NUCHAIN: WEB 3.0 PLATFORM FOR DECENTRALIZED TECHNOLOGY ECOSYSTEMS IN INDONESIA

Abstract. Web has been evolving from web 1.0 to the era of web 3.0. The idea of Web 3.0 is building a decentralized system that becomes a solution for problems that arise in a centralized web 2.0. Nuchain has been developed by utilizing the blockchain network used as a web 3.0 platform. Nuchain utilizes Substrate as a blockchain builder framework as the basis for developing web 3.0 ecosystem. Nuchain's features can be used for building smart contract, digital certificate, on-chain organization, and digital assets. Users can control their personal data without involving third parties, ensuring data availability and user data security.

I. Introduction

Web 1.0, a simple-static web display, was firstly invented by Berners-Lee in 1990. The technology used in Website 1.0 is read-only, which means that the reader has no opportunity to share information and gives any contribution. The technology evolved into web 2.0, which allowed users of the web to interact with the application. Web 2.0 enables users to download and exchange information and eventually become the basis for the emergence of social media, social web, and blogging [1]. Web 2.0 still has some fundamental weaknesses, one of which is the vulnerability to Single Point of Failure (SPOF) due to its centralized system [2].

A. Centralized System

The internet eases our work and communication in everyday life. Applications we run so far are client-server, which means that they are on the development's server. For example, when using a banking application, we have to visit the bank's server. In this centralized system, failures will appears if the company's server gets problems.

B. Data Control

In the centralized system, data are controlled at the application layer, resulting in users being forced to follow the rules made by the application. Users cannot control their personal data, and they do not know for what purpose the stored data in the application are used.

C. Security

Currently, data on the web is almost stored on centralized servers and data centres. Centralizing data storage at a single server increases the risk of massive data loss and breaches from a security point of view. A failure in a single point makes all the services that depend on that point will fail simultaneously.

II. WEB 3.0 (Decentralized Web)

The presence of blockchain allows various innovations. One of the pioneers is Bitcoin, a well-known blockchain used for payment and Ethereum, used as a platform to build applications on the blockchain network [1]. The previously centralized web 2.0 now shifting and becoming more decentralized by utilizing the blockchain network as the platform [3].

A. Layers on Web 3.0 Technology

Nuchain is based on technology developed by the Web3 Foundation that holds a vision of allowing users to control their data, identity and purpose, leads the internet to become more decentralized. [4]. The web3 foundation's mission is to maintain and manage technologies and applications in decentralized web software protocols.

B. DApps (Decentralized Apps)

Blockchain uses a peer-to-peer connection. Each connected node stores data separately between nodes [1]. A distributed system can be implemented to realize web 3.0 by using blockchain technology. DApps are known as distributed applications that run on a blockchain network. DApps are at layer 3 of the web3 technology layer, and their appearance is similar to today's web. While web 2.0 consists of a front-end and a back-end, DApps also have a front-end and a back-end. The difference between web 2.0 and Web 3.0 lies in the back-end [6]. Web 2.0 storage is located on a centralized server, and then the client accesses it using the HTTP protocol. In web 3.0, the applications are not connected to a central point; instead, they are connected to a blockchain network. Data in web 3.0 will be shared among nodes, which guarantees that data in web 3.0 will always be available even if a single point of failure happens.

C. Advantages of Web 3.0

The background of web 3.0 development is the drawbacks of the current web 2.0 [7]. The centralized nature of data management in Web 2.0 poses a high risk of data failure. With the existence of a distributed web that uses blockchain to build web 3.0, data management systems for the web can be distributed to nodes on the blockchain network. A failure at one node does not trigger the failure of all data. Data control does not go through third parties or application providers in distributed networks because personal identity is required when entering the blockchain network, not when entering the application. The users' personal data are safe. Users can communicate with each other without knowing the faces of other users since we have been convinced to use zero-knowledge proof [8]. Web 3.0 security is guaranteed by distributed nodes and uses consensus to perform block generation. An attacker can not execute an attack on the system at one point only [9].

III. NUCHAIN

Nuchain is a 3rd generation web platform that allow users to control data and access services independently. This feature is a solution to a problem that arises in today's web technologies. Nuchain is built on a decentralized system so that the Nuchain's availability is more guaranteed, and it is safer from SPOF (Single point of failure). Nuchain is built using blockchain technology. Blockchain technology is supported by a consensus mechanism, using distributed machines that are interconnected and agree on every valid operation / computation / transaction in changing state, and executing every business function required.

Nuchain is developed using a Substrate framework. Substrate is the the most advanced 3rd generation blockchain framework with many advantages over previous technology [1]. Nuchain is designed as a dynamic platform and developed to meet the wider community's needs, especially in Indonesia. It is not limited to one function (e.g., for a digital value store) but also bridges the community to utilize decentralized technology; small and medium business units (Indonesian: usaha kecil dan menengah / UMKM), serverless app development, digital certificate, digital assets, and smart contract are several examples of potential uses of Nuchain.

Nuchain is a web 3.0 platform that utilizes the development of blockchain technology. The peer-to-peer technology on the blockchain allows Nuchain to use libp2p technology to communicate between nodes on the blockchain network. The interconnected nodes will be the resources to run web 3.0. Building a blockchain requires a framework that is used as the foundation for developing nuchain. Several frameworks can be used as a blockchain foundation. Substrate is an open-source framework for building blockchains that

can be modified as needed. Nuchain chose Substrate as a framework because it fits the requirements for developing a digital ecosystem in Indonesia. Following are the advantages of the framework [10].

1) Supports various types of consensus algorithms such as PoW, PoA, and PoS.
2) Flexibility. The Substrate is a very flexible blockchain framework; it allows nuchain to expand without the need for hard forks that's common on previous generation of blockchains.
3) On-chain Governance. The Substrate supports on-chain governance, allowing nuchain to execute strategic decisions via the blockchain network. The decisions are taken democratically and directly.
4) WASM. The Substrate supports Web Assembly by using it as a runtime and smart contract. The feature allows smart contracts to be created in particular programming languages and, in the future, can also be written in various programming languages that support Web Assembly.
5) Extensible, The Substrate allow developer to add module called pallet to enrich the system as needed.

B. System Design

This section describes how Nuchain is built. As Nuchain is built using the Substrate framework, the technical specifications are derived from the Substrate. The detail is not explained in this text because the Substrate documentation has described the technical specifications clearly. This document will only explain what functions are used in its composition.

1) Consensus

In consensus, Nuchain will fully use NPoS (Nominated Proof of Stake), BABE and GRANDPA algorithms to produce blocks [11].

BABE (Blind Assignment for Blockchain Extension) is an algorithm for creating slot-based blocks. The mechanism that BABE uses to create blocks uses VRF (Verifiable Random Function). Each validator is assigned a weight for an epoch. This epoch is split into slots, and the validator evaluates its VRF in each slot. On each slot, all validators generate a new random number with the VRF function, and if it is lower than the given threshold (which is proportional to the weight), they have the right to generate a block. Other partners will use proof of execution of the VRF function to validate the validity of the slot claim [12].

GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) is used for block finalization. Finalization is done to select the blocks that the validators have made. The validators decide which block is the best, and validator's voices are applied transitively for all previous blocks. After more than 2/3 of the GRANDPA authorities select the block, the block is considered final [13].

2) Validator and Nominator

Validators were selected using the NPoS (Nominated Proof-of-Stake) consensus. The sequential Phragmen method is used in the Nominated Proof-of-Stake scheme to select validators based on their self-stake and stakes chosen from the nominator [14]. When the validator slot is still empty, anyone can become a validator without a minimum stake. But when the validator slot is filled, the minimum number of stakes will be taken from the smallest stake of the active validator in the slot. In this NPoS method, the reward value received by validators is the same even though the stakes given are different.

Nominators are individuals who support validators so that the algorithm can select validators to enter the validator slot. In contrast to validators, nominator do not need machines to validate/produce blocks but only need stakes for the validators so that validators have more accumulated total stakes to compete with other validators. The nominator is only functionally effective when the validator slot quota has been

fulfilled, and many other validator candidates are queuing up to enter the validator slot. With a stake to the validator, the validator will have a higher stake value and have a high probability of being selected by the algorithm to enter the active validator slot.

C. Economic Model

Nuchain ecosystem uses the token economy concept with ARA as the native token. ARA's function is for:

1. Network financing such as paying for computational load, bandwidth usage, and data storage.
2. As a service fee (gas fee).
3. Paying validators as an incentive for contributing to the life and security of the network.
4. Governance needs such as voting in determining development policies and decisions.

At the initial initiation, nuchain issued 17,000,000 ARA pre-mined tokens, and these tokens have been allocated with the following distribution (Table 1).

Table 1. Token Sharing Allocation

Token Allocation	Allocation (%)	Total
Team	26%	4500000
Advisors	9%	1500000
Strategic	9%	1500000
Ecosystem Growth	15%	2500000
Liquidity Incentives	12%	2000000
Community Development	18%	3000000
Foundation Reserves	12%	2000000

D. Roadmap

Nuchain has the following development roadmap (Figure 2).
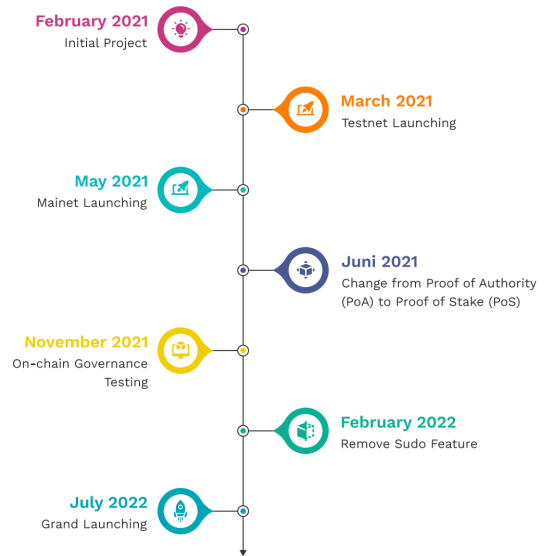
Figure 2. Nuchain Development Roadmap

E. Features

Nuchain currently has several features built-in (natively) developed in the form of a pallet. The following features are available.

1. Decentralized Organization

A decentralized organization is a foundation for managing resources related to organizational needs in a decentralized world. An example is the implementation of DAO (Decentralized Autonomous Organization), a form of organization in a decentralized world where the statutes and bylaws are written in computer code and executed automatically according to mutual agreement. Examples of DAO implementation are joint fund management, crowdfunding, asset management, and other functions requiring mutual trust. Organizations in Nuchain are similar to accounts, having the same addresses as regular user accounts, but their operations are not independent; they need administrators (admins) to carry out their operations. In addition, organizations also have basic information natively on-chain such as organization name and description. Other information is website and email, but other custom information and properties can be added if needed using additional field.

2) Digital Certificate

Nuchain supports digital certificate creation, where certificate data created on Nuchain is immutable and can be verified globally [16]. Certificates can only be created and issued by on-chain organizations.

3) Supply Chain

Nuchain supports supply chain system functions. This function allows an entity in an on-chain organization to register products, create tracking data and provide access to other stakeholders to update tracking data.

4) Digital Assets

Nuchain supports creating digital assets, layer 2 tokens like ERC20 standard, and unique tokens like ERC721 (NFT) standard.

5) *Smart Contracts*

Nuchain supports smart contract written in Rust with Parity's ink eDSL.

F. Role

Nuchain was created for a distributed system so that in Nuchain, a regulation was made to uphold democratic values. To realize the democratic values in Nuchain, some roles that contribute to implementing the system are needed.

1) Validators

Validators in the Nuchain network are computers connected in a distributed and publicly owned manner to power and secure the Nuchain network. Anyone can contribute to securing the Nuchain network by becoming a validator by providing computers to create or validate blocks, and in return, validators will receive ARA tokens.

2) Nominator

Nominator are individuals who wish to participate in securing the network without being a validator. Unlike the validator, the nominator does not require a machine to perform block validation. Nominator use the tokens to help strengthen validators so that they are strong enough to be elected and easily enter the ranks of validators. In return, the nominee will receive ARA tokens according to the profit-sharing percentage set by the validator.

3) Organization

The basic representation of on-chain organization. The function of the organization is to act not as person but as entity, this type of on-chain entity is fundamental for DAO, and needed to do operation like give legitimacy to digital certificates and supply chains.

4) Governance

Nuchain supports on-chain governance, a strategic decision making conducted by voting by Nuchain users directly on the network. Directly on the network means that all processes are running and recorded on the blockchain to ascertain their legitimacy. This feature facilitates the governance process in the system so that the process is easy, safe, fair and accountable. Within governance, two important roles influence decisions on the Nuchain system: the council and the technical committee. The council is made up of several representatives who are elected by the community using ARA tokens. The function of the council is to submit proposals and conduct a referendum on incoming proposals. The technical committee is the chosen team and has expertise in system development. In the governance system, technical committee members will be added or reduced based on the majority vote of the board. Technical committees make proposals either in an emergency (such as a bug that threatens the system's sustainability) or for system development.

G. Usage

As a decentralized platform (platform), nuchain can be used for various

functions. Several agencies and academics have used Nuchain for publishing digital certificates. Nuchain is also used by small and medium business units and multinational corporations for various needs, from loyalty programs to the Internet of Things development. As nuchain enters phase 5 of the roadmap, nuchain will improve services by opening smart contracts to develop DApps as distributed applications on top of the nuchain network.

IV. CONCLUSION

Nuchain is built to create a distributed system on top of a blockchain network by utilizing peer-to-peer technology. The development of this distributed system aims to welcome web 3.0 technology in Indonesia by adjusting existing regulations so that web 3.0 technology can run following democratic values. Nuchain help Indonesia prepare for entering the age of distributed network by providing ready-to-use system. Nuchain will attract the interest of developers and investors to contribute to the development of a distributed system in Indonesia, and eventually, bring benefits for Indonesia.

REFERENCE

[1] A. G. Khan, A. H. Zahid, M. Hussain, M. Farooq, U. Riaz, and T. M. Alam, "A journey of WEB and *Blockchain* towards the Industry 4.0: An Overview," *3rd Int. Conf. Innov. Comput. ICIC 2019*, no. January 2020, 2019, doi: 10.1109/ICIC48496.2019.8966700.

[2] F. A. Alabdulwahhab, "Web 3.0: The Decentralized Web *Blockchain* networks and Protocol Innovation," *1st Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2018*, pp. 1–4, 2018, doi: 10.1109/CAIS.2018.8441990.

[3] N. Garg and N. Garg, "Next Generation Internet (Web 3.0: Block Chained Internet)," *Cybernomics*, vol. 1, no. 6, pp. 19–23, 2019.

[4] "WEB3 Foundation." [Online]. Available: https://web3.foundation/.

[5] "Web3 Technology Stack." [Online]. Available: https://web3-technology-stack.readthedocs.io/en/latest/.

[6] (Eds.), M. Yano, C. Dai, K. Masuda, and Y. Kishimoto, *Blockchain and Crypt Currency Building a High Quality Marketplace for Crypt Data*. 2020.

[7] A. E. Prasetiadi, "Web 3.0: Teknologi Web Masa Depan," vol. 1, no. 3, pp. 1–6, 2011.

[8] M. Harikrishnan and K. V. Lakshmy, "Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network," *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, pp. 307–312, 2019, doi: 10.1109/ICACCS.2019.8728462.

[9] S. M. Habibul Mursaleen Chowdhury, F. Jahan, S. M. Sara, and D. Nandi, "Secured *blockchain* based decentralised internet: A proposed new internet," *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3377049.3377083.

[10] "Substrate." [Online]. Available: https://Substrate.dev/.

[11] "Substrate Consensus." [Online]. Available: https://Substrate.dev/docs/en/knowledgebase/advanced/consensus.

[12] "BABE Consensus." [Online]. Available: https://Substrate.dev/rustdocs/v3.0.0/sc_consensus_babe/index.html.

[13] "Finality Grandpa." [Online]. Available: https://Substrate.dev/rustdocs/v3.0.0/sc_finality_grandpa/index.html.

[14] "Sequential Phragmén Method." [Online]. Available: https://wiki.polkadot.network/docs/learn-phragmen.

[16] A. S. Jat, "Comparative Analysis of Existing *Blockchain* Based Certification DApps Comparative Analysis of Existing *Blockchain* Based Certification DApps," no. January 2020, 2021.