Topic 3: addressing the effects of cryptocurrency on global economic security

**Intro:**

Any kind of money that exists digitally or virtually and uses cryptography to safeguard transactions is known as cryptocurrency, also referred to as crypto-currency or crypto. Cryptocurrencies use a decentralized mechanism to track transactions and create new units rather than a central body to issue or regulate them.

**Key terms:**

Cryptocurrency: a type of digital currency where records are kept and transactions are validated by a decentralized system employing encryption as opposed to a central authority.

Cryptography: the skill of creating or deciphering codes.

Centralized: collected, monitored, and handled by one particular authority.

Decentralized: when a distributed network assumes control or authority over a centralized entity, which lowers transaction costs, reduces administrative responsibilities, and allows people to hold their own assets.

Economic security: the capacity of individuals, families, or communities to meet their basic requirements in a respectable and sustainable manner. This can change depending on a person's physical requirements, the surrounding environment, and current cultural norms.

**General overview:**

Any kind of money that exists digitally or virtually and uses cryptography to safeguard transactions is known as cryptocurrency, also referred to as crypto-currency or crypto. Cryptocurrencies use a decentralized mechanism to track transactions and create new units rather than a central body to issue or regulate them.

Utility, payment, security, and stable coins are the four main types of cryptocurrency  DeFi tokens, NFTs, and asset-backed tokens are further token types. The most widely used cryptocurrencies are payment and utility tokens.

Cryptocurrencies run on a distributed public ledger called a blockchain. This is a record of all transactions updated and maintained by currency holders.

Units of cryptocurrency are created through a process called mining. Mining uses computer power to solve complex math problems to generate coins. Users can also buy currencies from brokers and stores and spend them using crypto wallets.

When you own cryptocurrency, you don't own anything tangible. What you have is the key that allows you to send records or units of measurement from one person to another without a trusted third party.

Bitcoin has been around since 2009, but the application of cryptocurrency and blockchain technology is still increasing in the financial field, and more applications are expected in the future. Transactions such as bonds, stocks, and other financial assets may eventually be traded using this technology.

**Parties involved**:

Some of the main major companies dominating the cryptocurrency market are: Bitmain (China), NVIDIA (US), Xilinx (US), Intel (US), Advanced Micro Devices (US), Ripple Labs (US), Ethereum Foundation (Switzerland), Bitfury Group (Netherlands), Coinbase (US), BitGo (US), Binance Holdings (China), Canaan Creative (China), Bitstamp (Luxemburg), Ifnex (Hong Kong), Ledger SAS (France), Xapo (Hong Kong), Alcheminer (US).

**UN involvement:**

A number of measures have been recommended by UNCTAD to stop the growth of cryptocurrencies in developing nations. To achieve complete financial regulation of cryptocurrencies, the agency asked authorities to regulate crypto exchanges, digital wallets, and decentralized finance.

**Possible Solutions**

**Diversifying security measures**

As the business world looks for the best ways to ensure that innovative brains from all walks of life are represented, diversity is a subject that is receiving more and more attention. The security community, like every other sector, continues to work to foster an inclusive atmosphere that fosters innovation and growth.

We are creating a series of material highlighting the bright minds shaped from distinctive experiences and backgrounds that continue to push our industry forward in keeping with Think Curity's mission to bring the most crucial subjects and areas of growth to the fore in the private security business.

**Improve cybersecurity**

Make computer updates. Your laptops, desktops, and mobile devices will always have the most recent threat protection if you regularly update them.

Restrict access. It should go without saying that only people who work for your company should have access to your computers and accounts.

Check out your workers. The amount of companies that use software packed with sensitive data and information and don't run background checks on their personnel is startling.

Create secure passwords. There is a good reason why many login pages have a password strength indicator meter.