SESSION 9

Risks in Crypto

Learning Objectives

- Explain risks related to cryptocurrencies
- Discuss various crypto exchange hacks
- Explain legal issues related to cryptocurrencies
- Discuss cryptocurrency regulations in various countries

SESSION 9

Introduction

Cryptocurrencies are a new addition to the cyber world and the financial system. In their short journey spanning just 10 years, they have changed the dynamics of the financial world, at least in the developed countries so far. However, they are still not regulated to a large extent and have some risks associated with them. With the rising popularity of cryptocurrencies, the amount of money being invested in these currencies has witnessed an exponential increase in the last couple of years. With this, they are becoming continuous targets for various crypto exchange hacks. In case of cryptocurrency transaction frauds, there is not even a proper regulatory framework in many countries such as India and China.

In light of such developments, it is being suggested in various countries to implement regulations so that public issue norms are not breached. It is now being viewed as a necessity to regulate the trade and exchange of cryptocurrencies for the protection of investors.

In this session, you will learn about various risks associated with cryptocurrencies. You will also learn about some of the major crypto exchange hacks happened over the past years. Next, you will be made conversant with the legal issues related to cryptocurrencies. Towards the end of the session, you will learn about the cryptocurrency regulations implemented in major countries of the world.

Exploring Various Risks in Cryptocurrency

[LO - Explain risks related to cryptocurrencies]

Cryptocurrencies are similar to e-money such as WebMoney and PayPal. It means that they have the same problems as classic e-payment systems. However, the working principle of cryptocurrencies adds more risks to them. For example, if you want to invest in cryptocurrencies, a huge mistake can be investing all your life savings on a technology which is extremely volatile.

Some of the examples of key risks with cryptocurrencies are as follows:

- **Extreme hype**: The development of Bitcoin and other cryptocurrencies has brought revolution in many aspects of finance. It has created a lot of hype with cryptocurrencies because most of the people do not know about the basic principles on which they operate and end up taking decisions based on hearsay.

  The crypto hype in 2017 is one of the major examples of hype. On June 4, 2017, bitcoin was valued at 2,550 dollars. The hype around bitcoin led a great number

of investors to invest. This led to a bullish run and by December 2017, bitcoin price witnessed a jaw-dropping rise to 19,500 dollars. However, throughout the year 2018, a crisis of confidence occurred among investors causing a historical drop to 3,300 dollars.

To avoid such scenarios, you, as an investor, must be well-versed with the finer aspects of a cryptocurrency before buying it. You should invest with a well-structured strategy rather than just going by the hype.

- **Security:** With the increasing demand for skills in cryptocurrencies, security expertise is not increasing in the same proportion. Many businesses and individual investors are dealing with problems such as large disappearances of their cryptocurrency, complex ransomware and extortion events.

  When the cryptocurrency exchanges or firms work in a centralized manner, they put the main security feature of decentralization provided by the blockchain technology at stake.

  As an investor, you must read and analyze the whitepaper of the cryptocurrency in which you wish to invest. This way you can judge the soundness of the cryptocurrency's protocol and assure yourself about any kind of possible bugs that might compromise the security of investments. However, any cryptocurrency's website will never reveal the flaws in its protocol and underlying technological architecture. Such a problem can be easily tackled by reading reviews on websites such as Reddit and Investdiva.com.

- **Volatility:** Volatility refers to the risk involved in the unexpected fluctuations occurring in the cryptocurrency market. The chance of sudden movements or fluctuations in a direction contrary to your expectations is ever-present which can lead to a loss of large amount of money invested in the market.

  The volatility risk can be resolved by having a long-term investment plan rather than looking for short-term gains. A long-term plan can convert volatility into an opportunity. You should know how to determine the best time to cash out, or to hold on to the cryptocurrency.

- **Liquidity:** In the context of cryptocurrencies, lack of liquidity is a scenario wherein it becomes difficult to sell them at a reasonable price within a timeframe when a cryptocurrency investor needs to liquidate his/her investment the most. Problem of liquidity is one of the major factors that leads to high volatility. However, this is not a core issue, but rather depends upon the perceived value of the cryptocurrency and number of people invested in it.

  When liquidity is low, it also increases the risk of price manipulation. This can drive the market in a situation in which an investor with deep pockets will buy a huge amount of cryptocurrency and earn big profits at a later stage.

  However, on the upside, with cryptocurrency investment becoming easily accessible and gaining widespread acceptance in due course of time, it might solve the problem of liquidity. Easy accessibility to cryptocurrency investments will be facilitated by an increase in the number of crypto currency exchanges deemed trustworthy.

The problem of liquidity can be effectively tackled by analyzing the acceptance, popularity and the number of exchanges on which a cryptocurrency is being traded. Lesser-known virtual currencies might lure you because of their potential but they can also cause trouble due to their lack of liquidity.

- **Unclear regulations:** One of the major risks related to cryptocurrencies is the lack of regulation. Earlier crypto investors did not have to worry about government regulations. However, with the surging demand for cryptocurrencies, this has become tougher to avoid. These risks were earlier overcome by a common anti-money-laundering (AML) approach. Various insurers have refused to provide any coverage to a client being engaged in cryptocurrency or related business until regulatory standards are in place.

Exploring Crypto Exchange Hacks

[LO - Discuss various crypto exchange hacks]

Since Bitcoin has made its debut, its prices have skyrocketed to a level that anyone could have never imagined. Today, one Bitcoin is worth thousands of dollars. However, the irreversible nature of cryptocurrency transactions makes them risky as once cryptocurrency gets stolen, it is not possible to recover it. The virtual marketplaces where crypto exchanges occur contain a large amount of digital cash which makes them an attractive target for hackers.

Over time, hackers have stolen millions of dollars' worth of cryptocurrencies from various exchanges. Some exchanges recovered from the attacks and some went bankrupt. Some of the biggest crypto exchange hacks arranged by year are as follows:

- **Mt. Gox part 1 (June 2011)**: Mt. Gox was the largest Bitcoin exchange that had over 70% of the trading volume. It had some issues with the exchange. In June 2011, the trading volume of Bitcoin increased massively with a decline in its price. This was allegedly caused by a hacker gaining control of the computer of an auditor of Mt. Gox. Due to the massive sell-off, the price of Bitcoin fell from $15 to as low as $0.01. The hacker reportedly acquired 2000 Bitcoins.
- **Mt. Gox part 2 (February 2014)**: Earlier, Mt. Gox was able to recover from the attack. However, in January 2014, an issue of delay in transactions was found in the platform. Then, on February 7, all the Bitcoin withdrawals were halted to identify and resolve the issues. Then the company issued a statement saying it was due to a bug in the Bitcoin code. On February 24, Mt. Gox stopped trading and their website went offline. It was discovered that a hacker infiltrated the network years ago and was siphoning coins the entire time. This infiltration resulted in the theft of 850,000 BTC having an approximate value of 460 million dollars.
- **Cryptsy (July 2014)**: The founder of Cryptsy announced the hacking of the exchange more than a year after its discovery by his technical team. The exchange was not allowing users to access their funds while the public did not know about the hack. Cryptsy tried to hide the hack by distributing the earned money to the affected users. The attackers inserted a Trojan into the code of Cryptsy which enabled them to transfer coins.

Around 13,000 Bitcoins and 300,000 Litecoin were stolen amounting approximately to 6 million dollars.

- **Mintpal (July & December 2014)**: In July 2014, Mintpal announced that millions of vericoins had been hacked from its exchange hot wallet. During this attack, Bitcoin and Litecoin funds were targeted. However, they were unaffected as they were in cold storage.

  In December 2014, 3700 BTC were stolen again and then the company went bankrupt, saying that all the Bitcoin had been stolen. However, later, its CEO was found guilty of selling 3700 stolen BTC on Bitcoin sales site LocalBitcoins.

- **Bitstamp (January 2015)**: In December 2014, an attacker targeted Bitstamp employees with phishing attempts. One of the employees downloaded a malicious file believing it to be from an authentic company source. This enabled the attacker to gain access to the hot wallet and password stored on the servers, which were made accessible through the compromised computer. The attacker took 18,866 Bitcoins from this wallet amounting to approximately 5 million dollars. The theft came into notice on January 4, 2015.

- **Decentralized Autonomous Organization (DAO) (June 2016)**: The DAO was a smart contract on the Ethereum network. It was created as a venture capital fund. When it was created, there was funding. In this, people could invest in ETH and receive DAO tokens. It was created so that companies could formulate proposals for digital applications which would subsequently be voted on by token holders. If the proposal got the desired number of votes, then they will get the required funding.

  It was extremely successful. It had more than 11,000 contributors who were able to raise more than 150 million dollars over a period of 30 days. During this period, many people raised concerns about its security flaws. Then an attacker exploited these flaws and drained almost 3.6 million Ether into a different DAO. It caused a large drop in the price of Ethereum, from $20 to $13. This attack is the reason behind the separation of ETH and Ethereum Classic. The developers decided to fork the Ethereum to rectify this massive security flaw in the DAO code.

- **BitFinex (August 2016)**: BitFinex is one of the largest cryptocurrency exchanges. However, it became a victim of a massive theft of Bitcoin in August 2016. It has implemented multi-signature wallets to increase the security of the users. These wallets were attacked and around 119,756 BTC were stolen. At that time, the value of stolen bitcoins was estimated to be 72 million dollars.

- **NiceHash (December 2017)**: NiceHash is a Slovenian cryptocurrency hash power broker that links buyers of hashing power with its sellers using the sharing economy approach. It was closed temporarily for 24 hours after being hacked in December 2017. In this attack, the wallet owned by NiceHash having 4,450 Bitcoin was emptied.

- **Coincheck (January 2018)**: In January 2018, Coincheck, an exchange in Tokyo, Japan was hacked. The attacker stole NEM coins having a worth of almost 500 million dollars. All the coins were stored in a single hot wallet and no security measures were implemented.

- **Coinrail (June 2018)**: Coinrail is a crypto exchange in South Korea which was hacked in June 2018. It faced a loss of about 40 million dollars.
- **Zaif (September 2018)**: In September 2018, Zaif suffered from an attack in which cryptocurrencies worth 60 million dollars were stolen.
- **Cryptopia (February 2019)**: Cryptopia, an exchange in New Zealand, suffered from two data security failures. In the first incident of failure, it lost cryptocurrency amounting to 16 million dollars. In the second failure, the attackers were also able to siphon an additional 1,675 ETH coins that were equivalent to about 180,000 dollars.

Figure 1 illustrates some of the major crypto exchange hacks:

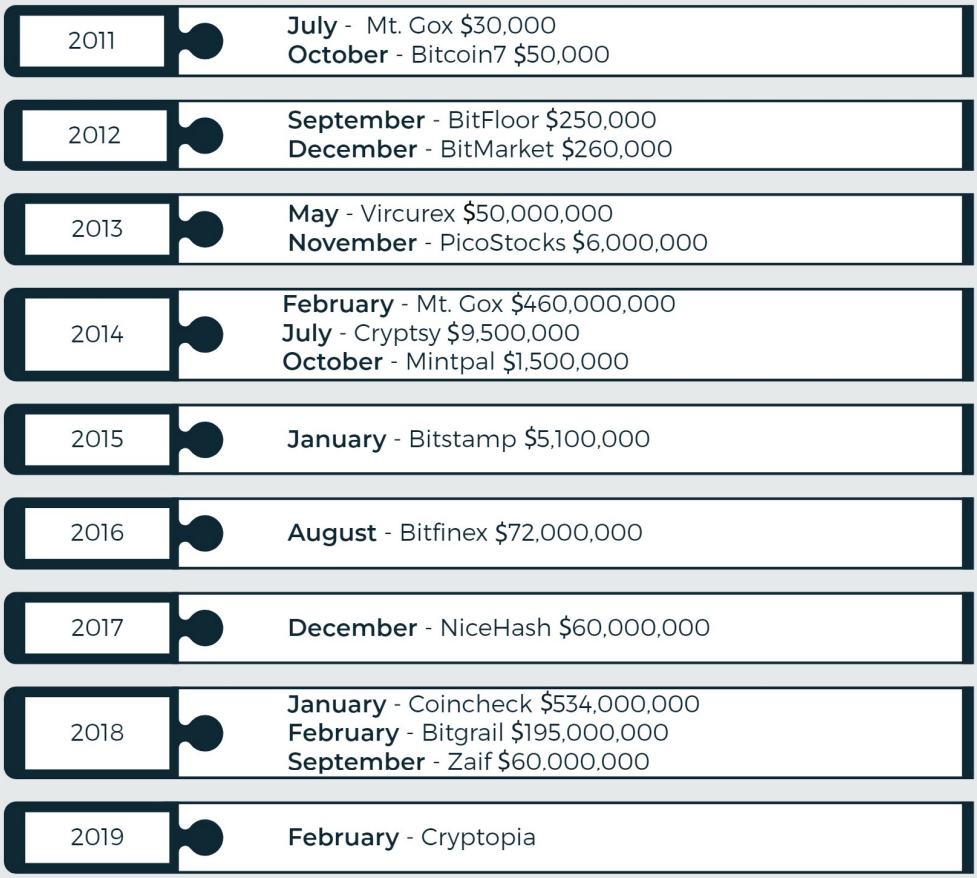

Figure 1: **Some Major Crypto Exchange Hacks**

Exploring Legal Issues in Cryptocurrency

10 min

[LO - Explain legal issues related to cryptocurrencies]

Cryptocurrency is a decentralized, anonymous, and unregulated form of digital currency that has become extremely popular in the last few years. It has mainly become popular due to its decentralized economy and usage of a peer-to-peer network.

The anonymity provided by cryptocurrency framework makes it a haven for illegal activities, such as money laundering and tax evasion, as the identity of criminals remains

hidden to a large extent. Now, most countries are getting alarmed and beginning to initiate legal action against such transactions. In some countries, cryptocurrencies are legal and in some, they are not. Some of the legal issues that cryptocurrencies have raised are as follows:

- **The validity of the transaction as a currency**: Generally, only government has the sole authority to manage currencies. Sometimes, the government delegates this authority to a central bank or any other authority. However, cryptocurrencies do not come under any regulatory framework. Therefore, they possess issues related to liquidity, operational risk, fraud, credit and solvency. The transactions are carried out on the Internet which can be of great risk. Cryptocurrency is unregulated and has digital form. There is no record about its accounting, stock or inventory.
- **Absence of a well-defined legal framework**: Most countries do not have a proper framework which can be used to control the value and the flow of virtual currencies. It becomes tough to monitor a decentralized currency.
- **The volatility of virtual currencies**: The value of virtual currencies is very volatile and suffers from various ups and downs that introduces instability in the market and economy.
- **Independent wallets**: Cryptocurrencies are normally stored in wallets and transactions are managed by private organizations which are not controlled by the government. The organizations do not have any liability in case of customer's loss as well as any type of financial crime committed by the use of these wallets.
- **Taxation**: One of the major concerns associated with cryptocurrencies is taxation. Due to the anonymous nature of cryptocurrencies, they can be used for tax evasion by means of hiding assets. In various countries such as US, cryptocurrencies are classified as a taxable asset. When a large amount of foreign currency is brought into a country, then it can destabilize the economy of the country.
- **Money laundering**: Another serious issue with cryptocurrency is money laundering. It is a key issue because it is easy to move cryptocurrency between countries without any problem.

Exploring Cryptocurrency Regulations

[LO - Discuss cryptocurrency regulations in various countries]

As you have learnt in the previous section, there were some legal issues with cryptocurrencies related to taxation and money laundering issues. Currently, there is no uniform regulation on cryptocurrency, and it differs from one country to another country. However, with time more countries are applying some regulations on cryptocurrencies. Some of the countries which have imposed their regulations on cryptocurrencies are as follows:

- **United States**: In the United States, a consistent legal approach is not defined, and cryptocurrency exchange regulations vary from state to state. Major regulatory bodies such as the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC) are working to provide effective consumer protection.

- **Canada**: In Canada, cryptocurrencies are not considered a legal tender, however, the Canada Revenue Agency taxes them. The cryptocurrency exchange regulations in Canada are also inconsistent. Canadian authorities brought all the entities (be it a firm or an individual) dealing in virtual currencies under the purview of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act in June 2014.

  There are inconsistencies in cryptocurrency exchange regulations at the provincial level. However, at the federal level, cryptocurrencies are treated as securities.

  As a proactive measure, in June 2018, Canadian authorities have issued draft amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. With these new amendments in place, cryptocurrency exchanges are bound to reporting obligations and are regulated at par with Money Services Businesses.
- **Singapore**: In Singapore, cryptocurrencies are not a legal tender. However, Singapore's tax authority treats Bitcoins as 'goods' and therefore, they levy Goods and Services Tax on them. The cryptocurrency exchanges and trading are legal in Singapore.
- **Australia**: In Australia, cryptocurrencies and exchanges are legal. According to the Australian government, cryptocurrencies should be treated as property, and subject to Capital Gains Tax (CGT). The cryptocurrency exchanges must register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and should identify and verify users.
- **Japan**: In Japan, cryptocurrencies and exchanges are legal. According to the Japanese government, cryptocurrencies should be treated as property, and subject to the Payment Services Act. The cryptocurrency exchanges must register with the Financial Services Agency (FSA).
- **South Korea**: In South Korea, cryptocurrencies are not considered legal tender and exchanges must register with Financial Supervisory Service (FSS).
- **China**: In China, cryptocurrencies are not considered legal and the People's Bank of China (PBOC) has banned financial institutions from handling Bitcoin transactions. Cryptocurrency exchanges are also illegal. It has put in place strict cryptocurrency regulations.
- **India**: In India, cryptocurrencies are not considered legal tender and crypto exchanges are legal. However, it is very tough for exchanges to operate. The tax status of cryptocurrencies is currently unclear. However, the chairman of the Central Board of Direct Taxation has said that anyone making profits from Bitcoin will have to pay taxes on them.
- **UK**: In the UK, cryptocurrencies are not considered legal tender and exchanges must be authorized and must comply with the Financial Conduct Authority (FCA).
- **Switzerland**: In Switzerland, cryptocurrencies are considered as assets and they are subject to the Swiss wealth tax. Exchanges must be registered with the Swiss Federal Tax Administration (SFTA).

SUMMARY

- Cryptocurrencies suffer from risks related to volatility, liquidity, security, hype, and unclear regulations.
- Some of the major crypto exchange attacks were on Mt. Gox, Coincheck, Bitgrail and BitFinex.
- Some of the major legal issues that arise in cryptocurrencies are due to their decentralized and anonymous nature.
- Currently, there is not a uniform regulation upon cryptocurrency, and it differs from one country to another country.
- In Switzerland, Australia and Japan, cryptocurrencies and exchanges are legal.