Mr Pham Thai Ky Trung

Lecture4 : Bitcoin and Crypto Asset

Learning Objectives

- Gain a deeper understanding of how the Bitcoin network works
- Examine the differences between top crypto-assets
- Examine the top cryptocurrency exchanges
- Look at different cryptocurrency valuation models
- Discuss the concept of digital tokens and value
- Learn how block explorers can be used to gather data

What Are Crypto-assets?

- Bitcoin and the rise of cryptocurrencies
- Become a darling of the fintech industry
- Just 2008 by Satoshi published a proposal for the development of a new digital token “Bitcoin” -> billion of dollars
- Digital coins after the creation of bitcoin were called **“altcoins”** and include popular cryptocurrencies such as ***Ripple, Litecoin, and Ethereum’s “ether.”***

What Are Crypto-assets? (cont1)

- Bitcoin and the rise of cryptocurrencies
- Become a darling of the fintech industry
- Just 2008 by Satoshi published a proposal for the development of a new digital token “Bitcoin” -> billion of dollars
- Digital coins after the creation of bitcoin were called **“altcoins”** and include popular cryptocurrencies such as ***Ripple, Litecoin, and Ethereum’s “ether.”***

What Are Crypto-assets? (cont2)

- **Crypto-assets** are the broadest concept of value on a blockchain. They are **purely digital** and transacted in the form of **coins or tokens**, but can represent anything from a store of value to a means of payment (or medium of exchange), to a physical asset.
- A useful way to think about all **crypto-assets** is across **three broad categories** that have some differences: **cryptocurrencies, crypto commodities, and crypto-tokens**.

Cryptocurrencies

- **A cryptocurrency is defined** as *“any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.”*

Cryptocurrencies (Cont1)

- As a currency it functions as a "**digital asset**" that can be used as a medium of exchange that works on a blockchain or a distributed ledger to provide a record of financial transactions.
- ***These digital assets*** *can also be called* ***"coins" or "currency tokens." (Bitcoin – AltCoin :Bitcoin Alternative)***

Cryptocurrencies (Cont2)

- In addition to **running on its own blockchain,** A digital coin is designed to function like currency in that it represents a store of “value” and can be used as a medium of exchange (e.g. for payments)
- In economics, “value” is commonly defined as a measure of the benefit provided by a good or service to an economic agent.
- In fact, twenty-four of the top twenty-five digital tokens are currency tokens

Crypto-commodities

- Commodities are a class of assets that represent raw materials and different goods or things that bring value.
- Crypto commodities are not that dissimilar [khác biệt] – they are the digital way to represent commodities or physical assets on a blockchain.
- These tokens are also secured with the time, computational power and cost of electricity that cryptocurrencies like bitcoin require

Crypto-commodities (Cont1)

- Governments are looking at regulating tokens like ether – used to perform transactions on the **Ethereum network** – under the lens of **commodities**, in part because the tokens are being used as a way to run smart contracts rather than just store value or make payments.
- Right or wrong : ***Categorizing certain tokens as commodities is just a way to get around industry regulations ?***

Crypto-commodities (Cont2)

- A subset of **crypto-commodities** includes **“asset-backed tokens**,” which are designed to be digital representations of **tangible assets (***stones or real estate*) or ***intangible assets (*** *intellectual property*)
- Everledger is a company that tokenizes diamonds, linking the physical asset with a digital twin
- Representing and tracking assets that are unique (non-fungible) has been a challenge for many businesses dealing with existing assets (*think land titles, diamonds, or art*)

Other Crypto-tokens

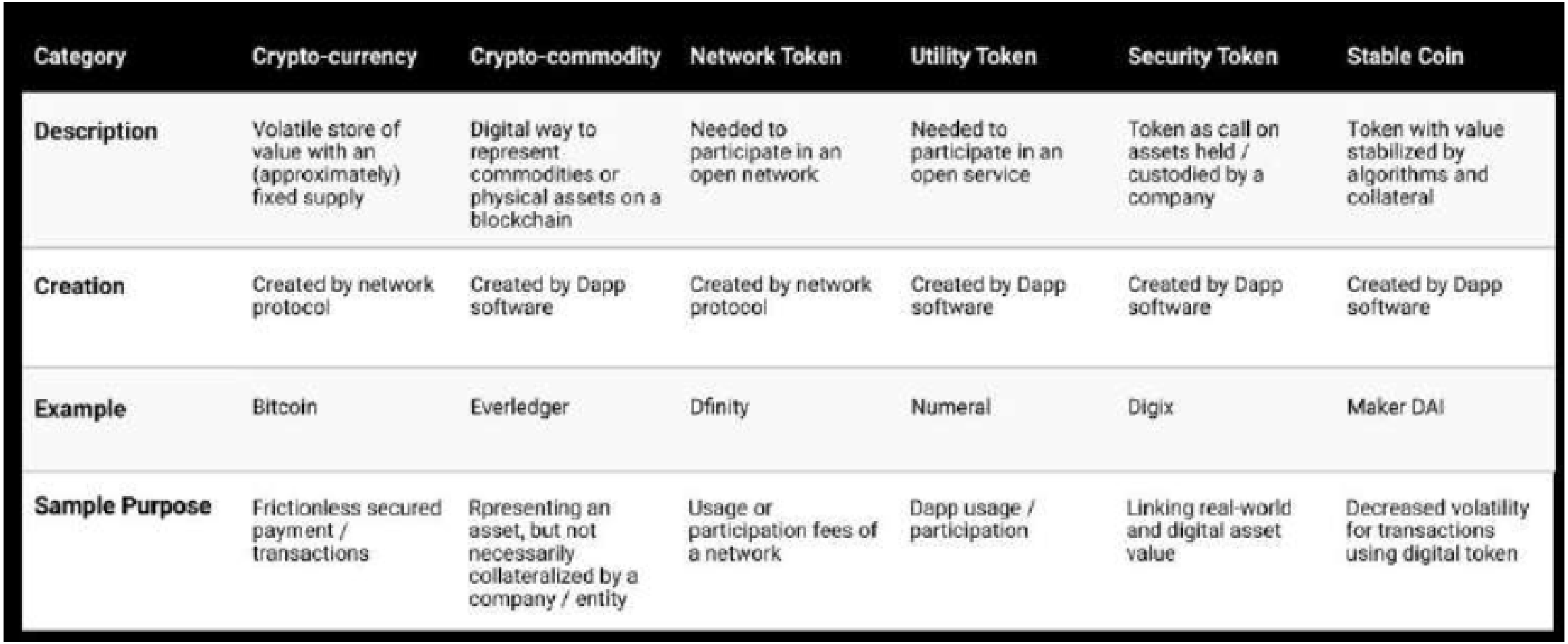
- **Crypto-tokens** represent a smattering of other tokenized assets or purposes in a blockchain environment that **fall** outside the categories of cryptocurrency and commodity.
- Traditional world of finance (Cash, commodities, fixed income, and stocks)
- Stocks offer rights such as governance and ownership, as well as dividends -> similar functionalities in the **blockchain space.**
  - **The ability to use tokens to confer voting and governance rights in a network is an important element of using a blockchain.**
  - **Conferring dividends and interest is also possible, depending on how a blockchain or token is implemented**

Other Crypto-tokens (Cont1)

- Besides cryptocurrencies, today we have terms like
  - network tokens,
  - security tokens,
  - utility tokens,
  - stable coins/tokens,
  - and reputation/reward tokens.

Other Crypto-tokens (Cont2)

- Broader crypto-tokens (or assets)



Category	Crypto-currency	Crypto-commodity	Network Token	Utility Token	Security Token	Stable Coin
Description	Volatile store of value with an (approximately) fixed supply	Digital way to represent commodities or physical assets on a blockchain	Needed to participate in an open network	Needed to participate in an open service	Token as call on assets held / custodied by a company	Token with value stabilized by algorithms and collateral
Creation	Created by network protocol	Created by Dapp software	Created by network protocol	Created by Dapp software	Created by Dapp software	Created by Dapp software
Example	Bitcoin	Everledger	Dfinity	Numeral	Digix	Maker DAI
Sample Purpose	Frictionless secured payment / transactions	Rpresenting an asset, but not necessarily collateralized by a company / entity	Usage or participation fees of a network	Dapp usage / participation	Linking real-world and digital asset value	Decreased volatility for transactions using digital token

Network Tokens

- **Network tokens (similar to utility tokens)** are a broad category that encapsulates tokens created by their network (not by Dapp)
- these tokens to install software, run software, store data, pay for computation, or participate in governance on a given blockchain network.
- **Example: Dfinity** network, where you would need to buy or possess Dfinity tokens (DFN) in order to perform these functions
- **Ether :** can be classified as both as crypto currency token and a network token (on Ethereum platform itself)

Utility Tokens

- Utility tokens are sometimes called “app coins” because they are usually linked to a specific company or project’s blockchain application.
- Many tokens that are built on top of existing blockchain platforms like Ethereum
- **Numerai**, which is an application built on the Ethereum network that aims to crowdsource trading algorithms for hedgefunds, and requires Nuermaire (NMR) tokens to participate.
- **Utility tokens** are growing in popularity

Security Tokens

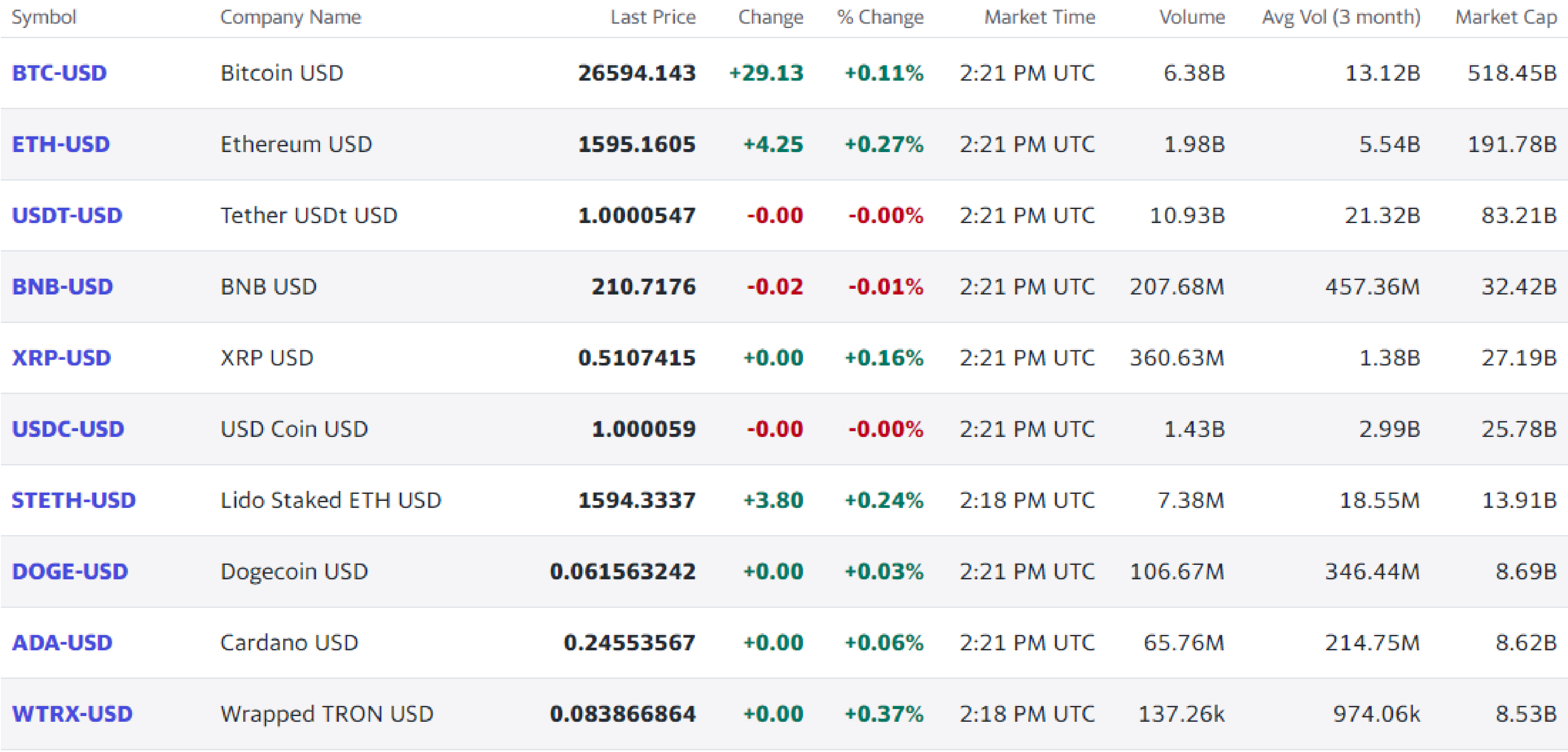
- **Security tokens** represent an investment inan asset. *Like a security, they are backed by the tradable resources of the issuing entity.*
- ***For example**, Digix and Goldmint are asset-backed tokens that make it easier to own gold assets*
- The Security and Exchange Commission (SEC) in the U.S. has taken note, moving to regulate these tokens just as they would securities

What are ICOs

- In the rush to get into cryptocurrencies many Initial Coin Offerings (ICOs) have been created.
- Similar to an Initial Public Offering (IPO), this is when a project opens up for investment by individuals and institutions.
- In return for sending cryptocurrencies like bitcoin or ether to a project, investors receive some amount of tokens related to the project.

Top Ten Cryptocurrencies by Market Capitalization

○ sasa



Symbol	Company Name	Last Price	Change	% Change	Market Time	Volume	Avg Vol (3 month)	Market Cap
BTC-USD	Bitcoin USD	26594.143	+29.13	+0.11%	2:21 PM UTC	6.38B	13.12B	518.45B
ETH-USD	Ethereum USD	1595.1605	+4.25	+0.27%	2:21 PM UTC	1.98B	5.54B	191.78B
USDT-USD	Tether USDt USD	1.0000547	-0.00	-0.00%	2:21 PM UTC	10.93B	21.32B	83.21B
BNB-USD	BNB USD	210.7176	-0.02	-0.01%	2:21 PM UTC	207.68M	457.36M	32.42B
XRP-USD	XRP USD	0.5107415	+0.00	+0.16%	2:21 PM UTC	360.63M	1.38B	27.19B
USDC-USD	USD Coin USD	1.000059	-0.00	-0.00%	2:21 PM UTC	1.43B	2.99B	25.78B
STETH-USD	Lido Staked ETH USD	1594.3337	+3.80	+0.24%	2:18 PM UTC	7.38M	18.55M	13.91B
DOGE-USD	Dogecoin USD	0.061563242	+0.00	+0.03%	2:21 PM UTC	106.67M	346.44M	8.69B
ADA-USD	Cardano USD	0.24553567	+0.00	+0.06%	2:21 PM UTC	65.76M	214.75M	8.62B
WTRX-USD	Wrapped TRON USD	0.083866864	+0.00	+0.37%	2:18 PM UTC	137.26k	974.06k	8.53B

Bitcoin

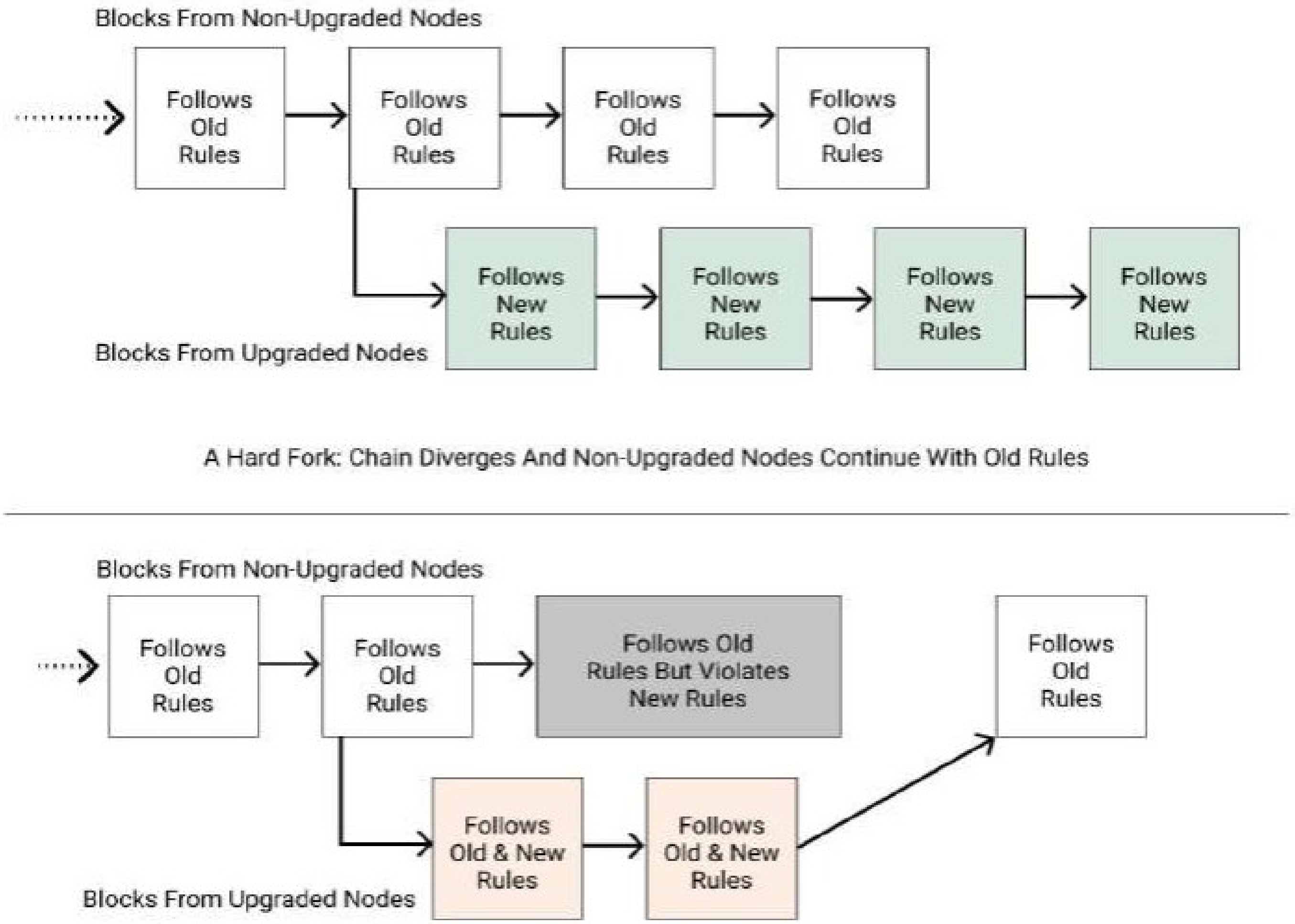
- Bitcoin is important because it has proven that a digital asset running on a decentralized network was feasible.
- Bitcoin network is the fact that it is not controlled by any government or banking institution
- Millions of dollars-worth of tokens can move freely between digital wallets

Bitcoin

- potential benefits of the Bitcoin network
  - Maintaining a permanent and transparent record of transactions on the blockchain
  - Faster payment processing
  - Cutting down on transaction fees from third parties
  - Supporting international payment processing
  - Simplifying processing of high-value payments
  - Reducing the paperwork associated with banking accounts by using wallets
  - Domestic and international transactions confirmed within an hour regardless of size
  - First truly global (and non-national) currency

Bitcoin

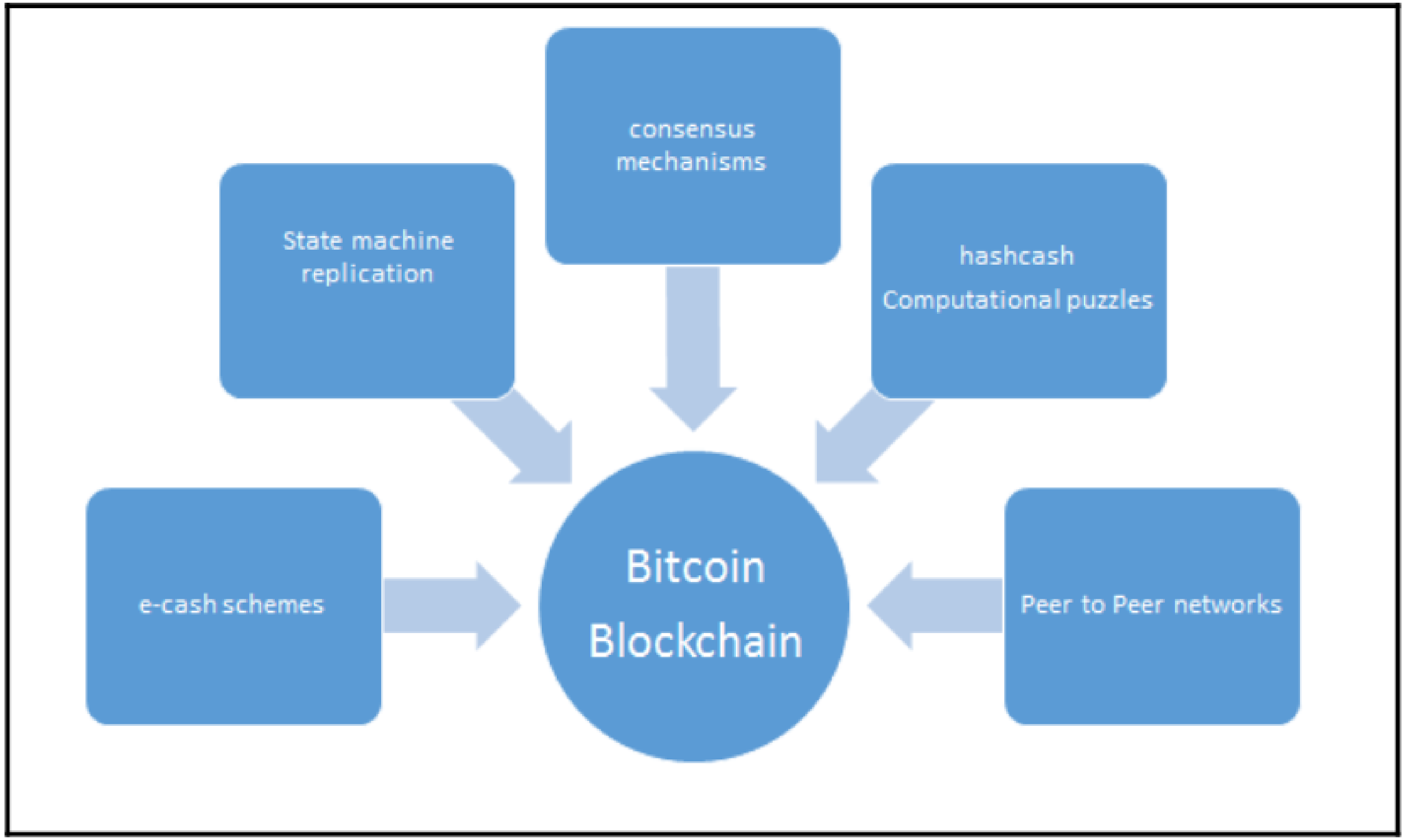
- Bitcoin continues to evolve and change

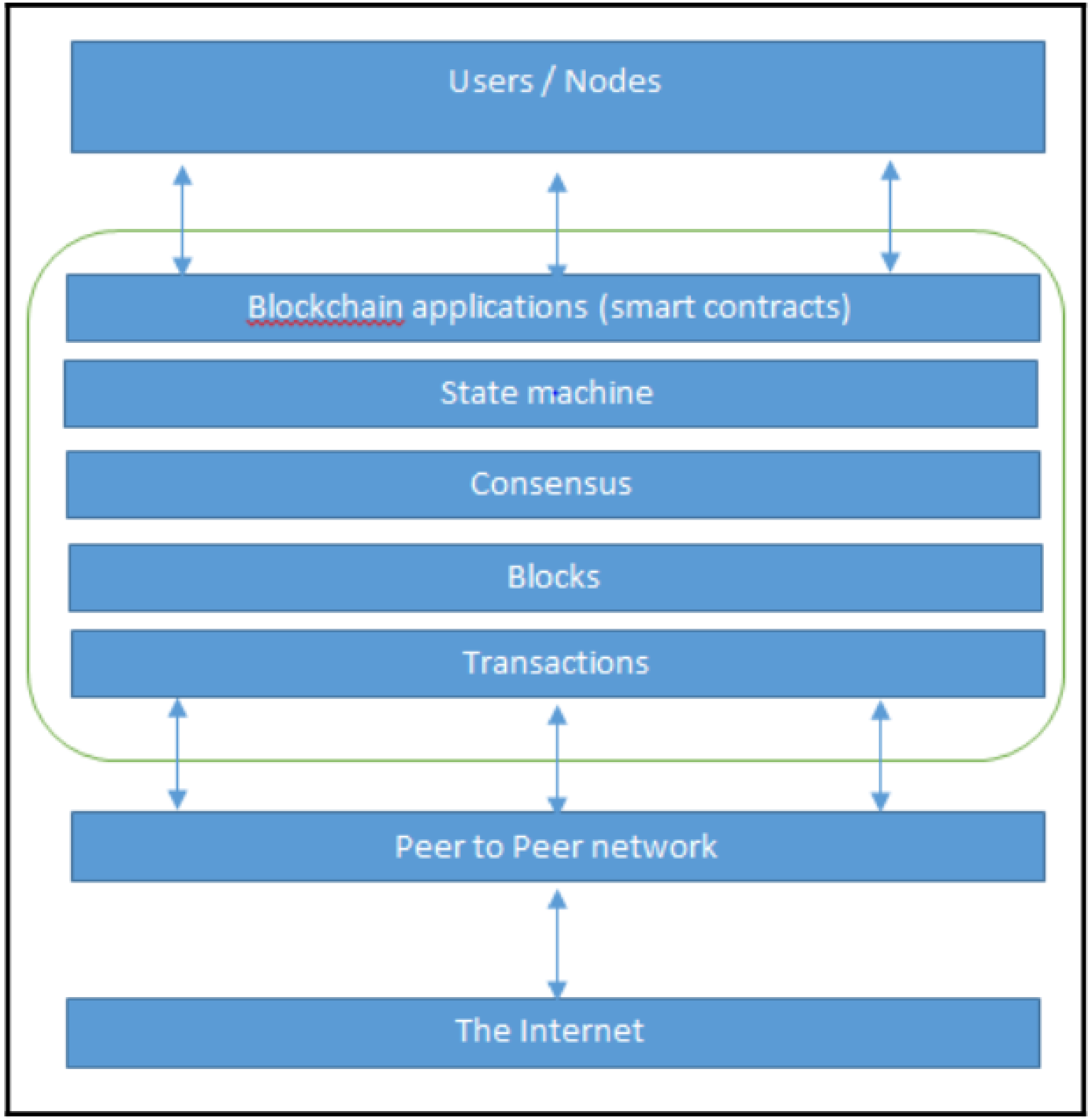


22

The various ideas that helped with the invention of bitcoin and blockchain

- how ideas and concepts from electronic cash schemes and distributed systems were combined together to invent bitcoin and what now is known as blockchain



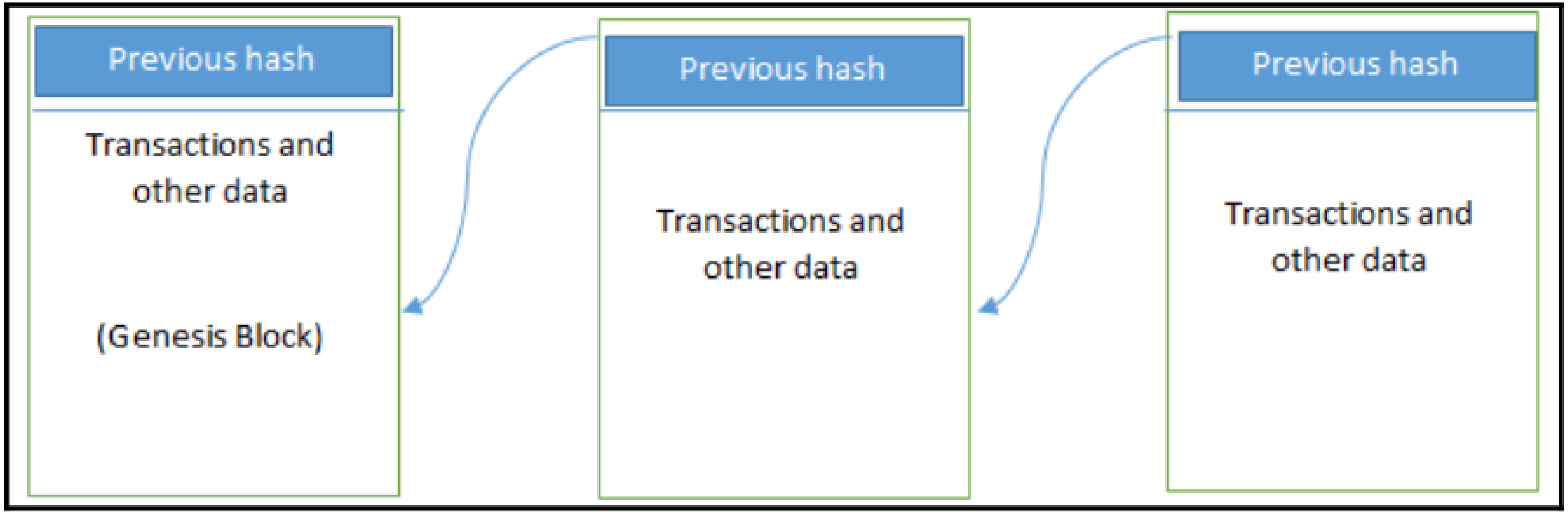


Network view of blockchain

- Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the Internet, as can be seen below in the diagram. It is analogous to SMTP, HTTP, or FTP running on top of TCP/IP

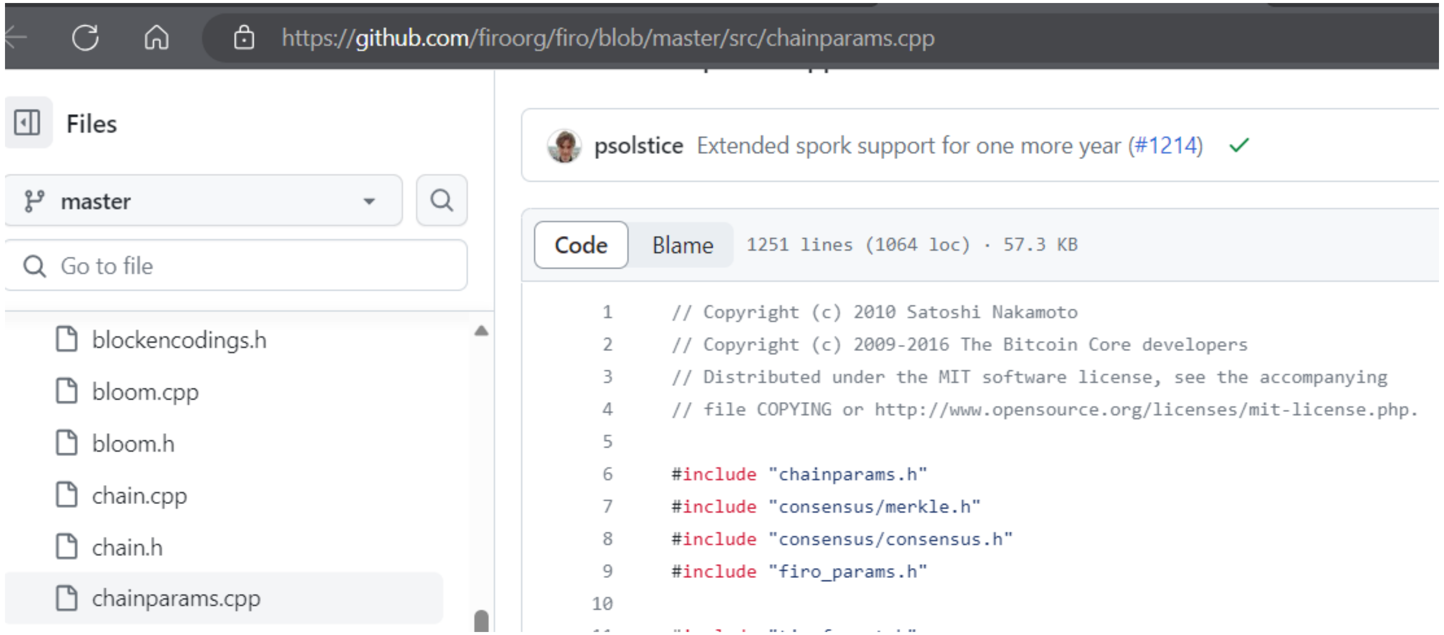
Generic block chain

- A genesis block is the first block in the blockchain that was hardcoded at the time the blockchain was started

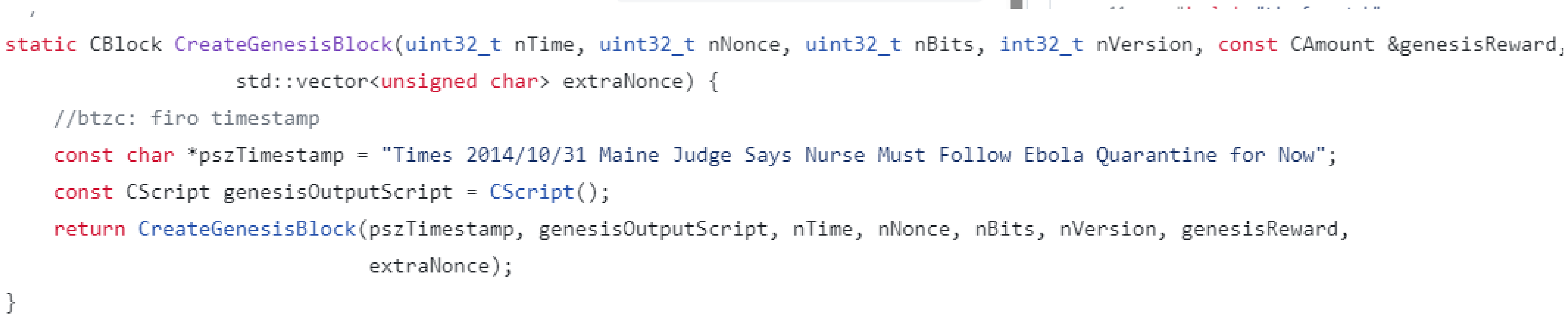

Previous hash
Transactions and other data
(Genesis Block)
Previous hash
Transactions and other data
Previous hash
Transactions and other data

Generic block chain

- https://github.com/firoorg/firo/blob/master/src/chainparams.cpp
- This is the first block in the bitcoin blockchain. The genesis block was hardcoded in the bitcoin core software. It is in the chainparams.cpp file.

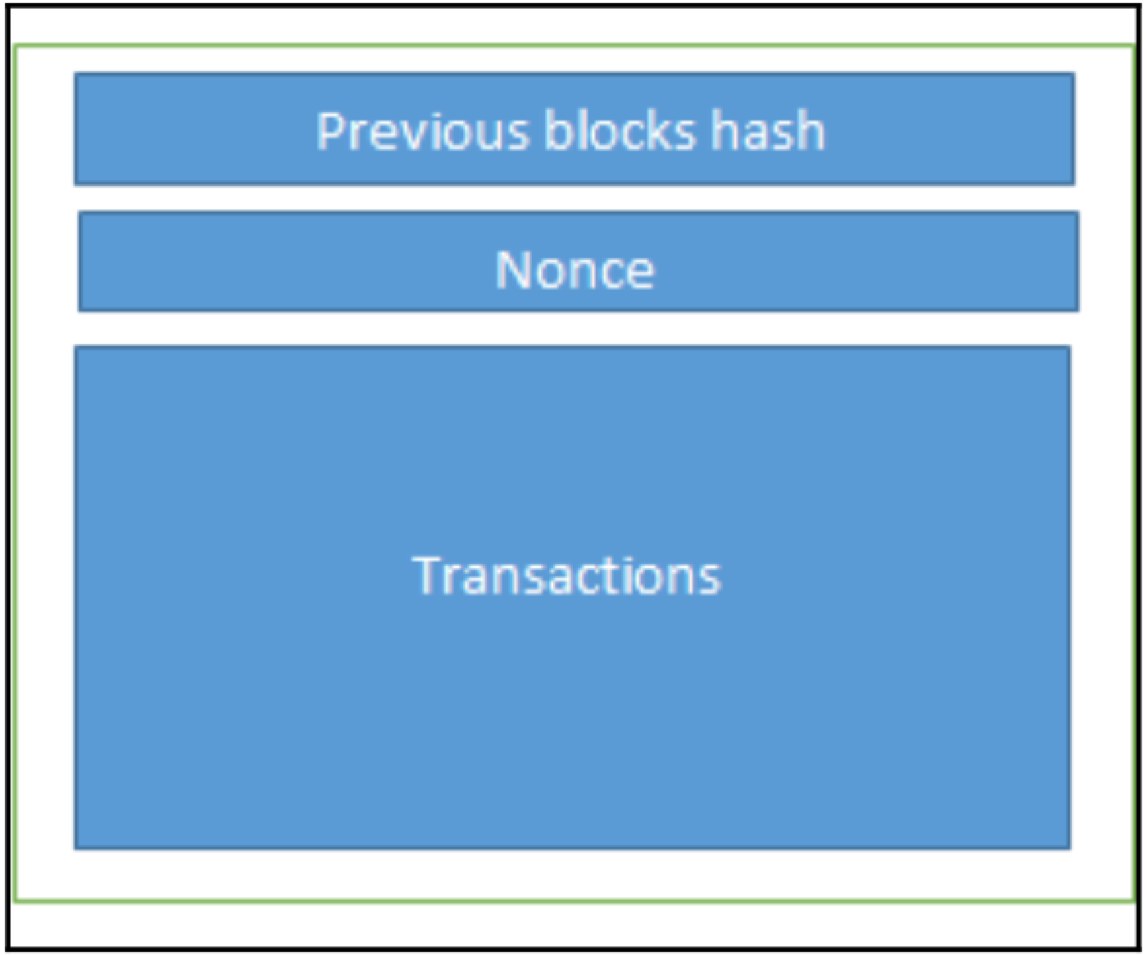

https://github.com/firoorg/firo/blob/master/src/chainparams.cpp
Files
master
Go to file
blockencodings.h
bloom.cpp
bloom.h
chain.cpp
chain.h
chainparams.cpp
psolstice Extended spork support for one more year (#1214) ✓
Code
Blame
1251 lines (1064 loc) · 57.3 KB

```
// Copyright (c) 2010 Satoshi Nakamoto
// Copyright (c) 2009-2016 The Bitcoin Core developers
// Distributed under the MIT software license, see the accompanying
// file COPYING or http://www.opensource.org/licenses/mit-license.php.

#include "chainparams.h"
#include "consensus/merkle.h"
#include "consensus/consensus.h"
#include "firo_params.h"

```



```
static CBlock CreateGenesisBlock(uint32_t nTime, uint32_t nNonce, uint32_t nBits, int32_t nVersion, const CAmount &genesisReward,
                   std::vector<unsigned char> extraNonce) {
    //btzc: firo timestamp
    const char *pszTimestamp = "Times 2014/10/31 Maine Judge Says Nurse Must Follow Ebola Quarantine for Now";
    const CScript genesisOutputScript = CScript();
    return CreateGenesisBlock(pszTimestamp, genesisOutputScript, nTime, nNonce, nBits, nVersion, genesisReward,
                              extraNonce);
}
```

The structure of a block



- **A block** is composed of multiple transactions and some other elements such as the previous block hash (hash pointer), timestamp, and nonce.
- **A transaction:**
  - is the fundamental unit of a blockchain.
  - represents a transfer of value from one **address** to another.

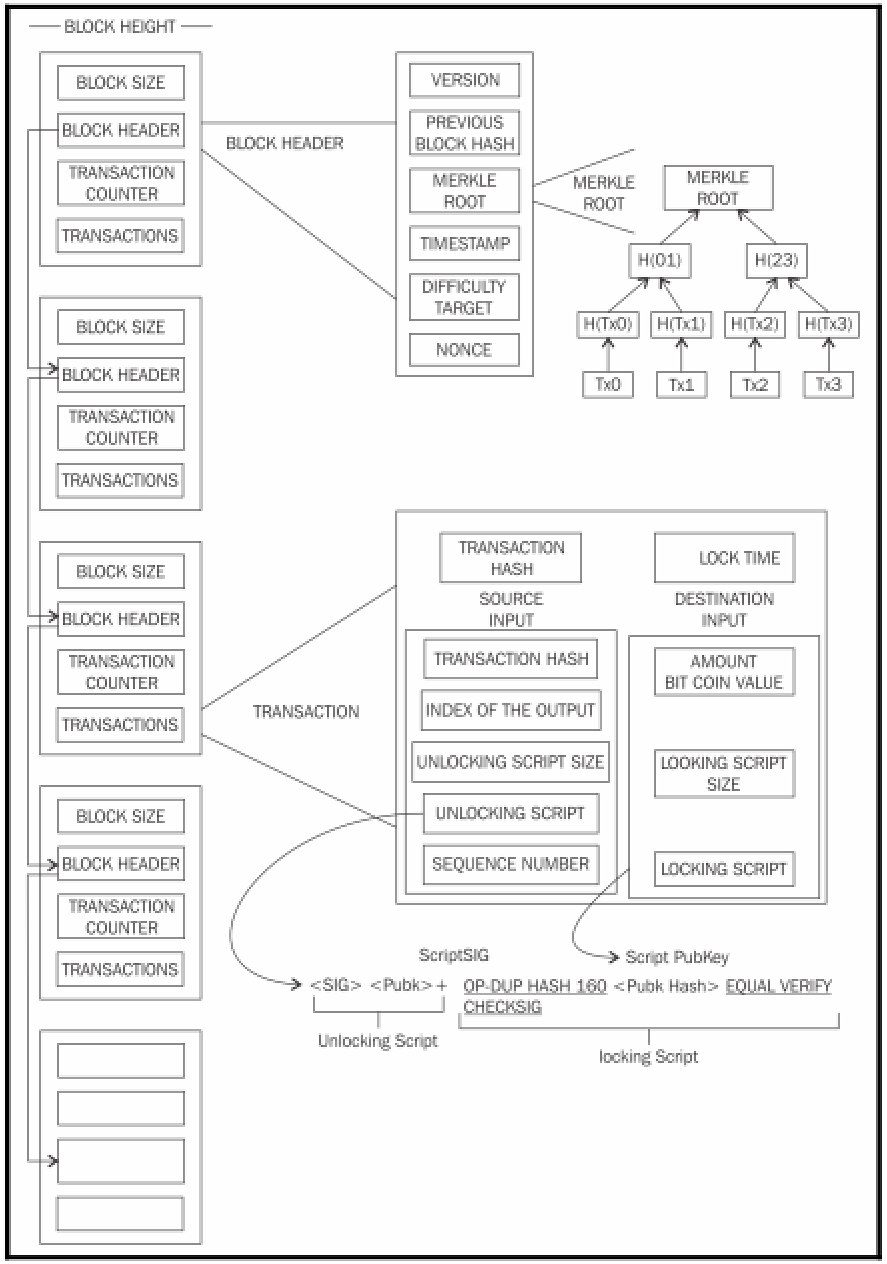
Addresses

- Addresses are unique identifiers that are used in a transaction on the blockchain to denote senders and recipients.
- An address is usually a public key or derived from a public key.
- Users generate a new address for each transaction in order to avoid linking transactions to the common owner, thus avoiding identification

How blockchains accumulate blocks

- 1. A node starts a transaction by signing it with its private key.
- 2. The transaction is propagated (flooded) by using much desirable Gossip protocol to peers, which validates the transaction based on pre-set criteria. Usually, more than one node is required to validate the transactions.
- 3. Once the transaction is validated, it is included in a block, which is then propagated on to the network. At this point, the transaction is considered confirmed.
- 4. The newly created block now becomes part of the ledger and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first.
- 5. Transactions are then reconfirmed every time a new block is created. Usually, six confirmations in the bitcoin network are required to consider the transaction final

Consensus in blockchain



The structure of a block

Bytes	Name	Description
80	Block header	This includes fields from the block header described in the next section.
variable	Transaction counter	The field contains the total number of transactions in the block, including the coinbase transaction.
variable	Transactions	All transactions in the block.

The structure of a block header

Bytes	Name	Description
4	Version	The block version number that dictates the block validation rules to follow.
32	previous block header hash	This is a double SHA256 hash of the previous block's header.
32	merkle root hash	This is a double SHA256 hash of the merkle tree of all transactions included in the block.
4	Timestamp	This field contains the approximate creation time of the block in the Unix epoch time format. More precisely, this is the time when the miner has started hashing the header (the time from the miner's point of view).
4	Difficulty target	This is the difficulty target of the block.
4	Nonce	This is an arbitrary number that miners change repeatedly in order to produce a hash that fulfills the difficulty target threshold.

Mining

Task of Miner

- Once a node connects with the bitcoin network, there are several tasks that a bitcoin miner performs:
  - Synching up with the network
  - Proof of Work
  - The mining algorithm

Synching up with the network

- A new node joins the bitcoin network:
  - Transaction validation: *validated by full node*
  - Block validation: *The verification of each transaction in the block along with verification of the nonce value*
  - Create a new block : *propose a new block by combining transactions broadcasted on the network after validating*
  - Perform Proof of Work : *the core of the mining process*
  - Fetch reward: *once accepted, the miner is rewarded*

Proof of Work

- This is a proof that enough computational resources have been spent in order to build a valid block. Proof of Work (PoW) is based on the idea that a random node is selected every time to create a new block

$$H\,(\,N \,||\, P\_hash \,||\, Tx \,||\, Tx \,||\, .\,.\,.\; Tx) < Target$$

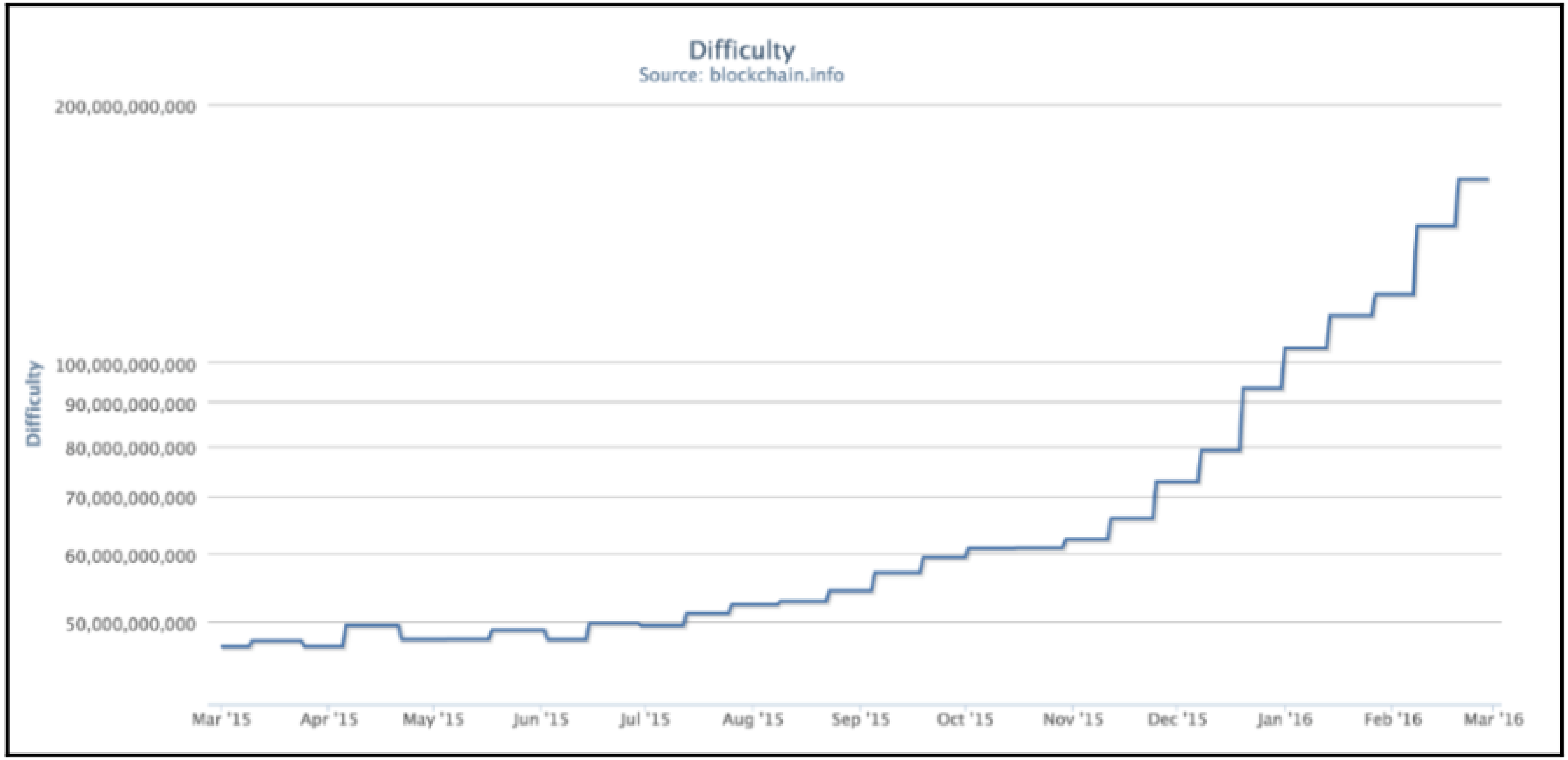
- N is a nonce, P_hash is a hash of the previous block, Tx represents transactions in the block, and Target is the target network difficulty value

The Mining Algorithm

- Consist of steps:
  - The previous hash block is retrieved from the bitcoin network.
  - Assemble a set of potential transactions broadcasted on the network into a block.
  - Compute the double hash of the block header with a nonce and the previous hash using the SHA256 algorithm.
  - If the resultant hash is lower than the current difficulty level (target), then stop the process.
  - If the resultant hash is greater than the current difficulty level (target), then repeat the process by incrementing the nonce

Mining difficulty increased

- $bitcoin-cli getdifficulty



Mining Systems

- **CPU** : *first type of mining but no longer profitable*
- **GPU**: *faster and parallelized calculations but overheating, specialized motherboards to have multiple graphics cards*
- **FPGGA :** Field Programmable Gate Array
- **ASICs**: Application Specific Integrated Circuit : perform SHA-256 operation

Questions & Answers

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