Clover:
Next Generation DeFi Platform

by Clover

Version 1.0.0

Abstract

Recently, we have seen many DeFi-centric projects which have created a brand new business model and a large amount of locked-in value assets in the blockchain space. In fact, the total value locked in the DeFi projects grew from just under $600M to more than $7B within a span of 12 months. However, most of these projects are either too slow, very expensive or centralized. In this project, we propose a brand new decentralized exchange, called Clover, which is fast, cheap, and trustless to eliminate these drawbacks. Clover has been designed as a parachain on Polkadot as open DeFi platform by leveraging all the excellent features of Polkadot and providing both secure and fast communication with other existing parachain projects.

Contents

1 Introduction

DeFi (or decentralized finance) is an area of great interest in the blockchain space. This refers to financial services using smart contracts (that are automatically enforceable agreements) through the blockchain network that do not need intermediaries such as a bank. As of writing this paper, the total value locked in DeFi contracts exceeds $7 billion [3]. Along with this interest, DeFi caused a huge increase in the value (market value) of all tradable tokens used for smart contracts. However, many DeFi projects have still not been able to deliver the desired performance.

Main Challenges of DeFi:

- Many DeFi projects have been built on the Ethereum blockchain. During times of high usage, Ethereum has had blockchain blockage issues. If the network is congested, the transaction may remain in a standby state, ultimately causing market inefficiency and information delays. These technical scalability issues are closely related to liquidity risks. Given the current situation in terms of efficiency, DeFi can only be efficient on Ethereum if Ethereum will have greater user base growth.
- While Ethereum-based DeFi remains an unattainable investment for small retail investors, the need for a fast and cheap blockchain is growing day by day. Increasing gas fees in Ethereum in particular are just one example of this.
- DeFi projects that live exclusively on Ethereum are only heavily dependent on a successful Ethereum 2.0 that is expected to take at least a few more years. Other smart contracts offering blockchain platforms (such as EOS, Tezos) could also take over Ethereum's leading role in the DeFi space. However, they have other issues such as insufficient decentralization.
- Many DeFi applications have also been managed by certain team or company and are far from being truly decentralized, although, once established, they generally aim towards de-centralizing governance and decision making. As long as an application is semi-centralized (with funds transiting through an intermediary or with an intermediary being able to freeze funds), counterparty risk exists, and the intermediary that has control over the assets may use the funds maliciously.

Substrate, which is the foundation for Polkadot (designed Rely chain act as a link between many different Para chains) is a standalone blockchain framework, which allows developers to build highly advanced blockchains customized for any project. Clover is an open DeFi platform which is a parachain developed on the Polkadot network [6, 8].

1.1 Features of Clover

Clover creates a marketplace for issuing, exchanging, staking, and lending digital assets. On Clover, users can basically

- issue new tokens to digitalize assets,
- propose to create trading pairs between two different tokens, buy or sell assets through trading pairs created on the chain, put assets into a pool for lending, and
- stake native token to join Clover governance and hold the native token to receive rewards.

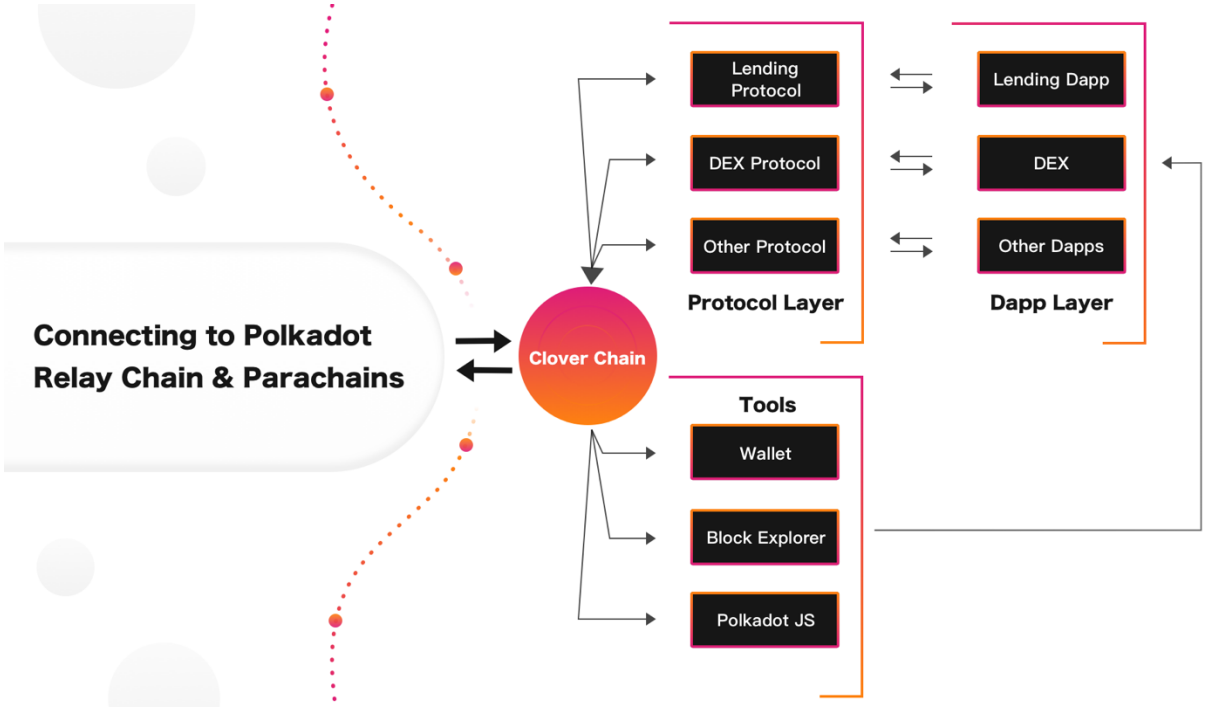

Figure 1: The features of Clover

1.2 Advantages of Clover Compared to CEX

Compared to Centralized Exchanges (CEX), Clover has the following advantages:

- Quick access: No need to register or verify an account.
- Peer-to-peer: No one can stop or control the trading.
- Trustless: There is no centralized entity for governance. Namely, the crowd community (i.e., token holders) has the full control over the system through voting process using governance smart contracts.
- Cheap and faster transactions: Operations are direct, there is no need to wait for the exchange and to pay fees.
- Security: The exchange does not hold your funds (i.e., they do not possess the signing keys).
- Privacy: No personal information has been stored on an external data storage.
- No manipulation: No one can create fake orders or market volume to activate the trades.
- Efficiency: Since Clover is a parachain on Polkadot, it enables scalability by al-lowing specialized blockchains to communicate with each other in a secure and trustless environment. Clover can communicate with other parachain projects through the Polkadot platform.

1.3 Native Token

Clover has its native token which is called CLV, it represents the value of Clover.

CLV will be used in the following functions:

- Staking to maintain the its own consensus mechanisms.
- Serving as a transaction fee to be used in the marketplace.
- Has the right to receive rewards from Clover's profit.
- Used for election and voting of Clover governance mechanism.

Users can be nominator who secure the blockchain by selecting good validators and staking CLV tokens, and the meanwhile, nominator can earn CLV token by nominating any validators. Similar to some other blockchain system, CLV token serve as a transaction fee to maintain the system running. Namely, users use their CLV when they use the marketplace resources. A CLV token holder is also the shareholder of Clover. The profit of Clover will be regularly distributed to the CLV token holder.

2 Blockchain

Polkadot is a heterogeneous multi-chain technology which consists of a large number of parachains with potentially different features aiming to facilitate anonymity and verification processes. The Polkadot Relay chain aims to distribute the incoming transactions among the chains, so that more transactions can be transparently processed within the same period of time. Furthermore, it ensures that each chain remains secure. Customized adapters developed in parachains are able to open the connection by acting as a bridge between Polkadot and chains such as Ethereum and Bitcoin. Substrate, an open source, is modular and extensible software framework that you can use to develop your own blockchain project covering many scenarios with its various customizable modules. The code, that is developed with basic libraries such as database, net-working, consensus mechanism, memory pool, offered by Substrate is run in the blockchain is called Runtime. Runtime consists of a combination of many libraries which are developed in the Rust programming language. Clover protocol will focus on an open DeFi platform which will be implemented with Substrate framework, and will communicate with other existing parachains such as Bitcoin and Ethereum parachains (see Figure 2). Namely, Clover will be another parachain on Polkadot. Once the parachain got the slot to join to Polkadot relay chain, they can communicate with each other through Cross-chain Message Passing (XCMP) protocol [7]. That means Clover can build its DeFi with the other parachain assets, like the DeFi protocols on Ethereum.

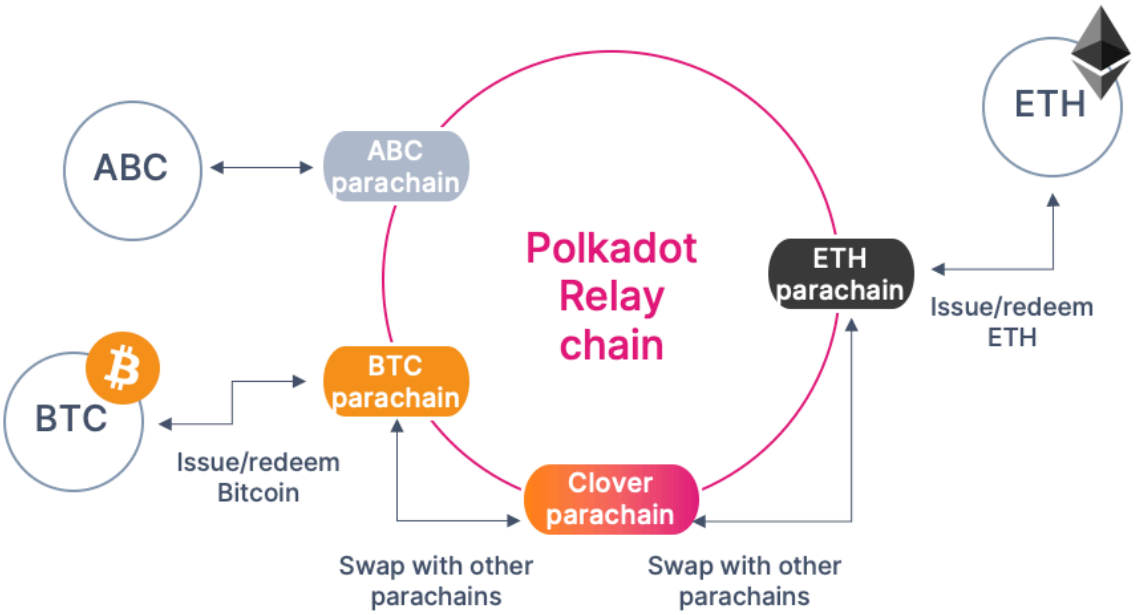

Figure 2: Clover with Polkadot Network

2.1 Consensus Mechanism: NPoS

The consensus mechanism in Clover is Nominated Proof-of-Stake (NPoS) which is the process of selecting validators to be allowed to participate in the consensus protocol [5, 2, 1]. We note that, on Polkadot Network, Validators and Nominators are the two main actors involved in NPoS.

- **Validators:** They provide the infrastructure and are responsible for the maintenance of the network. Namely, they are responsible to produce new blocks, validate Parachain blocks, guarantee finality, and ultimately secure the network. They are required to be responsive at all times and run secure, reliable infrastructure.
- **Nominators:** They are the token-holders who contribute to the security of the network by economically nominating up to 16 validators of their choice with their staked tokens. They share part of the rewards earned by the validators in the active set that they nominated. We would like to highlight that they are also subject to slashing in case of misbehavior by one of their nominated validators.

With NPoS, developers can continue to work on bounties, validators can secure the blockchain and validate proofs, and nominators can participate in the staking environment by nominating validators.

2.2 Substrate O -chain Worker (OCW)

To make the o -chain data integration secure and more efficient, Substrate provides o -chain workers (OCW). OCW is one of the most important features in substrate, it provides a strong native oracle solution to deal with complex task which cannot handle on-chain such as web requests, encryption/decryption and signing data, or the random number generation.

As for Clover, OCW can solve two main big issues: (1) providing large number of transaction per second (TPS), (2) lowering transaction fee by providing secure lightning network, state channel.

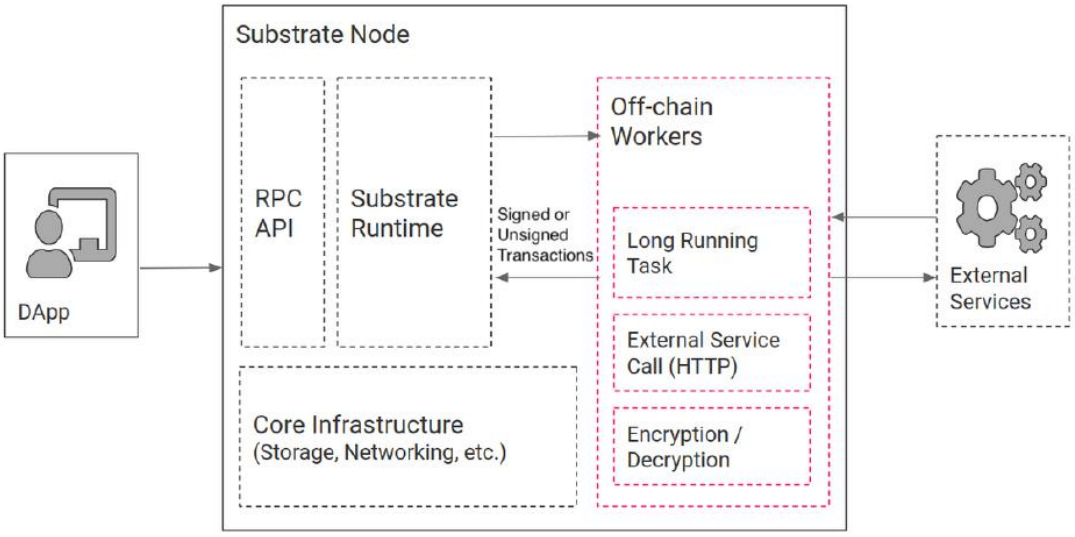

Figure 3: The architecture of Substrate Framework

2.3 The Usage of Oracles on Clover

Oracle is the most important part in Clover, some scenarios needs oracles like lending. In Clover, there is often a need to query and/or process o -chain data before it can be included in the on-chain state. The conventional way of doing this is through oracles which are external services that typically listen to blockchain events and trigger tasks accordingly.

When these tasks are completed, their results are submitted back to the blockchain through transactions. While this approach works, it has still several flaws with respect to security, scalability, and infrastructure efficiency. Substrate's OCW will make the o -chain data integration secure and more efficient. It provides ability to submit transactions (either signed or unsigned) to the chain to publish computation results, and a fully featured HTTP client allowing us to access and fetch data from external services. And the most important part is all things goes like \on-chain". Furthermore, it can be forkless upgraded by set the WASM code.

3 Services of Clover

3.1 Staking Liquidity Protocol

One of the most crucial tasks of Clover is to solve the illiquidity challenge of staked assets. In fact, more and more projects tend to use the PoS consensus mechanism as the first choice to tackle this challenge. On Clover, we would establish a staking pool tokenizing users' staked asset as S-Asset (e.g., SABC as a locked ABC), which users can invest or use in other applications. For example, you can lend SABC to earn interest or use SABC as collateral for a stablecoin like USDT. In summary, for any asset ABC, the staking liquidity protocol has the following features:

1. The protocol
    - manages the issuance of SABCs and the redemption of underlying assets, manages the locked assets,
    - participates in staking,
    - executes staking strategies (e.g., validator selection according to their uptime), manages rewards and slashed penalties.
2. SABC is tradable and liquid across all chains on the Polkadot network.
3. SABC is redeemable for underlying ABCs at any time with an option of redeeming immediately or transferring unbounded ABCs earlier.
4. The collateral ratio of SABC is algorithmically adjusted for staking strategy in order to ensure liquidity.
5. The protocol leverages the Polkadot's fascinating blockchain features such as security, speed, and reliability.

Through the protocol, staked assets (ABC) become fungible and liquid SABCs that exploit the derivative value of the ABCs fueling and powering more applications without sacrificing the security of the whole network. Users can essentially mint SABCs by supplying ABCs to the staking pool and redeem SABCs. The exchange rate between SABCs and the underlying ABCs are likely to increase over time, as staking rewards are accrued by validating and nominating, and is equal to the effective profit/loss, however, is determined by various factors including but not limited to:

- inflation rate of ABCs.
- the chosen staking strategy.
- the performance of chosen validator nodes.

As an example of ABC, the Clover staking liquidity protocol tokenizes staked DOT (called SDOT). The Clover staking liquidity Protocol establishes a decentralized staking pool where users would lock their tokens such as DOTs to gain staking yield while receiving SDOTs as a receipt that are liquid and tradeable.

3.2 Redeeming of a Synthetic Asset

Whenever a user wants to redeem his/her synthetic token (SABC) for the underlying ABCs, the users generally would have to wait for a certain recovery time for the ABCs to be transferable (e.g., for DOTS, 28 days as this is written). If the users do not want to wait

during that time and still are willing to redeem their SABCs immediately (or within a shorter period of time), then the staking liquidity protocol will charge a small portion of the locked assets and will return the rest to the user. Moreover, the redeem service fee is payable in CLV tokens.

Insurance Pool. In order to request an immediate redeem, a certain amount of collateral assets should have been reserved in advance on an Insurance Pool. Users can deposit their assets to this pool but not receive any synthetic token in return. In case of an immediate redeem demand for a synthetic token (e.g., 100 SABC), a certain portion of the corresponding asset will be sent back to the user (e.g., 98 ABC) and the difference between synthetic and the corresponding assets (2 SABC = 100 - 98) will be distributed to the supporters who deposited to Insurance Pool.

4 Decentralized Trading Protocol

Each trading pair stores a combined reserve of two assets and provides liquidity for these two assets, thereby maintaining the invariability of irreducible reserve products. The parity rate between two real tokens is defined as

$$Index_{i,j} = token_i / token_j$$

where $token_i$ and $token_j$ denote existing assets in the exchange to reach an automatic liquidity agreement.

Moreover, the trader pays 0.3% fee for every transaction which will be proportionally distributed to the liquidity provider.

4.1 Support any Trading Pair

Because of Polkadot's own heterogeneous multi-chain architecture design, DOT will become the anchor asset of each parachain, which will make routing simple and reduce the dispersion of liquidity. However, all liquidity providers have \DOT exposure". If DOT is used as a transition currency, it will bring more costs to the transaction. Bene ting from Polkadot's architectural design, each parachain asset can circulate freely on the Polkadot network. Hence, this agreement will support arbitrary Polkadot transaction pairs to provide liquidity, achieve specific transaction requirements, and reduce transaction wear and tear.

4.2 Price Oracles

The marginal price provided Clover at t-th block number can be calculated as:

$$p_{a,b} = r_t^a / r_t^b$$

where $p_{a,b}$ is constant value, and r_t^b, r_t^b denote reserve of token a, b at the block t respectively. The arbitrageur will trade with this agreement. The price provided by the agreement tends to track the relative market price of the asset, which also means that it can be used as an approximate price prediction.

4.3 Protocol Fees

This agreement defaults that the trader needs to pay 0.3% of each transaction as the transaction fee, but the developer can set the specific fee for each transaction pair. If it is set to 0, only the transaction fee on Polkadot needs to be paid.

5 Decentralized Lending Protocol

Centralized exchanges allow customers to use the exchange's built-in \lending market" to trade. However, in a centralized marketplace, any issue of trust is resolved by relying on a trusted third party. On the other hand, the peer-to-peer agreement directly promotes mortgage and unsecured loans between market participants. The agreement establishes a fund pool based on changes in the supply and demand of assets, and the interest rate is calculated by algorithms. The supplier and borrower of the asset interact directly with the agreement to earn or pay floating interest rates.

5.1 Supply Assets

In a peer-to-peer platform, a user's assets are lent to another user. Unlike the exchange's platform, the agreement summarizes the supply of each user; it provides more liquidity and maintains the balance of the capital system. Borrowers and lenders can receive rewards (interests) by complying with the corresponding agreements while circulating digital currency. The exchange can adjust the agreement increment or reward users by \clearing" the balance.

5.2 Borrow Assets

Users can mint synthetic tokens (SABC) by supplying assets (ABC) to the market where these are used as collateral for asset borrowing. Every money market has a floating interest rate set by market forces, which determines the borrowing cost of each asset.

- **Collateral value.** The assets held by the agreement have a mortgage factor ranging from 0 to 1. The liquidity and value of the underlying assets determine the size of the mortgage factor. The collateral and multiplied by the mortgage factor are equal to the user's loanable amount.
- **Risk and liquidation.** If the outstanding loan value of an account exceeds its ability to repay the loan, a portion of the loan can be repaid at the current market price minus the liquidation discount to eliminate the risk of the agreement. If the user's funds are in a repayment crisis, the liquidation process may continue. Any Clover address with borrowed assets can call the clearing function and exchange its assets for sToken collateral of the borrower. Since these two users, assets and prices are included in the agreement, the clearing can be executed very conveniently and does not rely on any external systems or orders.

Use Cases. Borrowing mechanism provides the following advantages to the DApp consumers, traders and developers.

- DApp can borrow tokens from our system without waiting for order execution or requiring o -chain computation,
- Traders can use their existing investment portfolios as a collateral to raise their funds by borrowing DOTs or a stable token.
- Traders who wish to short the token can borrow it, send it to the exchange and sell the token, and then gain short-selling.

5.3 Interest Rate Model

The interest on our system depends only the rate equilibrium between supply and demand. When demand is low, interest rates will also be low, and vice versa. The money market is defined by interest rates that are uniformly applicable to all borrowers. As the relationship between supply and demand changes, interest rates will adjust over time.

5.4 Liquidity Incentive Structure

The agreement does not guarantee liquidity; instead, it relies on the interest rate model to motivate it. During periods of extreme demand for assets, the liquidity of the agreement (tokens that can be withdrawn or loaned) will fall; when this happens, interest rates will rise,

stimulating supply and inhibiting lending. This is based on automatic incentives provided by the market and algorithms. However, the main incentive provided in the initial stage of the agreement is the incentive to obtain tokens through loan behavior.

6 Staking Rewards Protocol

Pledge liquidity, trading and lending will all get the token incentives of this agreement. The token will be set to pledge status by default, and the daily DOT handling fee generated by the platform will be proportionally distributed to the agreement token pledge users. Rewards weights need to measure two parameters, one is the number of tokens, and the other is the pledge duration, in order to encourage users to continue to provide liquidity for the platform and increase user stickiness, with the goal of truly accumulating product value, and the agreement token is the platform After the initial empowerment, users are inclined to use the tool attributes of the agreement for a long time.

7 Governance

Clover is open platform and it will have the ability to get other people to contribute modules. In this context, we expect token holders to help guide the protocol to its fully potential through experimentation and active participation. Community can propose, vote, and implement changes through governance module. The structure is as follows:

1. **Proposal:** A proposal is mechanism for updating a parameter of the system where it is submitted for community votes to decide accept/reject. Every proposal has a submission fee in the system. The duration of a voting process for a proposal is 5 days whereas there can be max 5 proposals in the voting process (i.e., if there are more proposals they have to wait in the queue).
2. **Vote policy:** One token represents one voting power in the voting system. Tokens must be held for 7 days to be valid for votes. The proposal will be accepted as long as at least 2/3 of the votes accept. Only token holders can participate in voting process and they can get rewards once the proposal is successfully completed.
3. **Governing parameters:** Token holders can vote to set and change parameters in the DeFi environment. The parameters include the percentage of tokens for burning in different burning mechanisms, the percentage of tokens for staking, the amount of tokens that a new listing needs to pay, and incentive token release schedule etc. Parameters will be set to default at the beginning and can be voted to change after launch.
4. **Governing development:** This involves structural changes for the DeFi environment.

   For example: implementing new functionalities, deploying the protocol on additional smart contract blockchains, introducing more DeFi elements. Token holders need to make proposals and submit to the governance smart contracts for reviews and votes.

Unlike existing systems, Clover will utilize a decentralized governance of the protocol for setting the interest rate model per asset. A governor can submit a proposal for updating any parameter in our protocol. The proposal will be voted by the community that has native token. The governance module has the following rights:

- Listing a new asset on market.
- Withdrawal of the reserve of a token.
- Updating the oracle address.
- Updating the interest rate model per market.

References

[1] Alfonso Cevallos. How nominated proof-of-stake will work in polkadot, https://medium.com/web3foundation/how-nominated-proof-of-stake-will-work-in-polkadot-377d70c6bd43. Accessed: 2020-08-30.

[2] Staking Facilities. What is nominated proof-of-stake?, https://medium.com/@stakingfac/what-is-nominated-proof-of-stake-889fc22bef8f. Accessed: 2020-08-30.

[3] FR24NEWS. De exceeds $7 billion in locked-in funds, but only six projects hold 90% stake. https://www.fr24news.com/a/2020/08/de -exceeds-7-billion-in-locked-in-funds-but-only-six-projects-hold-90-stake.html, Accessed: 2020-08-30.

[4] Crust Network. Crust- chain to decentralized cloud, https://crust.network/. Accessed: 2020-08-30.

[5] Polkadot.Polkadot launch: Nominated proof of stake phase,

https://polkadot.network/launch-npos/. Accessed: 2020-08-30.

[6] Polkadot. Polkadot network, https://polkadot.network/. Accessed: 2020-08-30.

[7] PolkaWorld. Xcmp, https://medium.com/@polkaworld/whats-the-signi cance-of-xcmp-to-polkadot-ba9c4a283fd1. Accessed: 2020-08-30.

[8] Polkadot Wiki. Parachain, https://wiki.polkadot.network/docs/en/learn-parachains. Accessed: 2020-08-30.