of Coinbase® services are provided through AWS (Amazon Web Services) since they cover most of their needs through some specific tools, such as:



# 3 Purpose of the system

The main purpose of the system can be defined as providing accessible and user-friendly experiences that make it easier to participate in decentralised finance **(buy, sell and store *crypto*)** while maintaining a high level of security. Among other purposes of the system is to maintain a high level of service due to the scale of the deployment (Global). Protect customer privacy and segment based on the tax requirements of each region where they belong. Offer a platform where transaction security is prioritized.

# 4 Delimitation

A large part of the ecosystem to be analyzed will be based on the scenarios contemplated in recent years (post-pandemic) 2019 onwards. In addition, reference will be made to specific historical events within the world of cryptocurrencies since many of these threats are collective to the rest of the exchange providers.
With regard to threats, those that fall within the following areas will be considered:

1. Social engineering
2. Phishing
3. Corporate Account Takeover (CATO)
4. Distributed Denial of Service (DDoS) Attacks
5. Ransomware
6. Access to confidential information
7. Identity theft
8. Trashing

Therefore, we will exclude from the list of possible threats scenarios related to the price variations of cryptocurrency products, threats related to the variation in the price of shares (convertible and non-convertible) belonging to or related to Coinbase Global, Inc.

# References

**Notes:** None yet.