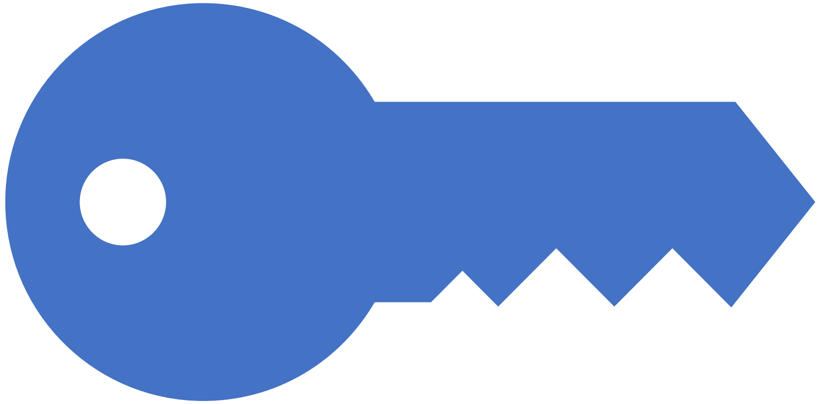


Mr Pham Thai Ky Trung

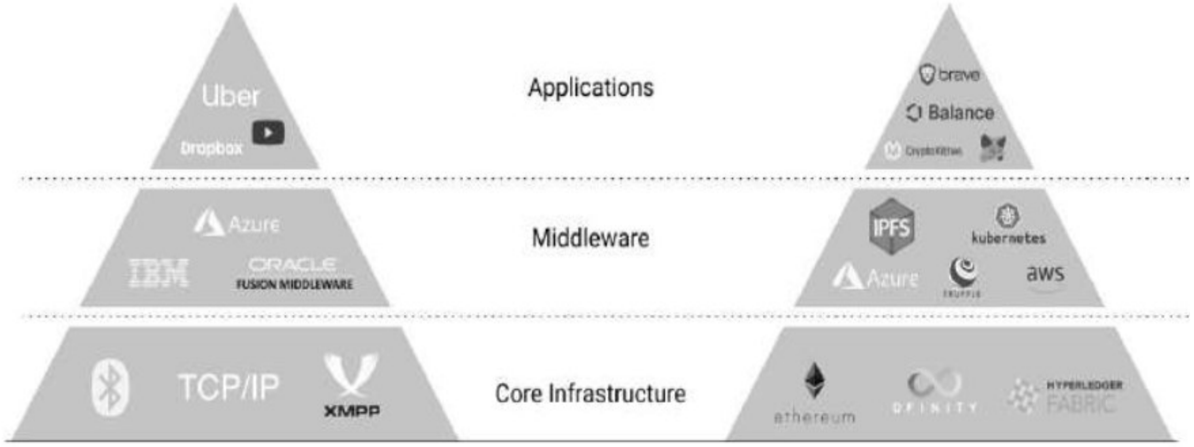
Lecture3 : Technology behinds Blockchain

Learning Objectives

- Gain a deeper understanding of how blockchain technology works
- Learn about the basic components of the blockchain technology stack
- Review how a transaction works on a blockchain from start to finish
- Examine how blockchain wallets work
- Understand how the SHA-256 cryptographic hash algorithm works
- Look at how mining works and the different options for mining digital tokens
- Discuss how blockchain itself can be used to improve the overall IT infrastructure

Comparing the Internet and blockchain technology stacks

- Blockchain Technology ~ Internet:
  - **Core infrastructure layer**: This layer consists of general protocols like TCP/IP to establish the communication between computers and the network architecture.
  - **Middleware layer**: Middleware refers to a set of tools, dev-tech, and services that make application development faster and easier.
  - **Application layer**: Built on top of core infrastructure and middleware live applications. These are the tools and products you are likely used to using such as Gmail or Shopee, etc.

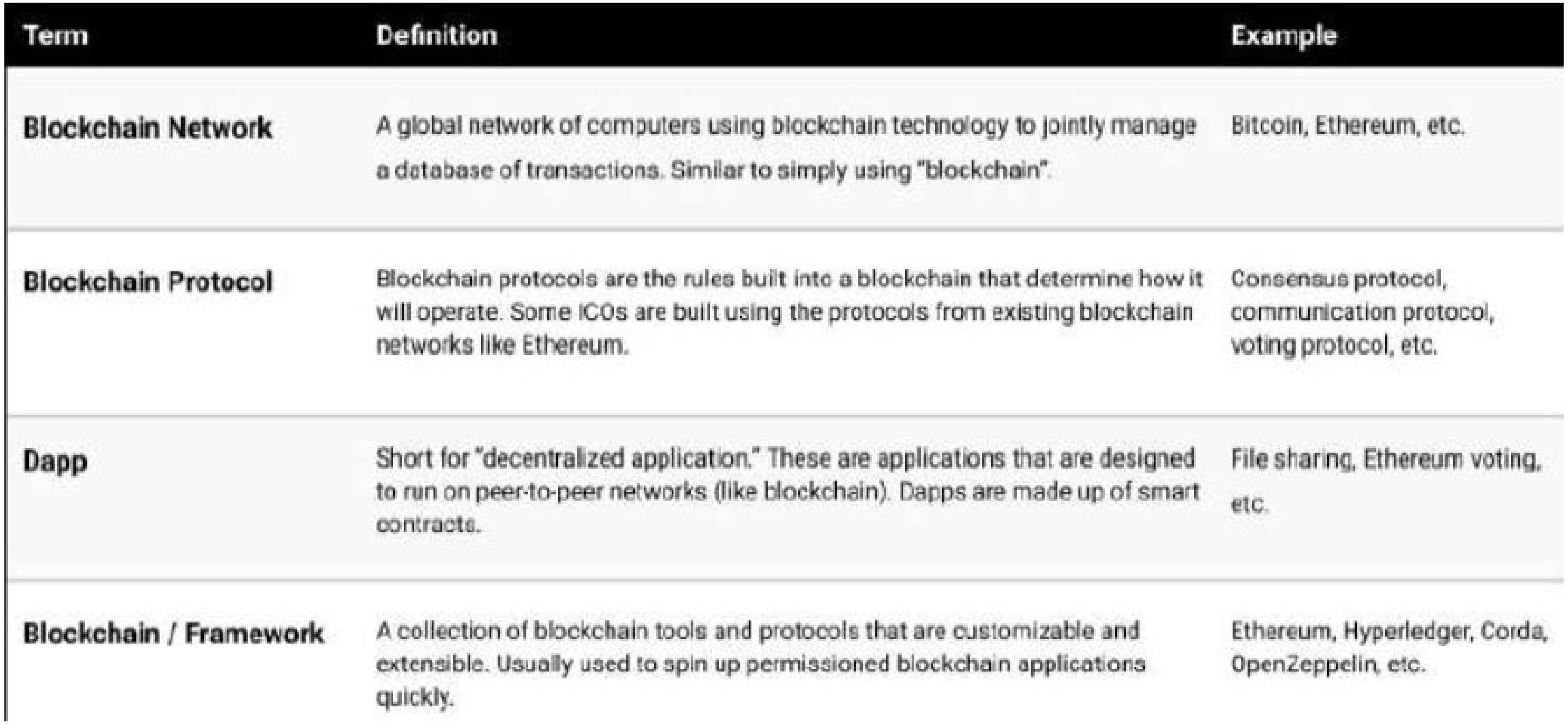


The bottom layer, or core infrastructure of a blockchain, is made up of a complex piece of software that is typically programmed in JavaScript, C ++, Python, or Go -> called **Protocols** (define behaviors for communication and transaction on the network).

A Server (*store***)- Client (***retrieve***) ~ Nodes (***both store & retrieve file***)** (*core blockchain protocols rely on nodes being able to store a complete copy of the entire blockchain*)

Blockchain Terminology

- The software is not an operating system but makes use of GNU (popular free software operating system) capabilities and TCP/IP Internet protocols to allow different types of devices running different operating systems to communicate across the network.
- Also built into the software are rules for creating new blocks using **consensus** (i.e. **Proof of Work** and longest chain rule) and rules for how the blocks will be secured via encryption.



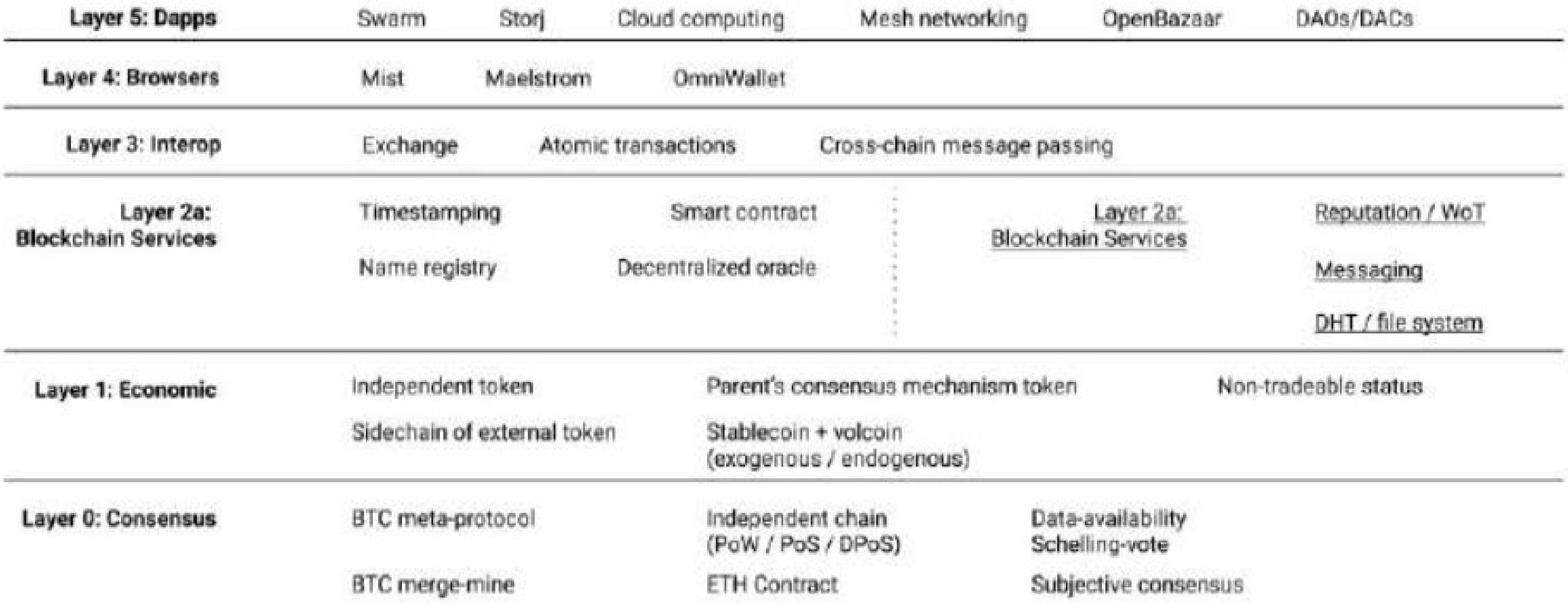
Term	Definition	Example
Blockchain Network	A global network of computers using blockchain technology to jointly manage a database of transactions. Similar to simply using "blockchain".	Bitcoin, Ethereum, etc.
Blockchain Protocol	Blockchain protocols are the rules built into a blockchain that determine how it will operate. Some ICOs are built using the protocols from existing blockchain networks like Ethereum.	Consensus protocol, communication protocol, voting protocol, etc.
Dapp	Short for "decentralized application." These are applications that are designed to run on peer-to-peer networks (like blockchain). Dapps are made up of smart contracts.	File sharing, Ethereum voting, etc.
Blockchain / Framework	A collection of blockchain tools and protocols that are customizable and extensible. Usually used to spin up permissioned blockchain applications quickly.	Ethereum, Hyperledger, Corda, OpenZeppelin, etc.

Blockchain Terminology (cont)

- ○Anyone can participate and install the blockchain software from the open-source community (sourceforge.net or bitcoin.org)
- ○By installing the software and downloading the blockchain, you are not necessarily running a "full node" on the blockchain and your node is not yet monetizable [**có thể kiếm tiền**]
- ○Running a node on a blockchain only becomes monetizable when the node agrees to participate in the contest to actively maintain the security of the blockchain by joining the "**community of verifiers**."
- ○Depending on the way the core blockchain protocols are configured, a full node might be considered to be a "**miner**" and would be rewarded with the native digital token (**bitcoin, ether, etc.)** for winning the competition to create a block and for verifying the transactions that were collected into the block.

The many layers of blockchain

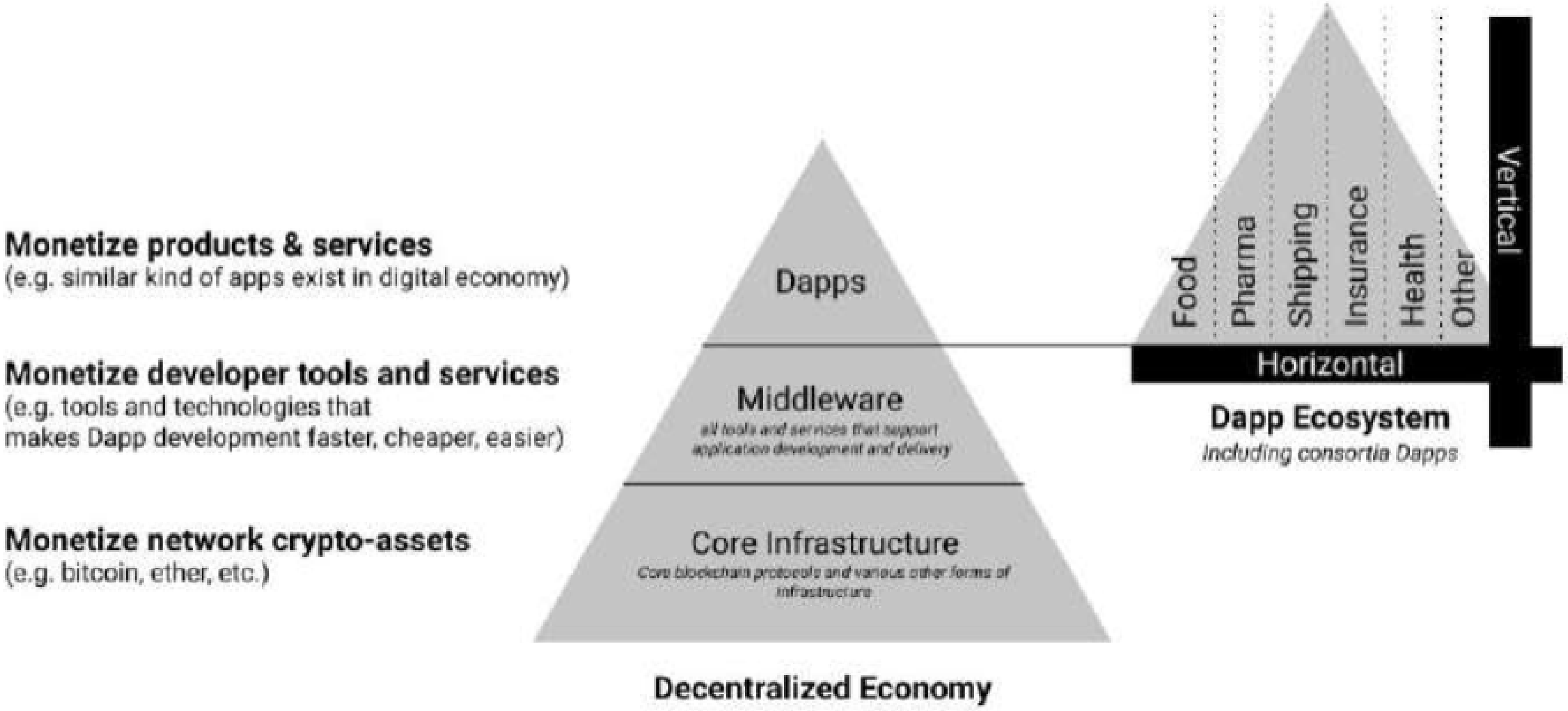
- Both the smart contract layer as well as the storage and content layer describe platforms for developing blockchain-based applications.



Layer 5: Dapps	Swarm	Storj	Cloud computing	Mesh networking	OpenBazaar	DAOs/DACs
Layer 4: Browsers	Mist	Maelstrom	OmniWallet			
Layer 3: Interop	Exchange	Atomic transactions	Cross-chain message passing			
Layer 2a: Blockchain Services	Timestamping Name registry	Smart contract Decentralized oracle	Layer 2a: Blockchain Services	Reputation / WoT Messaging DHT / file system		
Layer 1: Economic	Independent token Sidechain of external token	Parent's consensus mechanism token Stablecoin + volcoin (exogenous / endogenous)	Non-tradeable status			
Layer 0: Consensus	BTC meta-protocol BTC merge-mine	Independent chain (PoW / PoS / DPoS) ETH Contract	Data-availability Schelling-vote Subjective consensus			

Monetizing the Blockchain

- Monetizing the Core Infrastructure
- Monetizing Middleware
- Monetizing the Decentralized Economy

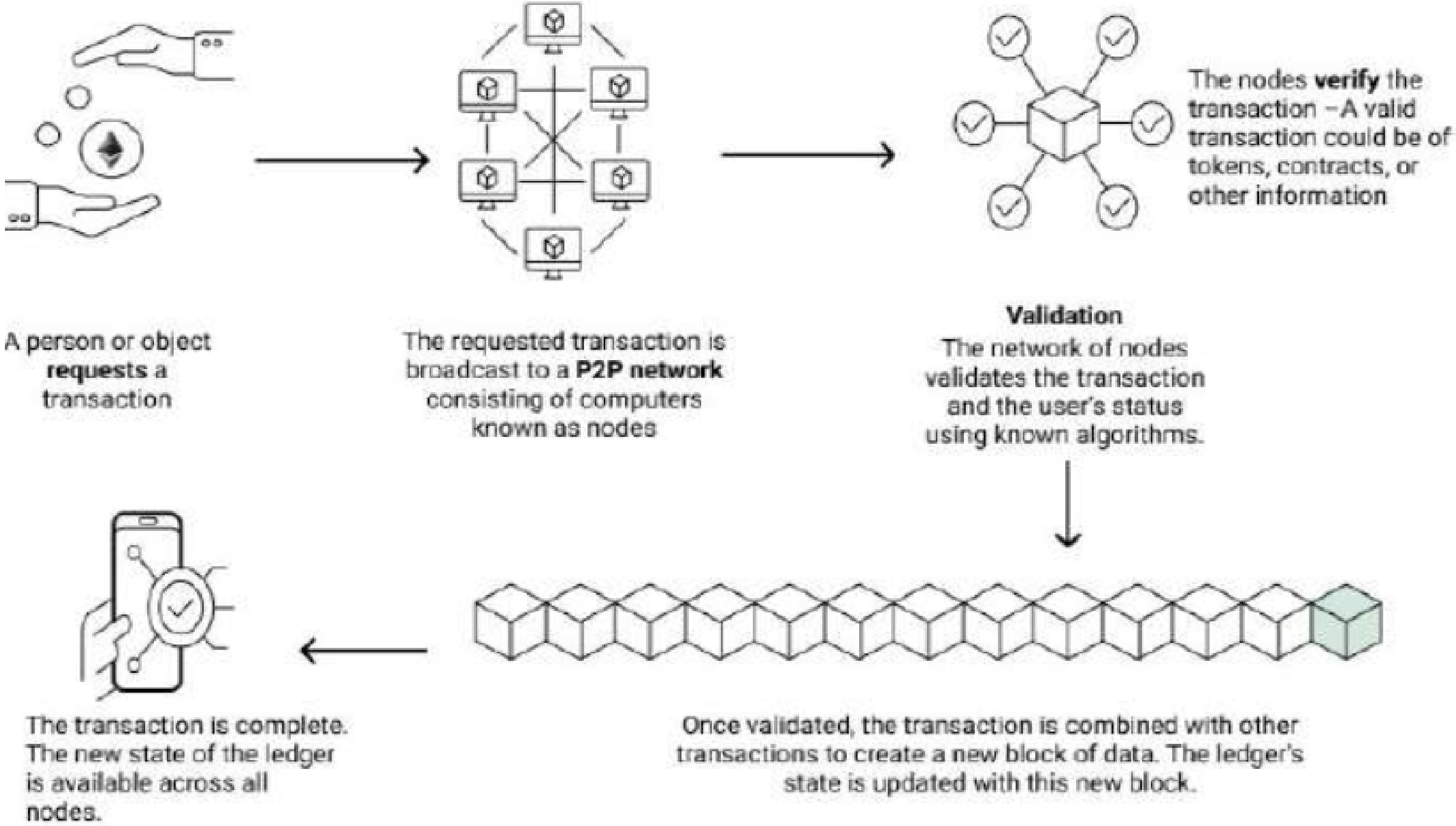

Monetize products & services
(e.g. similar kind of apps exist in digital economy)
Monetize developer tools and services
(e.g. tools and technologies that makes Dapp development faster, cheaper, easier)
Monetize network crypto-assets
(e.g. bitcoin, ether, etc.)
Dapps
Middleware
all tools and services that support application development and delivery
Core Infrastructure
Core blockchain protocols and various other forms of infrastructure
Decentralized Economy
Food
Pharma
Shipping
Insurance
Health
Other
Vertical
Horizontal
Dapp Ecosystem
Including consortia Dapps

Monetizing the Core Infrastructure

- Digital tokens are a key component of blockchain technology.
- A digital token simply represents value on a blockchain network
  - For example: earn miles with airlines, and can use those miles on functions like flights but also trade or sell them at times
- Tokens for blockchain networks come in many shapes and sizes, and people are experimenting with how to codify and incentivize participants in blockchains through token-based economic frameworks
- Bitcoin and ether can be considered examples of "**intrinsic**" [Nội tại] or "**native**" [Bản địa] digital tokens since each is built into its network. These tokens only exist as entries in a blockchain ledger and must be reached with a user's private key in order to receive any value for them.
- Many other types digital tokens and the number grows every day "**stablecoins**" that are pegged to a fiat currency (like a USD or Euro), **USDC, DAI, Tether (USDT)**

Monetizing the Core Infrastructure

- Many groups launched New blockchain with their own digital tokens
- Greater usage of a given blockchain(more transaction volume, more middleware and application will drive greater value of its token underlying token due to network effects.



A person or object **requests** a transaction

The requested transaction is broadcast to a **P2P network** consisting of computers known as nodes

The nodes **verify** the transaction – A valid transaction could be of tokens, contracts, or other information

Validation
The network of nodes validates the transaction and the user's status using known algorithms.

Once validated, the transaction is combined with other transactions to create a new block of data. The ledger's state is updated with this new block.

The transaction is complete. The new state of the ledger is available across all nodes.

Diagram of transactions on a blockchain

Monetizing Middleware

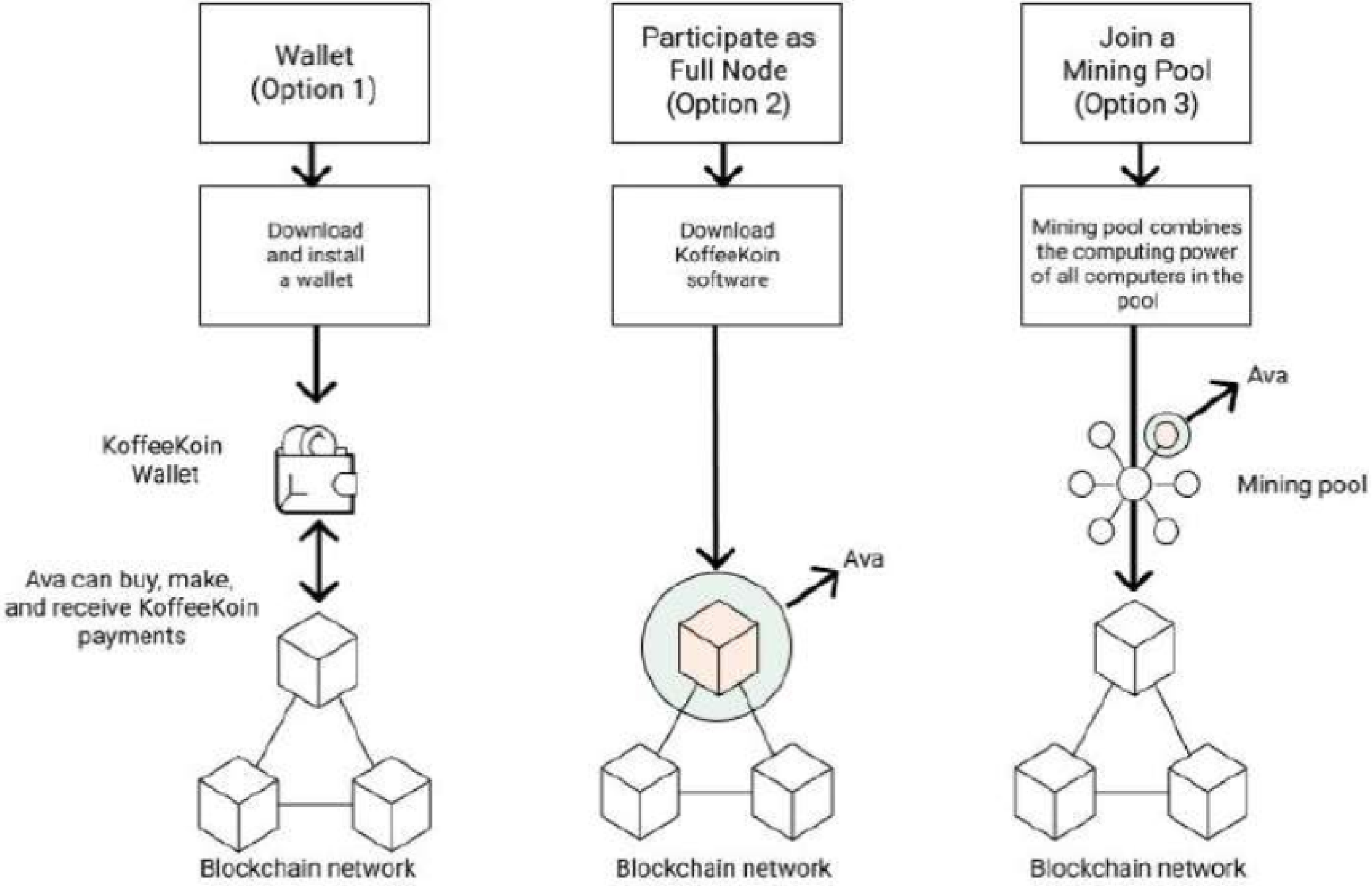
- The middleware layer of a blockchain technology stack is one of the areas where we are starting to see more experimentation because with the growth of middleware for any core infrastructure comes benefits, such as reduced complexity, improved efficiency, and an increase in application development.
- Today’s blockchain networks are just starting to see middleware development
- Various middleware solutions are being built with smart contracts and are monetizable products or services
- **For example:** *the Truffle suite exists for the Ethereum network, making it easier to build decentralized applications on top of Ethereum*

Monetizing the Decentralized Economy

- Enterprises and startups are already developing various Dapps for their specific industry verticals, and some Dapps will function horizontally across many industries
- Consumers can interact with specific Dapps that sit on top of the blockchain stack which take advantage of asset tracking, identity management, and so forth.
- **For instance,** *one Dapp may check a user's identity to make sure she is over the age of twenty-one and combine this certainty of identity with the ability to buy alcohol over the Internet; since it is generally illegal in the United States for people under twenty-one to purchase alcohol.*
- In short, A diverse opportunity for both existing products and entirely new kinds of products enabled by the "Internet of value" functions of this growing decentralized economy.

An Example: KoffeeKoin

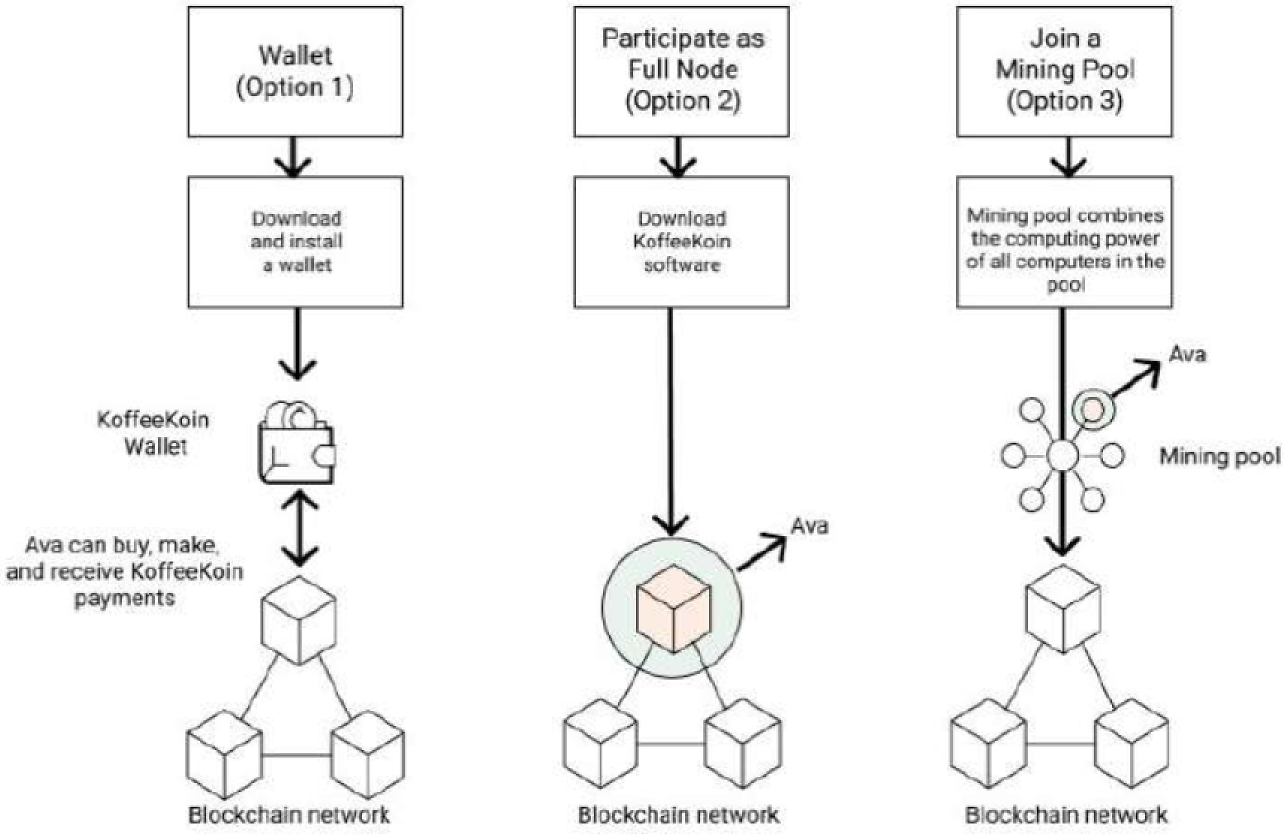
- ○ Barry accepts a new cryptocurrency called "KoffeeKoin" (KFK) in payment
- ○ Eva want to pay KFK, must download KoffeeKoin Dapp (**Wallet**) on smartphone.
- ○ **Wallet (cryptography)???**


Wallet (Option 1)
Download and install a wallet
KoffeeKoin Wallet
Ava can buy, make, and receive KoffeeKoin payments
Blockchain network
Participate as Full Node (Option 2)
Download KoffeeKoin software
Ava
Blockchain network
Join a Mining Pool (Option 3)
Mining pool combines the computing power of all computers in the pool
Ava
Mining pool
Blockchain network

12

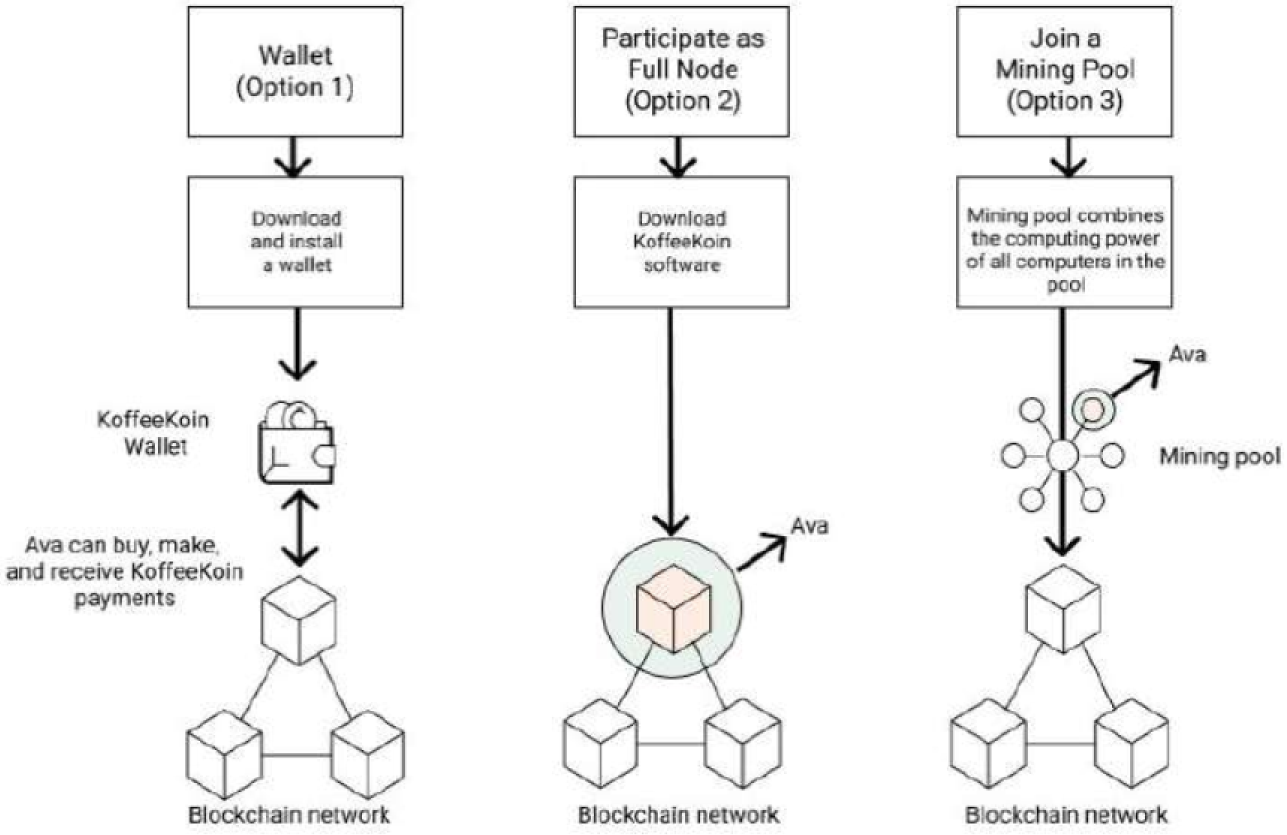
An Example: KoffeeKoin (2)

- If use the Bitcoin network as a reference point, when download the Bitcoin Core software you receive four different components:
  - the wallet,
  - the mining and consensus protocols
  - the full contents of the blockchain,
  - and the peer-to-peer network routing protocols
- Full node: validating transactions and creating new blocks
- KoffeeKoin: Ava would need the full copy of the blockchain and the mining protocols


Wallet (Option 1)
Download and install a wallet
KoffeeKoin Wallet
Ava can buy, make, and receive KoffeeKoin payments
Blockchain network
Participate as Full Node (Option 2)
Download KoffeeKoin software
Ava
Blockchain network
Join a Mining Pool (Option 3)
Mining pool combines the computing power of all computers in the pool
Ava
Mining pool
Blockchain network

An Example: KoffeeKoin (3)

- ○A third option for Ava is to just join a mining pool and let her computer be used on a shared basis among many other members of the pool to mine KoffeeKoin

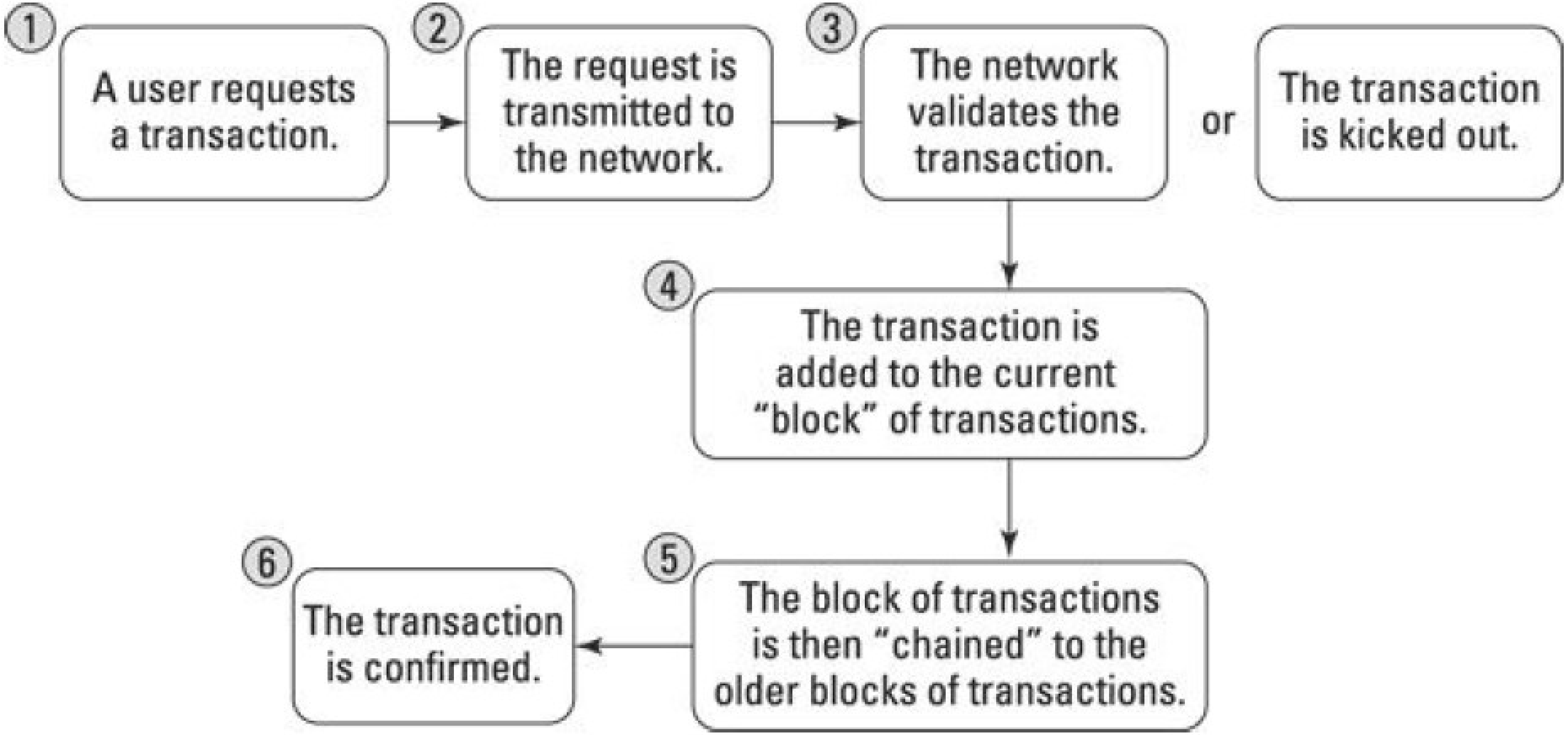

Wallet (Option 1)
Download and install a wallet
KoffeeKoin Wallet
Ava can buy, make, and receive KoffeeKoin payments
Blockchain network
Participate as Full Node (Option 2)
Download KoffeeKoin software
Ava
Blockchain network
Join a Mining Pool (Option 3)
Mining pool combines the computing power of all computers in the pool
Ava
Mining pool
Blockchain network

14

An Example: KoffeeKoin (4)

- Barry made Ava’s order (Mocha, Campuchino,..)
- She uses her installed wallet to send a payment to Barry.
- Her wallet broadcasts to the KoffeeKoin network via the peer-to-peer protocols in the software that she wants to send some KFK to Barry’s wallet
- Barry’s wallet does not know anything about whether Ava is trustworthy or whether she actually has some KFK in her wallet so the community of **KFK verifiers** sets to work to validate the proposed transaction
- The nodes in the KFK network compete against each other to see how fast they can verify her transaction because she is also offering a very small transaction fee as payment for verifying the transaction
- And the way KFK was set up, the first miner to create a whole block of transactions collects all of the transaction fees and also a reward of some extra KoffeeKoin which gets placed in their wallet.

Recall: How Blockchain work



1 A user requests a transaction.

2 The request is transmitted to the network.

3 The network validates the transaction.

or

The transaction is kicked out.

4 The transaction is added to the current "block" of transactions.

5 The block of transactions is then "chained" to the older blocks of transactions.

6 The transaction is confirmed.

An Example: KoffeeKoin (5)

- **Process of verifying Ava’s transaction:** ***a full node on the KoffeeKoin*** *network must* ***examine Ava’s wallet*** *to make sure that it is a* ***legitimate*** ***[hợp pháp]*** *wallet and also that the KoffeeKoin in her wallet is legitimate.*
  - Every time one of the nodes validates that Ava has a legitimate wallet address and that she has enough unspent digital tokens in her wallet, that node broadcasts the verification to the other nodes.
  - When **51% of the nodes** have validated this, the transaction is approved and given a time-stamp and the approved amount of KFK is transferred to Barry’s wallet and the transaction is added to the current table or digital ledger.
  - The way that the transaction is **validated** is **determined** by the **consensus protocol** that is built into the KoffeeKoin blockchain.
  - The nodes that participate in **consensus-building** serve to guarantee that the ledger in its final state is an accurate “system of record.”

What is a Blockchain Wallet?

- **Blockchain wallets** provide individual users the ability to transact on a blockchain network directly. To have a wallet essentially means that you have an account on a particular blockchain network. (Like bank account but …)
- Blockchain wallets are essential to participation in a blockchain network. Each blockchain network has its own version of a wallet, but the "access" that a wallet provides is much broader than just a financial warehouse as with a bank account.
- If you were to use a wallet on the Ethereum blockchain network, you can be an account owner of ether (the crypto-asset), you can work as a **miner** that provides computing power to the underlying network, and you can be a **Dapp participant** (by making transactions using smart contracts)
- **Cold storage** (simplest form : paper wallet ->print out public key and private key or QR Code), -> H**ardware wallets** (no virus and malware) : Trezor is most popular

Sorting Blocks

- When a digital ledger gets to a certain size, a protocol in its blockchain software determines that it is time to create a new block.
- In creating a new block, a node generates a unique identifier or block header for that block which will be used to identify it when it eventually gets chained into the blockchain's history. The block header is a hash of all the transactions in the block.
- The block header is a hash of all the transactions in the block. As a reference point, in the case of Bitcoin, a block header is 80 bytes long.
- In order to ensure that the identifier is unique the nodes participate in a mathematical game that involves using a cryptographic **hash algorithm (SHA-256)** to generate a unique hash for the entire block.
- By design, the size of each block in the Bitcoin network is about 1 MB and it will take roughly ten minutes to create a new block. Different blockchains arrive at consensus in different ways.

Rewarding Miners

- By finding the valid blockhash for the new block, the miner has provided a "proof of work" that means he/she has invested in the electricity and computing resources needed to find the blockhash.
- When a miner has found a winning blockhash, the miner announces this to the entire network and when 51% of the miners validate the blockhash, a reward is deposited in that miner's wallet.
- According to the Bitcoin protocol, **miners** currently receive **12.5 bitcoin** in addition to the total value of the transaction fees for all the transactions contained in that block. Originally, the reward was set at **50 bitcoin**, but it has been cut in half every four years; first to twenty-five and now to 12.5 bitcoin. As the reward keeps decreasing, the miners will have to rely more on higher transaction fees in order to pay for the costs of mining.

Consensus

- When you download blockchain software and become a full node on a network, this means that you can participate in generating a consensus among all of the nodes
- **Bitcoin**: *the consensus rules of the network determine how the participants in the network interact with each other*
  - The conditions under which a transaction (i.e. sending tokens from party A to party B) are valid.
  - The transaction costs related to sending money from party A to party B.
  - The incentive mechanism for validating transactions with a digital token.
  - Rules of how to change current consensus rules.
- The rules of consensus can vary widely between blockchain networks and can also be changed

So, You Want to Be a Miner…

- You may have heard stories about people becoming billionaires by mining bitcoin or other cryptocurrencies with their laptop computer in their garage, dorm room, or basement!
- Now that you know how blockchain works, you might want to start mining cryptocurrencies on your own. But you may wonder if these sorts of gains are still possible today and what you need to get started?
- It is crucial for the success of a permissionless blockchain network to attract miners to participate. This is why there is always a reward system built into blockchain design.
- In the past, many users served as miners just out of their altruistic desire to support the blockchain community. Now, large corporations with vast computing resources have taken over the bitcoin mining world, making it virtually impossible to compete and mine bitcoin on a personal computer.
- In fact, in late 2017, it was estimated that it would take 2.7 million years for a person mining bitcoin on a standard laptop computer to mine a single block.

Questions & Answers

- Next lecture: Essential of BlockChain
- Email: tg_phamthaikytrung@tdtu.edu.vn