**Unit 4-3 Notes**

**Tokens and Second-Generation tokens**

**3.1 Tokens**

* It is a self-authenticating data packets that represents a rare digital bit of information.
* It gains ability to represent themselves and prove authenticity automatically because they generated on blockchain.
* Tokens represent programmable assets or access rights, managed by a smart contract and an underlying distributed ledger.
* Token is like a cryptocurrency, it can act as bearer instrument and used to transfer value between two parties over a network.
* They are accessible only by the person who has the private key for that address and can only be signed using this private key.
* These are very flexible in nature.
* It is an object of value itself, or representation of any other asset on a digital ledger.
* A token can be native which serves as an incentive to help protect the network from attack and has governance rule-set.
* example is Bitcoin which is being paid to miners for block creation and validation.
* Ether; which is used for payment of transactions to the nodes carrying out block validation and confirmation.
* This is a perfect example of a token economy as it is reward based on the systematic reinforcement of target behavior.
* Tokens are not a new thing and have existed since long before the emergence of blockchain. Traditionally, tokens can represent any form of economic value.
* Shells and beads were probably the earliest types of tokens used.
* Other types of tokens are, for example, casinos chips, vouchers, gi cards, bonus points in a loyalty program, coat check tokens, stock certificates, bonds, concert or club entry tokens represented by a stamp on your hand, dinner reservations, ID cards, club memberships, or train or airline tickets.
* Most tokens have some inbuilt anti-counterfeiting measures, which may be more or less secure, in order to prevent people from cheating the system.
* Paper money or coins are also tokens.
* Tokens are furthermore used in computing, where they can represent a right to perform some operation or manage access rights.
* A web browser, for example, sends tokens to websites when we surf the web, and our phone sends tokens to the phone system every time we use it.
* A more tangible form of computer tokens is tracking codes that you get to track your parcel with postal services, or QR codes that give you access to a train or plane.
* In psychology, tokens have been used as a positive reinforcement method of incentivizing desirable behavior in patients, especially in a hospital setting.
* Cognitive psychology uses reward tokens as a medium of exchange that can be exchanged for special privileges within the setting of a hospital stay.
* Recyclable bottles are a good analogue example for a token.
* In some countries, bottles you buy in supermarkets are issued as tokens, as they have a recycling value of usually a few cents printed on them.
* This is money that you pay on top of the initial price of the product and has become a method for governments to encourage the recycling of materials and subsequent reduction of litter in public places.
* If you return the bottle to the supermarket or other collecting entities, you will get reimbursed with the recycling value stated upon the token you return – the bottle.
* Losing the bottle is equivalent to losing money.
* A garbage bag could also represent a recycling token if it is issued with a recycling value.
* In some parts of Switzerland, for example, you cannot just throw out trash in a bin in a random bag.
* You must pay for the bag up front, which includes a dumpster fee, and you can only use those bags to dispose of your trash.
* As opposed to most other countries, where you pay your garbage bill monthly, as part of your utility bill tied to the rent of your apartment or house,
* this system requires you to purchase these special plastic bags.
* These tokenized plastic bags come at a higher cost than regular supermarket plastic bags and are issued and managed by local authorities.
* Cryptographic tokens represent a set of rules, encoded in a smart contract – the token contract.
* Every token belongs to a blockchain address.
* These tokens are accessible with a dedicated wallet so ware that communicates with the blockchain and manages the public-private key pair related to the blockchain address.
* Only the person who has the private key for that address can access the respective tokens.
* This person can, therefore, be regarded as the owner or custodian of that token.
* If the token represents an asset, the owner can initiate transfer of the tokens by signing with their private key,
* which in turn generates a digital fingerprint or digital signature.
* If the token represents an access right to something somebody else owns,
* the owner of that token can initiate access by signing with their private key, thereby creating a digital fingerprint.
* If the token represents a voting, the owner of that token can vote by signing with their private key, creating a digital signature

**3.2 TOKEN GENERATION**

**First Method:**

Tokens created by sending a special transaction on bitcoin that had a small message.

This message says that some new assets had been created and were credited to a Bitcoin address.

**Second Method:**

* Tokens created by the complex transactions developed by blockchains.
  + Example: Ethereum foundation improved token technology by building a framework for the programming of tokens and allowing them to be used for more complex tasks.

**3.3 Token Types**

* Application Stack Tokens could be classified as work/utility, security or asset-backed token.

**First one is A work or utility token**

* It can be used as access right to contribute to a network like a DAO and receive reward for carrying out a particular task.
* This kind of token can also be exchanged for a service or product.
* A scarce utility token on a high-demand useful service can create massive value for holders of such token.

**Second one is Security token**

* **It** gives holders right of equity in your venture.
* Holders can lay claim to revenue or profit of the venture. Issuers of such tokens promise returns to holders.
* Any token that passes the Howey Test is considered an investment contract or simply a Security token
* this has been a long standing battle with Regulators still trying to find the right legislation for the industry.
* An example Security token is ERC1411

**And the third one is Asset-backed tokens**

* **These** are backed with tangible assets like bonds, stocks, properties, gold, car, etc.
* The tokens represent the physical assets and transferring from one person to another confers the new holder as the owner of such asset.

**3.4 Token Standards**

There are different forms of tokens with multiple properties and functionalities.

ERC 20

* + It is on Ethereum network
  + These tokens were used for crowdfuncing
  + The first blockchain tokens were the native tokens of state-of-the-art public & permissionless blockchains like Bitcoin, Ethereum, and the like.
  + The role of the native token in a blockchain, therefore, is to encourage a disparate group of people who do not know or trust each other to organize themselves around the purpose of a specific blockchain
  + With the advent of Ethereum, however, tokens have moved up the technology stack and can now be issued on the application layer with a few lines of code.
  + Such application tokens can have simple or complex behaviors attached to them.
  + Ethereum made it particularly easy to issue tokens with a few lines of code.
  + They developed a standardized smart contract, the ERC-20 standard, which defines a common list of rules for Ethereum tokens,
  + including how the tokens are transferred from one Ethereum address to another, and how data within each token is accessed.
  + These relatively simple smart contracts manage the logic and maintain a list of all issued tokens, and can represent any asset that has features of a fungible commodity.
  + A vast majority of early tokens issued on the Ethereum blockchain have been ERC-20 compliant fungible tokens,
  + where every token has an identical value with any other token of the same kind.
  + They can be fungible and therefore easily traded.
  + The native token on the Ethereum platform is Ether, KIN as an example could be an ERC-20 token created from the KIN ICO.
  + Each Ether and KIN square measure cryptocurrencies (AKA tokens) on the Ethereum network, however, one may check with KIN as “a token” to differentiate it from cryptocurrencies that use their own platform/ network/blockchain.

ERC 721

* + Main use of this is digital collectibles
  + First implemented in cryptokitties
  + ERC-721 introduced a free and open standard that describes how to build so-called non-fungible tokens on the Ethereum blockchain.
  + This has introduced the era of building more complex features into the tokens.
  + This standard has made it easy to create a token that represents any type of collectible, artwork, property, or personalized access rights, just to name a few examples.
  + These non-fungible tokens have special properties that make the token unique, or that are tied to the identity of a certain person,
  + and therefore represent less fungible or non-fungible assets and access rights.
  + They might pave the way for one of the most interesting use cases.
  + ERC-721 introduced a much richer spectrum of smart contract standards that exceed the possibilities of the fungible tokens that dominated the early days of token sales

ERC1411

* particularity of ERC1411 tokens is that they cannot be freely transferred like traditional ERC20 tokens:
* a third party is responsible for authorizing or not the transfer of these digital objects to comply with the laws and state regulations managing the underlying assets they represent.
* This authorization is managed by the smart contract through which these assets were generated.
* Digital assets thus adapt to existing law and it is likely that Security tokens will benefit most quickly from a legal framework,
* their existence representing only a simple technical evolution of traditional financial products.
* While there are other much more exotic forms of tokens.
* the most widely used are included in these three broad classifications.
* which already represent several thousand of assets with highly variable interest and value proposition.
* **The blockchain**is the foundation offering trustless transactions, fast settlement times, security and the network on which all higher levels in the stack are built.
* The blockchain offers issuers and regulators **visibility**and provides investors with connectivity and discoverability leading to **liquidity**.

**3.5 SECOND GENERATION TOKENS**

* Tokens saw a surge in popularity in 2017 and 2018, though recently interest has faltered due to the high level of fraud and the failure of many projects.
* However, a new spin on tokens has begun to gain a footing that addresses some of the core questions about the innate value of a token, such as what does it mean to own something “rare” and is it rare enough when it is just software? The two direction that tokens have taken are referred to as stable coins and security tokens.
* A stable coin ties its value to that of another asset such as a government-issued currency. Interoperability between cryptocurrency and traditional financial instruments is a massive issue across blockchains.
* **Stable coins** are a way for the old and new worlds of finance to meet. They interface with traditional fiat systems and offer a more palatable instrument that looks and feels like fiat currency.
* The first stable coin that gained a footing was Tether back in 2014, originally called Realcoin. The concept is simple, keep funds in a bank account that are equal to the number of Tether.
* However, it has had a rocky road with questions on transparency in terms of whether it had held the equivalent currencies in reserve.
* In addition, it had a system breach in 2017, and a hacker made off with over US$30 million worth of Tether.
* Another fascinating development is the U.S. government regulation of 1:1 currency tokens. Gemini, Circle, and a few others established a crypto exchange 1:1 US dollar token that is regulated by the U.S. government and is audited by a third party. With withering trust in Tether, this is a welcome reprieve for crypto traders who would like the stability of US dol- lars and the fluidity of a token.
* Stable tokens may be able to experience the same explosion in popularity thanks to the work of companies like Silamoney.com that has created an application programming interface (API) platform with a developer suite that issues stable coins on Ethereum blockchain called Sila tokens.
* **Security tokens (STOs)** are tied to the value of an outside asset such as equity in a company, ownership of a bond, or even a commodity like oil.
* The Venezuela Petro token is an exciting development as it is both issued by a sovereign government and was backed by oil, the country’s greatest commodity.
* The Petro was met with a high level of skepticism, indeed President Trump banned U.S. citizens from buying Venezuelan cryptocurrency.
* Unfortunately, corruption in Venezuela prevented the Petro from gaining much traction and sadly this was used by the Venezuelan government as an excuse to raid the bank accounts of its citizens.