YOSEMITE Public Blockchain

- **No ICO** : using real money (e.g. USD, EUR, CNY) with no native crypto-currency
- **Proof-of-Transaction (PoT)** : reasonable and fair consensus algorithm
- **General Financial Platform** : designed for government and enterprise uses

Technical White Paper

Bezalel Lim / bezalel@yosemiteX.com Patrick O'Grady / patrick.ogrady@yosemiteX.com

Brandon Griffin Joe Park Anthony Di Franco Eugene Chung Eric Hwang

Feb. 2018

Abstract

We introduce a new method of public blockchain design without issuing any native crypto-currency minted by blockchain itself. Instead, fiat-pegged stable coins (e.g. *dUSD*, digital USD-pegged credit tokens) are issued as the foundational crypto token of the blockchain, provided a trust entity such as a trusted financial institution or government backs the stable coins with an equivalent fiat money reserve. The YOSEMITE Blockchain is basically designed as a decentralized exchange platform in which various kinds of tokens, such as fiat-pegged-tokens, crypto-pegged-tokens and real-asset-tokens, are issued by the trusted entities (the Depositories) and traded securely and transparently on blockchain. We also proudly present a new blockchain consensus mechanism, called Proof-of-Transaction (PoT), which incentivizes the application service providers directly contributing to the blockchain ecosystem by generating actual blockchain transactions, quantitatively measured by Transaction-as-a-Vote (TaaV). A novel PoT-based BFT consensus with short block time and fast block finality realized by Optimistic-Block-Production and optimized block validity voting protocols enables the blockchain to scale, with extended scalability provided by the existing YOSEMITE on/off-chain hybrid exchange technology. The named multi-sig blockchain accounts organizing the trust network for account recovery enable the solid and stable YOSEMITE Blockchain ecosystem, along with the integrated KYC/AML support for the regulatory compliance.

Table of Contents

1 Public Blockchain Without Native Crypto-currency

The common belief for public blockchains holds that there should be a native crypto-currency which is pre-minted through an ICO presale process or minted by the blockchain itself for every new block as the reward to block producers. Bitcoin[1] and Ethereum[2] have their own native crypto-currencies (BTC, ETH) to incentivize miners to maintain the blockchain network securely through a Proof-of-Work(PoW)-based competitive consensus mechanism, which proves slow and inefficient. For Proof-of-Stake(PoS[3])-based blockchains (EOS[4], NEO, DASH, ...), native crypto-currencies are essential to elect block producers who participate in the consensus process to make new blocks. In PoS blockchains, governance is commonly designed by utilizing a voting system in which the native crypto-currency holders cast weighted votes in proportion to their currency holdings or stake (vest) their crypto tokens to have more influence over blockchain governance.

The native crypto-currency in one blockchain is regarded as the basic assumption and agreement among the stakeholders of the blockchain ecosystem (developers, investors, block producers, service providers, end users) and used as the basic building block for blockchain system design, though native crypto-currencies induce some critical problems in existing blockchain ecosystems. The public blockchain's native crypto-currencies traded in public exchanges are speculative assets which are constantly being involved in pump-and-dump schemes, making the native crypto-currencies highly volatile in price. For ordinary people who are naturally accustomed to stable fiat-currency like USD, it is very uncomfortable to use unstable crypto-currency as a payment/trading currency. People would not buy food in grocery stores using highly volatile company shares as a method of payment, and similarly they would not use existing crypto-currencies. Even worse, to use services provided by the blockchain platform, people first need to buy crypto-currency by selling their fiat money through an external crypto exchange. This is the big hurdle against mass adoption of blockchain-based applications setting aside the scalability issue which encumbers current public blockchains. Additionally, the financial benefits gained from these speculative crypto-currencies are unfairly concentrated amongst blockchain developers who maintain large portions of coins after ICOs and early stage investors who can buy a disproportionate amount of total supply at cheap prices. Meanwhile the followers adopting the blockchain, even if they are the service providers who are directly contributing to the blockchain ecosystem by making applications generating meaningful transactions, are relatively less compensated. In the same manner, blockchain governance power also can be unfairly concentrated to the big token holders resulting in inevitably centralized power. It is also impractical to expect most of the long tail blockchain users to

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf, 2008.
[2] V. Buterin, Ethereum: A next-generation smart contract and decentralized application platform, https://github.com/ethereum/wiki/wiki/White-Paper, 2013
[3] Proof-of-Stake systems - https://en.wikipedia.org/wiki/Proof-of-stake
[4] EOS.IO technical white paper, https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md, 2017

participate in an explicit voting process to democratically control blockchain governance (e.g. voting for electing block producers).

In this paper, we introduce a new method of public blockchain design without issuing native crypto-currency minted by the blockchain itself. Instead, the fiat-pegged stable coins (e.g. digital USD credit token) are issued as the foundational crypto-currency of the blockchain, provided a trust entity such as a trusted financial institution or government backs the stable coins with an equivalent fiat money reserve. Fiat-pegged stable coins are not likely to be involved in speculation and most people are familiar and comfortable with stable fiat currencies. And we proudly open a new horizon of blockchain consensus mechanism called Proof-of-Transaction (PoT) which incentivizes the application service providers directly contributing to blockchain ecosystem by generating actual blockchain transactions. The blockchain network collects transaction fee profits by using fiat-pegged stable coin as the currency for fee payment. Special administrative power is entitled to the trust entity under the social agreement of all players running and using the blockchain (e.g. citizens use their national blockchain whose trust entity is the national government, customers of a trusted financial institutions use the blockchain operated by the institution). The trust entity only can execute predefined and restricted administration operations on blockchain. All the blockchain transactions are provably immutable and transparent to everyone including the administration actions of the trust entity. Every block containing recent transactions is produced in a transparent and secure manner through the reasonable and fair Proof-of-Transaction consensus mechanism, allowing any entity to participate the blockchain consensus process together with the trust nodes appointed by the trust entity. The YOSEMITE Blockchain is basically designed as a DEX (Decentralized EXchange) blockchain which provides token exchange operations (token sell/buy order) as a core pre-built blockchain transaction type. The trading fees from on-chain token exchange transactions are collected and distributed to the trust entities and the service providers.

2 YOSEMITE Blockchain as Decentralized Exchange Platform

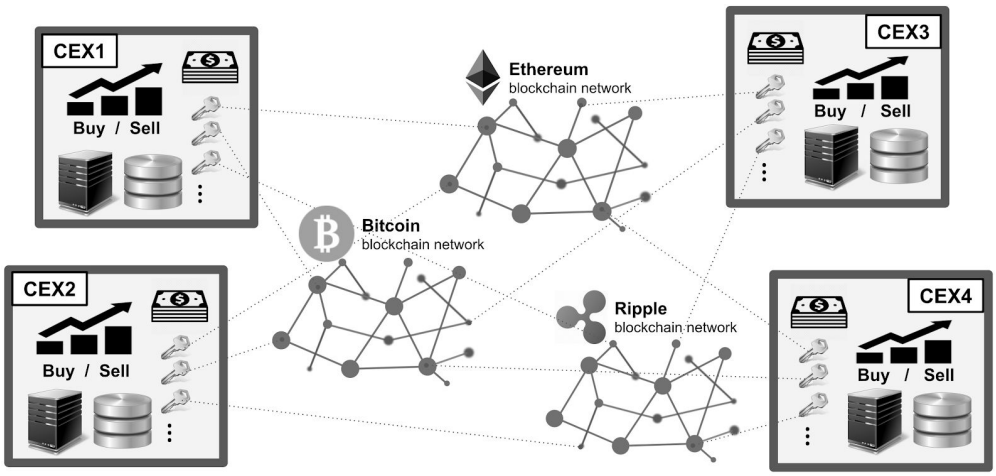

Figure 2.1 - Crypto trading on the siloed centralized exchange systems

The problem of centralized crypto-currency exchanges (CEX) is that they are the opaque siloed systems. Although the crypto-currencies traded in the exchanges are minted and circulated on the decentralized network of transparent public blockchains, the centralized exchange system itself is not an open platform. Rather, only the exchange service operator has full access rights in a siloed server system with the private application servers and database systems, like a usual web application. Nevertheless, the reason why most crypto-currency trading volumes so far are processed in these centralized exchanges is that the centralized servers can efficiently handle the huge trading transaction volumes and their relatively easy usability, whereas on-blockchain trading transactions are usually very slow, the transaction throughput is very low, and the blockchain transaction fees (e.g. gas fee in Ethereum) must be paid by users. But, the critical problem of any centralized exchange is that the trading transactions can be manipulated by the service operator, because once crypto-currencies and fiat funds are deposited to the centralized exchange, the trading transactions are actually just modifications of the private databases for which the service operator has full read/write access. The transaction data of the centralized exchanges are not immutably transparent to the external world. Even worse, since the deposited crypto-currencies and fiat funds are held by each centralized exchange, the assets can be maliciously hacked by external or internal hackers , which has resulted in huge financial loss to many exchange users.

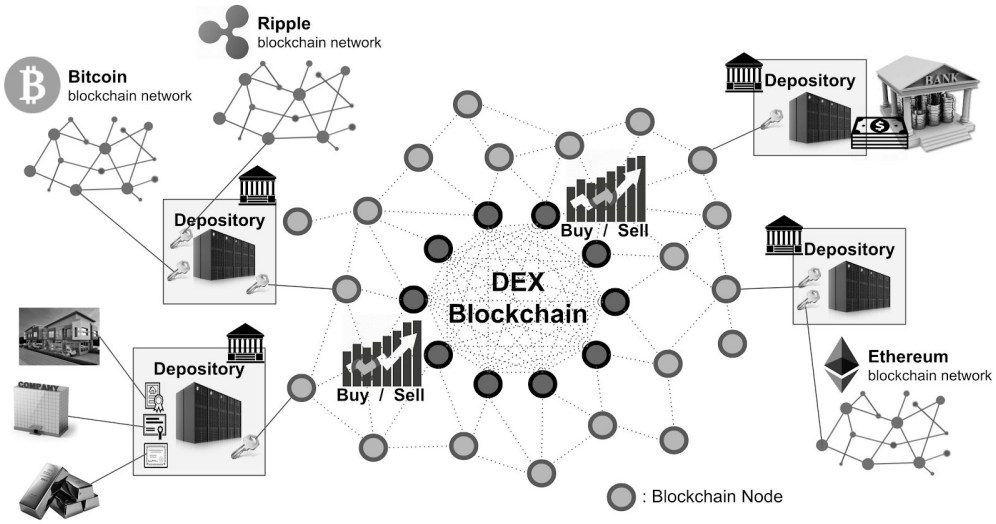

Figure 2.2 - Decentralized Exchange architecture of YOSEMITE Blockchain

The above diagram illustrates the decentralized exchange (DEX) platform architecture which can be built upon the YOSEMITE Blockchain. The crypto tokens backed by either fiat money funds held in trusted banks, crypto-currencies of external public blockchains, or real assets managed by trusted Depositories, are issued and circulated in the YOSEMITE Blockchain in a transparent and secure manner. Unlike a centralized exchange, buy/sell orders for the token exchange are submitted as blockchain transactions signed by the user's private keys, order-books are on-blockchain and all the order-matchings are validated and transacted by the elected block producers. The trading transactions are immutably transparent to the public and cannot be manipulated by a centralized actor. The fiat-pegged stable coins issued through the trusted Depositories are used as the trading currency and transaction fee payment. The YOSEMITE Blockchain is basically a decentralized exchange platform in which various kinds of tokens are traded securely and transparently with the fiat-pegged stable coin as the native crypto-currency of the blockchain providing high speed and throughput of blockchain transaction processing.

3 Depository and Tokens Issued on YOSEMITE Blockchain

The Depository is the entity that issues tokens in YOSEMITE Blockchain and ensures the value of issued tokens by holding assets outside the blockchain of equal value backing the issued tokens. Whenever a token holder requests to redeem or withdraw their tokens, the Depository who issued the token should burn the requested amount of tokens on blockchain and hand over the corresponding amount of the backing asset to the user. The YOSEMITE Blockchain provides built-in operations for issuing/redeeming(burning) tokens which can be circulated on the

blockchain. The issued token symbols are tagged by the account ID of the Depository who issued the tokens. A token can be redeemed by only the Depository whose ID is tagged on the token symbol.

dUXD/D1 : UX-Dollar-pegged digital UXD token issued by the Depository D1, only redeemable by D1
dBTC/D2 : Bitcoin-pegged digital BTC token issued by the Depository D2 holding the private keys controlling the issued amount of actual Bitcoin, only redeemable by D2

If multiple entities issue UXD-pegged tokens, each token tagged by each Depository should be redeemed by the tagged Depositories. The tokens can be issued by any blockchain accounts acting as a Depository, but should earn trust from the blockchain users to be circulated on the blockchain. The Depositories always are required to prove the secure existence of the backing real assets transparently to be trusted.

3.1 Fiat-Pegged Stable Coin (*dFIAT*) as Native Crypto-Currency of Blockchain

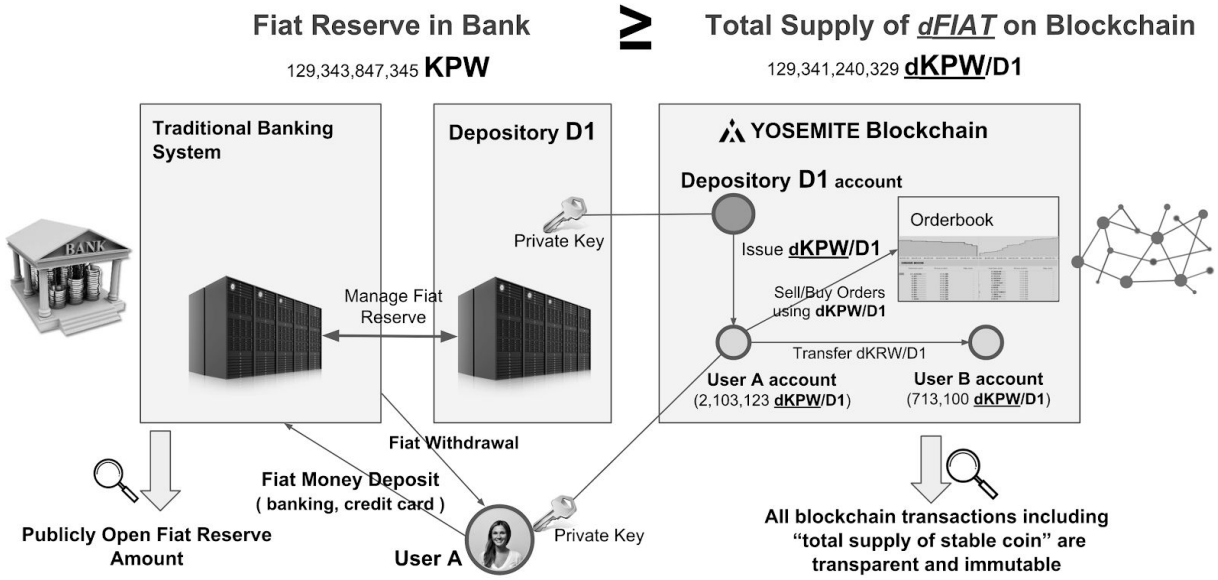

Figure 3.1 - Fiat-pegged stable coin(*dFIAT*) as native currency of YOSEMITE Blockchain

The fiat-pegged stable coin is the native crypto token on the YOSEMITE Blockchain, maintained by a one-to-one backing of fiat money reserve outside the blockchain, and is issued by special Depositories authorized by the top trust entity in the system, such as the government or a trusted financial institution. This special fiat-pegged stable coin is the foundational currency in YOSEMITE Blockchain, where it is used for transaction fee collection from every blockchain

transaction, as well as the trading currency for on-chain token exchange and the payment method for blockchain applications. In YOSEMITE Blockchain, these kind of stable coins are called as ***dFIAT*** (digital FIAT token). Below are the examples of *dFIAT*.

- **dUXD/TFI** : UXD-pegged stable coin, digital UXD, issued by a trusted financial institution (TFI), which could serve as the native crypto-currency of a blockchain operated in a country where people use UXD dollar as currency.
- **dKPW/BK1** : KPW-pegged stable coin, digital KPW, issued by a trusted bank (BK1), which could serve as the native crypto-currency of a blockchain operated in a country where people use KPW as currency

...

Unlike the other public blockchains' native crypto-currencies, there is no currency inflation for the native currency in YOSEMITE chain, *dFIAT*, because it is only issued when the users of the blockchain deposit their fiat money to the *dFIAT* Depository. If a user sends 1000 KPW worth of fiat money through an existing payment channel (e.g. wire-transfer, credit card payment) to the bank acting as the authorized Depository (BK1), the same amount (1000) of dKPW/BK1 can be issued to the user's blockchain account. The Depository system manages the fiat reserve by interfacing with traditional secure banking systems and handles *dFIAT* token issuance/redeeming by interfacing with the blockchain using the securely stored private key. Because the guarantee of redeeming of *dFIAT* to actual fiat money is crucial for the YOSEMITE Blockchain, the existence of trust entities receiving widespread public support is indispensable in YOSEMITE Blockchain design. Only the Depository(ies) authorized in blockchain by the top trust entity can issue and redeem *dFIAT*, but users will ultimately decide which Depositories' tokens to use and trust.

The public ledger of *dFIAT* token distribution for every blockchain account is maintained transparently and securely by the blockchain network. All blockchain transactions such as issuing/redeeming(burning) *dFIAT*, transferring *dFIAT* to another account (while consuming a small amount of *dFIAT* as transaction fee), and exchanging tokens using *dFIAT* as trading currency and transaction fee, are transparent and securely immutable since the transactions occur on the blockchain. Since all actions of the *dFIAT* Depository are also transparent and traceable, the total supply of the *dFIAT* token being circulated on blockchain is always public information. So, if the trustworthy bank holding the fiat money deposited through the *dFIAT* Depository allows public access to the current fiat money reserve balance in a reliable way, blockchain users can transact on the YOSEMITE Blockchain without fear or uncertainty of *dFIAT* redeem. Total supply of the *dFIAT* on the blockchain should always be less than or equal to the fiat reserve amount in the trustworthy bank.

3.2 External-Crypto-Currency-Pegged Token (*dCRYPTO*)

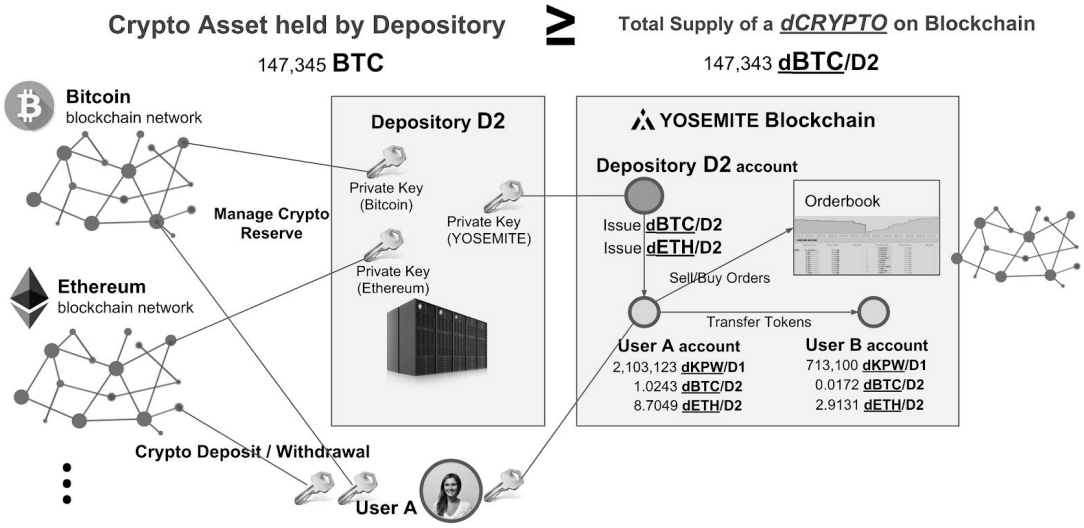

Figure 3.2 - Crypto-Currency-Pegged Token (*dCRYPTO*) issued by Depository

The crypto-currency-pegged tokens (*dCRYPTO*, digital CRYPTO token) can be issued by the Depositories in the same way as the fiat-pegged stable coins. A Depository issues the exact amount of *dCRYPTO* token only when a blockchain user deposits the same amount of crypto-currency to the Depository's external blockchain (e.g. Bitcoin, Ethereum) account, of which the private key is owned by the Depository. A *dCRYPTO* token holder can always request to redeem *dCRYPTO* to the actual crypto-currency, then the Depository has to burn *dCRYPTO* token in the YOSEMITE Blockchain and transfer the burned amount of the external crypto-currency to the token holder in the corresponding external blockchain. For example, the dBTC/D2 token is the Bitcoin-backed crypto token issued by the Depository D2. When user A deposits 1.25 BTC to Depository D2 on Bitcoin blockchain, 1.25 dBTC/D2 is issued to the user A's YOSEMITE blockchain account, regardless of the USD worth of the crypto-currency. If the user A requests Depository D2 to redeem 0.5 dBTC/D2, then D2 transfers 0.5 BTC to user A's Bitcoin account from the BTC reserve of D2. The issued *dCRYPTO* tokens can then be transferred and traded on the YOSEMITE Blockchain.

The total supply of *dCRYPTO* is transparent and tamper-proof public information because *dCRYPTO* is issued and circulated on the blockchain, i.e. all transaction data is held in the decentralized ledger. Also, the amount of the crypto-currency owned by the Depositories can be transparently verified by the corresponding external blockchain network. So, if the Depositories publish their account addresses holding the external crypto-currency reserve and provide the proof of the ownership of the private keys in external blockchains (e.g. providing the cryptographic signature for the unpredictable recent block hash), YOSEMITE Blockchain users can safely use *dCRYPTO* tokens on the YOSEMITE Blockchain. To gain trust from blockchain users, the Depositories issuing *dCRYPTO* tokens should be run by trusted institutions like banks

and the private keys must be securely managed within the environment guaranteeing high-level security.

3.3 Real Asset Token (*dASSET*)

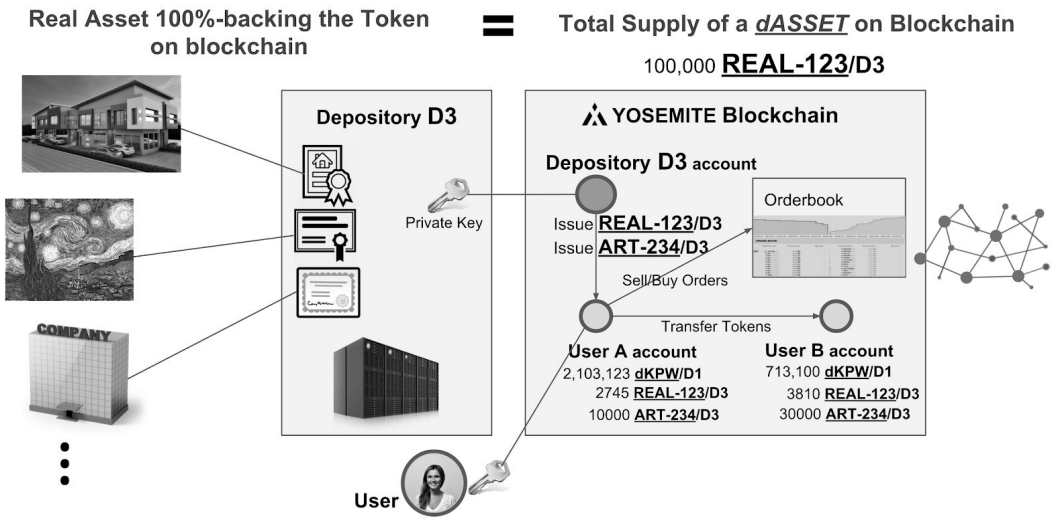

Figure 3.2 - Real asset token (*dASSET*) issued by Depository

Depositories can also issue real asset-backed crypto tokens (*dASSET*, digital ASSET token) on the YOSEMITE Blockchain. The real assets, such as real estate, art pieces, (unlisted) company shares, gold, diamond and so on, can be tokenized through trusted Depositories connecting the real assets and the *dASSET* tokens. For example, REAL-123/D3 is the real estate token issued for a building managed by Depository D3, and can be used to trade shares of the building. The Depository issuing *dASSET* is required to securely manage the ownership of the tokenized real assets and keep the real asset safe physically. The partial ownership of the tokenized assets can be traded on the YOSEMITE Blockchain. The open market determines the price of the assets through on-chain token trading. If there is revenue generated from the tokenized asset, e.g. getting monthly rent, the profit can be distributed to the *dASSET* token holders transparently on the blockchain. If someone wants to purchase total ownership of a publicly tokenized asset (e.g. real estate, art-piece), one can submit an asset acquisition proposal by escrowing a sum of fiat-pegged stable tokens corresponding to the proposed purchase price (usually total market cap of the asset plus premium). If the shareholders of the asset token approve the suggested price by voting in proportion to the *dASSET* tokens owned by each shareholder, the total ownership of the real asset is transferred to the asset buyer (e.g. ownership transfer on property deed, delivering the art-piece to the buyer), the escrowed purchase payment is distributed to the *dASSET* token holders proportionally, and all the *dASSET* tokens for the sold asset on blockchain are burned. The operations required to facilitate real asset tokenization such as issuing/burning tokens, transferring/trading tokens, revenue distribution, proposing asset acquisition, escrowing purchase payment, and voting are natively provided by the YOSEMITE Blockchain.

4 Built-in Token Operations in YOSEMITE Blockchain

In the YOSEMITE Blockchain, the built-in operations to implement the on-chain decentralized token exchange are provided at the core level. The crypto token issue/redeem, token transfer, and token exchange order operations are provided as primitive blockchain transaction types.

- **Issue / Redeem (Burn) Token**

  A Depository can submit Issue-Token transactions to issue crypto tokens backed by real assets securely held by the Depository on blockchain, and make Redeem-Token transactions to burn issued crypto tokens to withdraw the real asset to the requesting users. The Issue/Redeem-Token transactions should be crypto-signed by the private key of the Depository account.

  e.g. Issue 10,000 dKPW/D1 to account-A, Redeem(burn) 5,000 dKPW/D1 and withdraw 5,000 KPW to user-A's bank account, Issue 1.353 dBTC/D1 to account-B, Issue 10.515 dETH/D2 to account-C

- **Token Transfer**

  A blockchain user can transfer his/her own crypto tokens held by the user's blockchain account to any other blockchain accounts. The Token-Transfer transaction should be crypto-signed by the private key of the token sender's account. The transfer transaction fee should be paid using the fiat-pegged stable coin, native to the YOSEMITE Blockchain. A Token-Transfer transaction can be blocked if the transfer is not legitimate (e.g. not KYC-authorized account). For the Tx-Vote field, refer to 5.1 "Transaction-as-a-Vote" part.

  e.g. [From : account-A, To : account-B, Amount: 50,000 dKPW/D1, Tx-Fee : 100 dKPW/D1, Tx-Vote : Node-K-address]

- **Token Exchange Order**

  A blockchain user can submit buy/sell orders to trade his/her own crypto token. The token exchange orders are matched automatically by the block producers who execute the actual token trade between the buy/sell order submitters and collect the exchange transaction fees paid with fiat-pegged stable coins. The Token-Exchange-Order transaction should be crypto-signed by the private key of the order maker's account. For the Tx-Vote field, refer to 5.1 "Transaction-as-a-Vote" part. An open order which is not yet fully filled can be cancelled by a Cancel-Order transaction signed by the same

account, with no transaction fee charged for the cancel operation.

e.g. [*From* : account-A, *Buy* : dETH/D2, *Sell* : dKPW/D1, *Amount* : 3, *Price* : (1:150,000), *Tx-Fee* : 450 dKPW/D1 (0.1%), *Tx-Vote* : Node-A-address]
[*From* : account-B, *Buy* : dKPW/D1, *Sell* : dETH/D2, *Amount* : 200,000, *Price* : (100,000:1), *Tx-Fee* : 200 dKPW/D1 (0.1%), *Tx-Vote* : Node-Q-address]

Since the core operations required to build an exchange service are supported as the primitive blockchain transactions, the on-blockchain exchange service can be directly implemented on the YOSEMITE Blockchain.

The transaction fees, paid in fiat-pegged stable coins (e.g. dKPW/D1), are collected and held in the transaction fee profit pool on the blockchain. The collected transaction fee profits are periodically distributed to the blockchain operators like block producers.

Token-Transfer operations are immediately charged transaction fees in *dFIAT*, preventing DoS[5] (Denial of Service) attacks. For Token-Exchange-Order transactions, only blockchain accounts holding non-zero amount of tokens (including the transaction fee) not locked in the open orders can make exchange transactions, similar to bandwidth allocation based on token ownership without spending any tokens in EOS. To prevent multitudes of microtransactions trading a tiny amount of tokens to spam the blockchain, a minimum limit for the amount of tokens transferable or tradable in one transaction is enforced. Because Token-Exchange-Order transactions are not immediately charged transaction fees, i.e. fees are collected only when the buy/sell orders are matched, and the Cancel-Order transaction is fee free, malicious attackers can repeat Token-Exchange-Order and Cancel-Order transactions indefinitely to orchestrate a DoS attack without spending any tokens. To prevent this, the YOSEMITE Blockchain restricts the rate of the Cancel-Order transactions adaptively in proportion to the *dFIAT* holding of each account.

[5] Denial of service attack - https://en.wikipedia.org/wiki/Denial-of-service_attack

5 Proof-of-Transaction (PoT) Consensus Mechanism

5.1 Transaction-as-a-Vote (TaaV)

The key idea that makes Proof-of-Transaction a novel blockchain consensus mechanism is the concept of Transaction-as-a-Vote (TaaV). Transactions generated by the client side of the blockchain applications can optionally include a vote for a block producer candidate who can potentially participate or is already participating in the blockchain consensus process. In blockchain transaction messages which would incur some transaction fee, there is an optional "transaction vote" field where a blockchain account address can be specified as a vote. That means the entity generating the transaction on blockchain wants the blockchain core node having the voted address to be a block producer. The transaction message containing the vote for block producer is cryptographically signed by the private key of a blockchain account, so each transaction vote has its own cryptographic proof on blockchain.

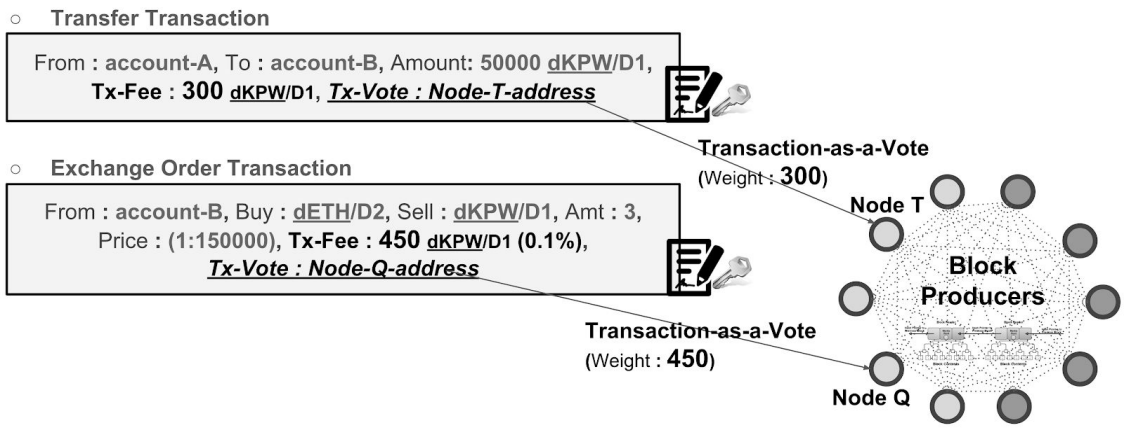

Figure 5.1 - Transaction-as-a-Vote examples

The blockchain core nodes who acquire the most votes from processed transactions will be elected as block producers that will cooperatively make new blocks and take rewards from blockchain. Not every transaction has the transaction vote field, only the transactions incurring transaction fees paid by blockchain users, i.e. transactions actually contributing to the blockchain itself, generating profit for blockchain operators including block producers. Each vote is not equally weighted, they are weighted in proportion to the transaction fee amount paid, the more transaction fee paid from the voted transaction, the more weighted votes are accumulated for the specified block producer. And the votes are only effective when the transaction fees are actually paid to the blockchain. The transaction votes of the open token exchange (buy/sell) orders unfilled yet are not tallied up as valid votes until the orders are actually executed. In the example in the Figure 5.1, the token transfer transaction incurring

transaction fee 300 dKPW/D1 with a transaction vote signed for the Node-T-address is 300-weighted vote to Node-T. The token exchange sell order transaction with a transaction vote signed for the Node-Q-address, which will incur 450 dKPW/D1 as transaction fee when the order is executed, is 450-weighted vote to Node-Q only effective when it's actually filled. If the order is cancelled by the user, it is not an effective vote.

In other blockchains, the voting process for blockchain governance and profit sharing are usually separate and explicit processes, where the blockchain users have to submit a separate, dedicated blockchain transaction in order to vote. Since most average users would not take the time to explicitly vote, especially if fees are incurred while doing so, voting rates are typically low in blockchain governance mechanisms. In EOS blockchain, the EOS token holders have to cast their votes explicitly to the delegated block producers[6]. In Stellar blockchain, the Lumens token holders have to designate a blockchain account address who will take a portion of the crypto-currency inflation[7]. But in the YOSEMITE Blockchain with TaaV, the voting process for blockchain governance and profit distribution is effectively integrated into the usual blockchain transaction processing, and blockchain users do not need to be bothered with explicit voting.

5.2 Proof-of-Transaction as Incentivization for Service Providers

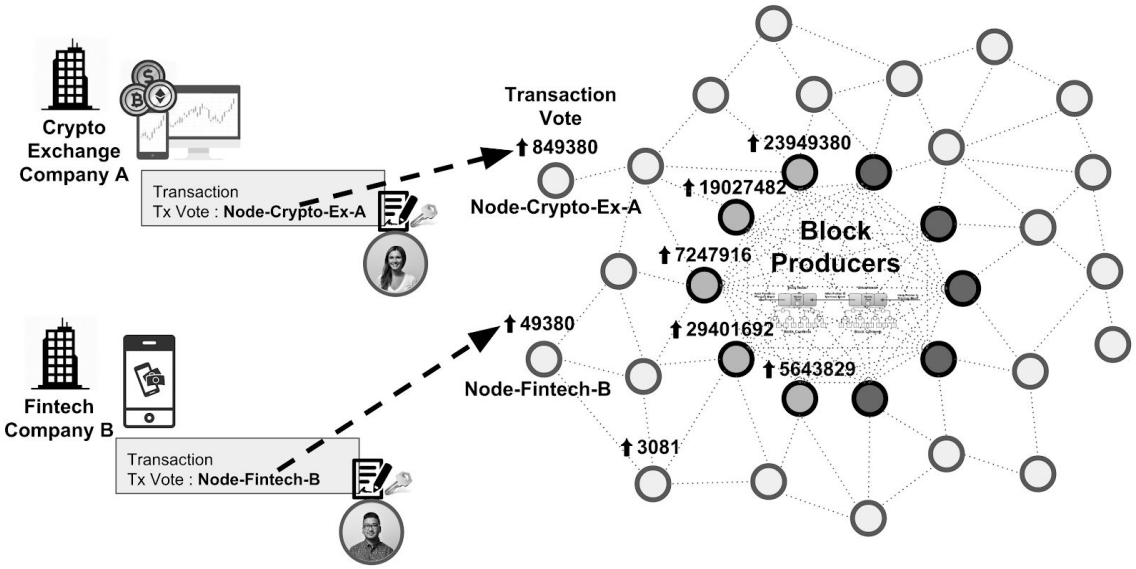

Figure 5.2 - Proof-of-Transaction as the incentivization for the blockchain-based service providers

The transaction votes for each blockchain core node (block producer candidate) are continuously accumulated as the newly-made transactions are processed on the blockchain. The

[6] EOS.IO Technical White Paper - Consensus Algorithm (DPOS) - https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md#consensus-algorithm-dpos
[7] Stellar Developers Guide - Inflation - https://www.stellar.org/developers/guides/concepts/inflation.html

amount of transaction votes acquired is solid proof of how much the blockchain account has produced meaningful blockchain transactions invigorating the economy of the blockchain. The accumulated vote amount is used as the key criteria for the block producer election in YOSEMITE Blockchain. Proof-of-Work (PoW) based blockchains incentivize the entities having a large hash power created from a huge amount of computation, which contributes nothing to the blockchain itself besides creating a competition for block production, and wastefully consumes massive amounts of electricity. Alternatively, Proof-of-Stake (PoS) based blockchains incentivise entities owning a large amount of the native crypto-currency. The validators or block producers of PoS, who already possess a lot of crypto-currency, will have more opportunities to earn newly-minted crypto-currencies generated as the block reward from the blockchain itself, essentially the-rich-get-richer. While both PoW and PoS incentivize the players who already have vested interests but do not directly contribute to the creation of the economic transactions, Proof-of-Transaction (PoT) incentivizes the blockchain-based service providers who can produce the tx-fee-revenue-generating transactions, directly contributing to the blockchain economy by creating real transactions, not just leveraging already vested computation power or financial wealth.

Though the blockchain transaction message must always be crypto-signed by the private key of the user's blockchain account, the transaction message itself is not written by human hands. Rather, the transaction voting field is encoded within the software developed for the specific blockchain application serviced to the user. So when the software implemented by the blockchain service provider creates blockchain transaction messages for application users, the account address of the blockchain core node being run by the service provider can be written in the vote field for every transaction generated from the blockchain application. In above example of Figure 5.2, the crypto exchange company A is providing its service built upon the YOSEMITE Blockchain. The crypto trading software built by the company A always inserts the company's own blockchain core node address (Node-Crypto-Ex-A) in the transaction vote field of every blockchain transaction message made for the user's sell/buy order. As the trading volume of the exchange service grows, the company A's node accumulates a significant amount of transaction votes that will qualify the node for the block producer election. The service providers, such as crypto exchanges, fintech companies, and so on, will compete in a transparent and fair way to get as many transaction votes as possible by providing useful services to the users.

5.3 Blockchain Consensus, Governance, Tx Fee Profit Distribution

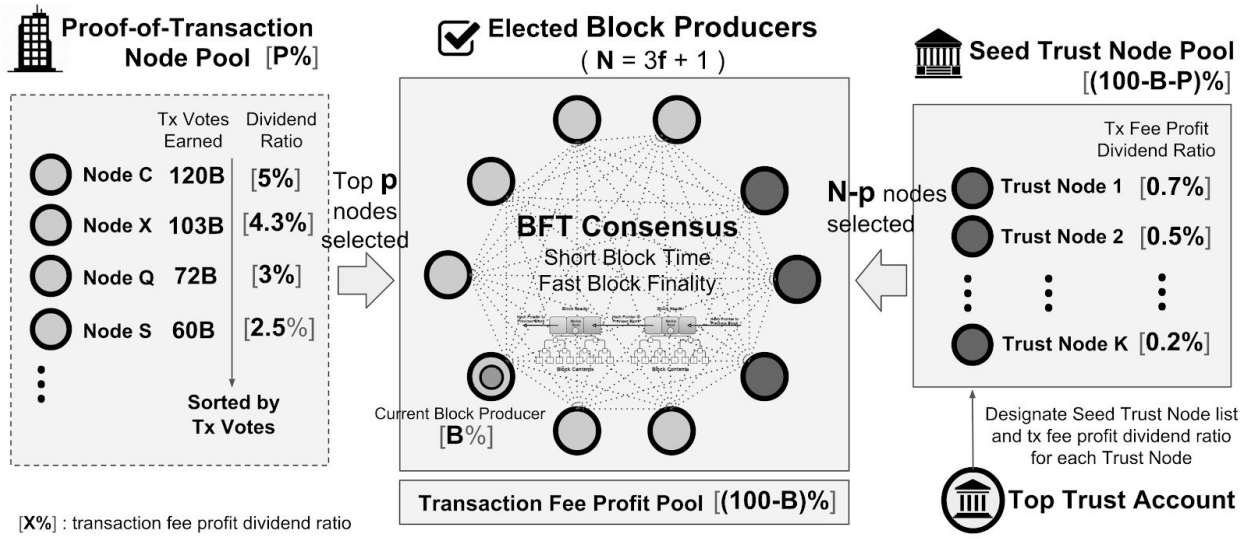

Figure 5.3 - Proof-of-Transaction based BFT blockchain consensus

5.3.1 Proof-of-Transaction (PoT) Node Pool

Proof-of-Transaction based blockchain consensus is designed as a new blockchain consensus mechanism for public blockchain like YOSEMITE Blockchain. Any entity can be elected as a block producer, and subsequently participate in blockchain consensus to make new blocks and collect profits, by earning sufficient transaction votes from blockchain users for whom the entity provides useful blockchain-based application services. The blockchain account addresses owned by the blockchain core nodes run by the service providers, which earn the relatively more amount of transaction votes are listed publicly in the Proof-of-Transaction Node Pool. The blockchain accounts in the PoT Node Pool are guaranteed to get a portion (dividend) of the transaction fee profits from the YOSEMITE Blockchain. The amount of user-signed transaction votes earned by each account is calculated by the elected block producers through BFT[8] (Byzantine Fault Tolerant)-based blockchain consensus in a secure and transparent manner, being utilized as the reliable and fair criteria to determine the beneficiaries of the blockchain system. The number of accounts in the PoT Node Pool is limited and there is a threshold amount of transaction votes to be earned for an account to be included in the PoT Node Pool. *P%* of the total transaction fee profits is allocated to the PoT Node Pool, among the *P%,* each account in the pool can claim its own profit in proportion to the transaction votes earned. In the example of Figure 5.3, the top rated Node C who earned *120 billion* points from weighted transaction votes can claim 5% of the transaction fee profits generated from a time window. The top nodes in PoT Node Pool also have the right to be elected to be block producers to make new blocks and earn the additional block reward profit.

[8] Byzantine fault tolerance - https://en.wikipedia.org/wiki/Byzantine_fault_tolerance

5.3.2 Seed Trust Node Pool

Though it is possible to run blockchain consensus with only the public nodes in PoT Node Pool, the blockchain could be vulnerable when there are none or only a very small amount of transactions occurring in the network. In that situation, there will be a higher probability for the PoT nodes to be Byzantine, i.e. to act maliciously to destroy or take advantage of the blockchain, as opposed to healthy conditions where multitudes of blockchain transactions are generated. Seed Trust Nodes running honest nodes even in a no-transaction situation is very helpful for the stability and reliability of the blockchain. In the YOSEMITE Blockchain, trusted Depositories providing *dFIAT*, *dCRYPTO*, and *dASSET* tokens is the crucial part of the blockchain ecosystem. It will create a virtuous cycle on the blockchain for the Depositories to run the Seed Trust Nodes always running their blockchain core nodes to maintain the blockchain stably. The trusted Depositories are highly incentivized to run Seed Trust Nodes full time, if they are guaranteed a portion of transaction fee profits (relatively smaller portion than the PoT Node Pool's share, see 5.3.4 tx fee profit distribution), and blockchain users can be assured of the stability and security of the chain given these nodes' participation. There exists a Top Trust Account in the YOSEMITE Blockchain who has the right to designate the blockchain accounts list in the Seed Trust Node Pool and the transaction fee profit dividend ratio for each appointed Seed Trust Node. The Top Trust Account must be owned by an entity having a very high level of trust within the YOSEMITE Blockchain ecosystem, such as a trusted financial institution or government organization. Although it is not always required for the Seed Trust Nodes to be run by the Depositories, it is desirable for the Depositories to be designated as the Seed Trust Nodes. While the Top Trust Account has the special right to appoint Seed Trust Nodes, all actions of the Top Trust Account are transparent and immutable in the blockchain, monitored by everyone in the blockchain ecosystem.

5.3.3 Election of Block Producers for BFT Consensus

The critical element of blockchain design which enables scalability, i.e. a high capacity to make more blockchain TPS (transactions per second), is whether the predefined number of consensus participants (i.e. validators, block producers) exists. There is no predefined set in PoW-based consensus (e.g. Bitcoin, Ethereum) where any node able to competitively find the solution of the hash puzzle for the new block can be a block producer. Neither does the FBA (Federated Byzantine Agreement) consensus with the 'quorum-slice' concept used in Stellar Consensus Protocol[9], in which the quorum set participating in the consensus could be arbitrarily large as the quorum-slices of the consensus nodes expand. In that situation, high TPS is not guaranteed in the Stellar network. In practical setup, a blockchain with FBA consensus is managed by a small, fixed set of authority nodes constituting the consensus quorum to achieve high TPS, but that in fact results in an effectively permissioned blockchain, in which new users have no direct

[9] D. MAZIERES, Stellar Consensus Protocol - https://www.stellar.org/papers/stellar-consensus-protocol.pdf , 2015

incentive to run a blockchain node due to lack of a guaranteed block reward and low probability of inclusion in the top tier quorum to participate in blockchain consensus. Whereas in the BFT-based consensus algorithms like PBFT[10] (Practical Byzantine Fault Tolerance), Tendermint [11], and DPoS[12] (Delegated PoS) of Steem/BitShares/EOS, there is a predefined number of elected consensus participants (i.e. validators or block producers) which leads to high TPS because the elected set of nodes can cooperatively make fast consensus for the new block creation with the agreement that the new blocks made through the consensus of the elected nodes are authoritative. The YOSEMITE Blockchain adopts the optimized modification of BFT-based consensus algorithms (5.3.5) to achieve short block time (inspired from DPoS of Steem/BitShares/EOS) and fast 100% block finality (inspired from Tendermint), with the unique block-producer-election mechanism using the Transaction-as-a-Vote and Proof-of-Transaction.

Block producers participating in the consensus protocol to generate new blocks in the YOSEMITE Blockchain are elected from the PoT Node Pool and the Seed Trust Node Pool. Let N represent the number of the block producers. The top p nodes sorted by the earned transaction vote amount are selected from the PoT Node Pool as block producers in each round. The remaining N-p nodes are pseudo-randomly (hard to predict but deterministically selected by the protocol) selected from the Seed Trust Node Pool. The numbers N and p are fixed values in the YOSEMITE Blockchain. The number p is chosen to be more than majority to give weight to the PoT nodes. Among the N nodes periodically re-elected from the two pool, the BFT-based consensus protocol is executed to generate new blocks.

For each new block, a portion of the total transaction fee amount collected from the new block is given as a block reward to each block producer who creates each block. Although the accounts receiving transaction votes are not necessarily forced to run blockchain core nodes, i.e. run a physical server, the block reward allotted to elected block producers strongly incentivizes the PoT nodes to run core nodes and participate in blockchain consensus. If a PoT Node account elected as a block producer by receiving a significant amount of transaction votes does not run the physical core node server or an elected core node malfunctions or acts maliciously as a Byzantine node, the account is penalized by slashing the already earned transaction votes, forfeiting the account's accumulated portion of the transaction fee profit pool, and depriving of the block producer position. If the number of the elected block producers is $N = 3f + 1$, up to f Byzantine nodes are tolerable in BFT-based consensus. Compared to the other public blockchains with BFT-based consensus, the probability that a node elected as a block producer in the YOSEMITE Blockchain is a Byzantine node can be regarded as very low because every elected block producer is either a PoT Node making profit by doing the blockchain-based service business seriously or a Seed Trust Node trusted by the ecosystem.

[10] M. Castro, B. Liskov - Practical Byzantine Fault Tolerance and Proactive Recovery - http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf , 2002
[11] Jae Kwon - Tendermint : Consensus without Mining - https://tendermint.com/static/docs/tendermint.pdf , 2014
[12] D. Larimer - BitShares - Delegated Proof-of-Stake Consensus - https://bitshares.org/technology/delegated-proof-of-stake-consensus , 2014

5.3.4 Transaction Fee Profit Distribution

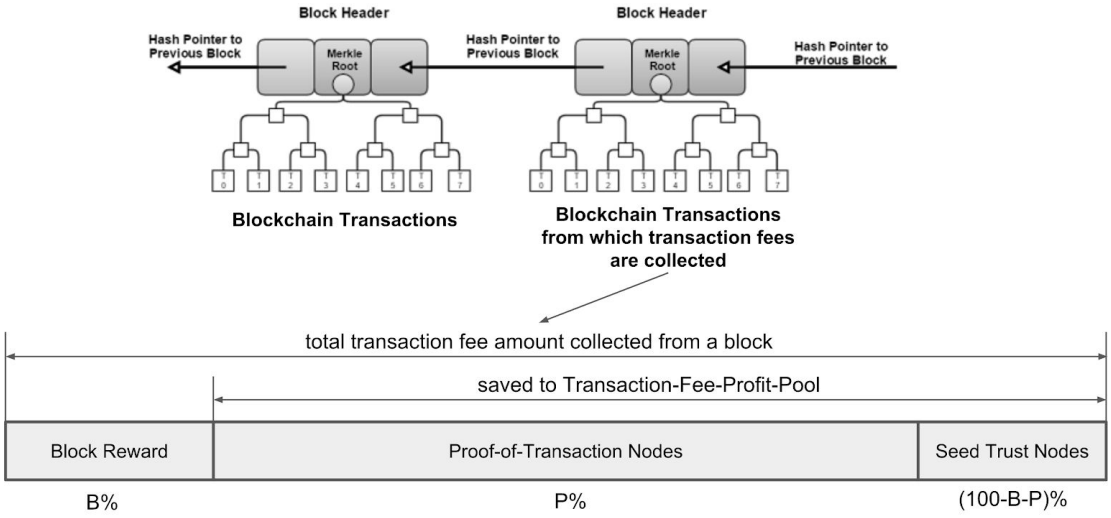

Figure 5.4 - Transaction fee profit distribution

For each new block, the total transaction fee amount collected from the transactions included in the block is distributed to the block producer, PoT Nodes, and Seed Trust Nodes. *B%* of the collected transaction fees is immediately allocated to the block producer as a block reward. The remaining *(100-B)%* is saved to the Transaction Fee Profit Pool with *P%* allocated to the PoT Node Pool and *(100-B-P)%* allocated to the Seed Trust Node Pool. Each account listed in PoT Node Pool can regularly claim its own profit in proportion to its transaction vote amount at the time of transaction fee collections. In the same way, each account in the Seed Trust Node Pool can claim its own profit in proportion to the dividend ratio designated by the Top Trust Account. The percentages *B*, *P* are fixed in the blockchain at each protocol upgrade, and *P* should be over the majority portion to give weight to the PoT nodes.

5.3.5 YOSEMITE BFT Consensus with Short Block Time and Fast Block Finality

The high speed and high transaction throughput processing capacity of a blockchain is a key factor for the next generation scalable blockchains. The short block time (time interval between consecutive block creations) and the fast block finality (time required for the new block to be immutable, guaranteeing no fork up to the block) are the crucial properties of a scalable blockchain.

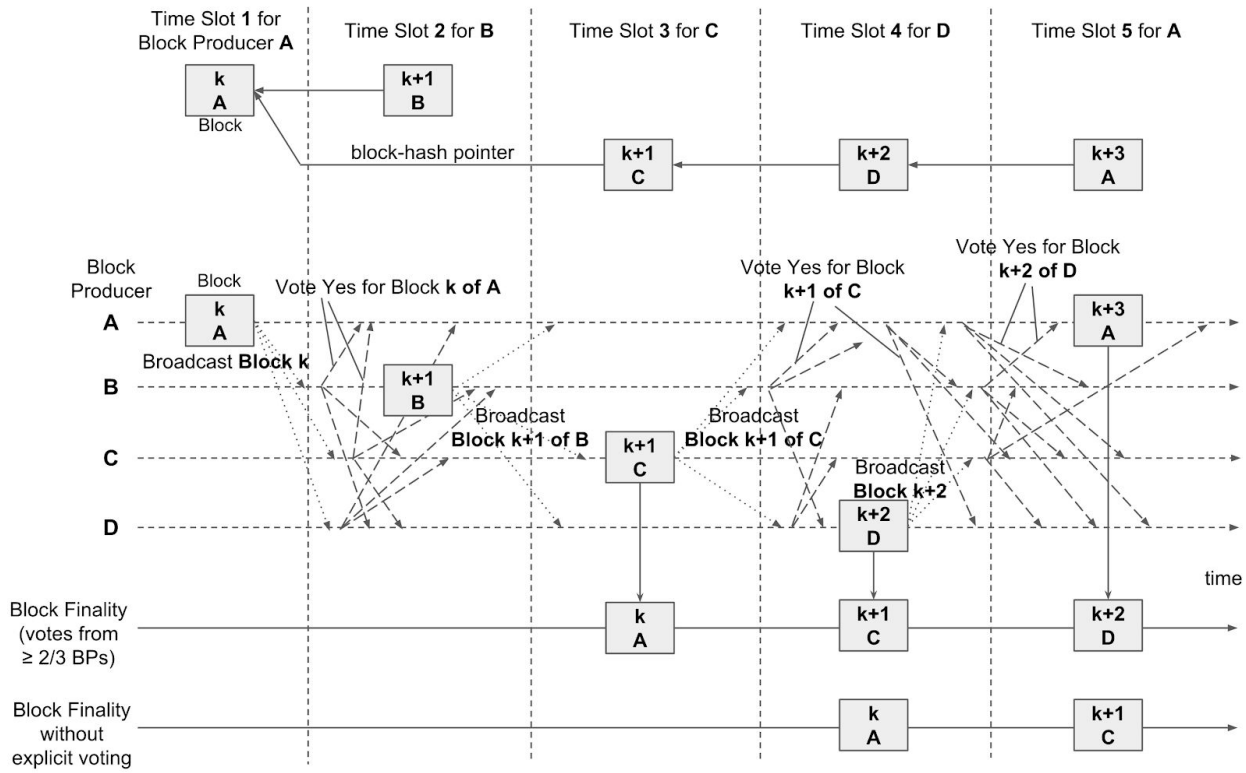

Figure 5.5 - BFT consensus protocol among the elected block producers

The short block time can be achieved by electing a fixed number of block producers to cooperate (not compete) to produce blocks, letting each block producer make a new block in its pre-allocated time slot and immediately progressing to the next block production turn without waiting to gather votes for the validity of the new block from more than ⅔ of the elected block producers. We call this mechanism "Optimistic-Block-Production". The last broadcasted block, created in the previous time slot allocated to the last block producer, is optimistically trusted as a valid block if the current block producer has verified the validity of the block, regardless of the final confirmation from a ⅔ majority of the elected block producers. However, if the next block producers do not agree about the validity of a block, the newly created block will contain the block-hash pointer of the last valid block, skipping over any invalid blocks. In the example of Figure 5.5, The block made by block producer B which is a Byzantine node (malicious attacker or having network problems) is skipped by the other block producers. There can be temporal forks of the blockchain, but eventually the longest fork will survive as the canonical chain. A block producer should not sign more than one temporary fork. If a single block producer's signatures are detected on multiple forks of the chain, the Byzantine block producer will be penalized. Remember up to f Byzantine nodes are tolerable when the number of the block producers is $N = 3f + 1$. The Tendermint consensus algorithm and its variants can be regarded as Pessimistic-Block-Production style which lead to relatively long block time because block-producing nodes must wait to receive voting messages from the majority of consensus participants for the confirmation of the block validity to continue to the next block production stage.

Fast block finality can be achieved through explicit block validity voting among elected block producers. Without block validity voting, block finality can still be achieved, though the time delay of block finality is somewhat long. The block finality of a block means that the block and all connected previous blocks are confirmed as immutable and only the next blocks after the finalized blocks have non-zero probability that they will belong to a temporary fork and eventually be excluded from the canonical chain. The block-hash pointer to the previous block included in the new block data is effectively regarded as a vote of the block producer for the validity of all the previous blocks. If the block-producer-majority number of blocks are attached after a block in a blockchain, it means that the block has received the majority number of votes for block validity from the block producers. Let the block number of a block be k and the number of the elected block producers be $N = 3f + 1$ where up to f Byzantines are tolerant. When the block with block number $k+(2f+1)-1$ is broadcasted, the block k will earn block finality status supported by a ⅔ majority of the block producers. Fast block finality is crucial for inter-blockchain communication because only the transactions in finalized blocks can be referenced in the external blockchains or the internal sibling chains of a blockchain (for the multi-chain architecture). The minimum block finality time without explicit voting is $2f*t$ where t is block time. If $N=25$, $t=3$ second then block finality time is 48 seconds, which is inappropriate for smooth inter-blockchain communication. The YOSEMITE Blockchain accelerates the block finality time through explicit block validity voting, independently of the block production progress, with the trade-off of higher network communication cost. When a block producer receives a newly broadcasted block from another block producer, the new block is validated and a validity vote for the block is broadcasted to all block producers. When a block producer creates a new block in its time slot, if the producer has gathered enough block validity votes for a previous block from the ⅔ majority of the block producers, the block finality of the previous block is declared in the new block. A further optimization for block validity voting is also designed in the protocol to accelerate the voting message propagation. The provable summary data of the block validity votes received from other block producers are also included in the new block message and the validity vote message being broadcasted. The example in Figure 5.5 shows that the block finality with the block validity voting is faster than the one without explicit voting. For larger numbers of block producers N, the resulting time difference is far more. Block validity voting enables block finality time near the block time (usually 1 or 2 block time).

6 Blockchain Accounts

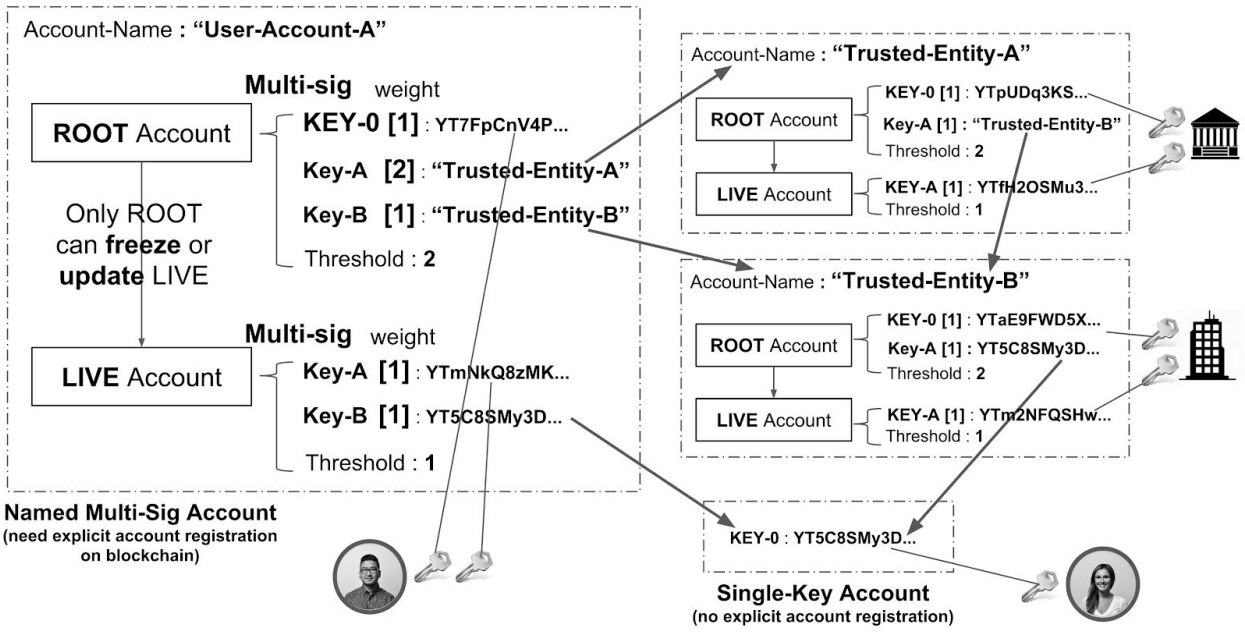

Figure 6.1 - Blockchain account scheme of YOSEMITE Blockchain

6.1 Named-Multi-Sig / Single-Key Blockchain Accounts

The YOSEMITE Blockchain natively supports named multi-sig[13] blockchain accounts. A blockchain account used in the YOSEMITE Blockchain consists of a *ROOT* account and *LIVE* account pair. Every usual blockchain transaction includes the crypto-signature of the *LIVE* account that should be validated by the block producers. The *LIVE* account can be freezed or updated on the blockchain only by the *ROOT* account when the *LIVE* account is found to be compromised. The *ROOT* and *LIVE* account themselves are multi-sig accounts, each having multiple weighted keys and threshold value. To make a valid transaction message signed by a multi-sig account, the transaction message needs to include valid signatures from the multi-sig keys with the sum of key weights over the threshold value. In the example of Figure 6.1, for the *ROOT* account of *"User-Account-A"* with threshold value of 2, a signature combination of *(KEY-0, Key-A) [weight sum : 3]* or *(KEY-0, Key-B) [weight sum : 2]*, or a single signature of *Key-A [weight : 2]* is required to make a valid transaction signature. Recursively, to get a valid signature of *Key-A* referencing to the *"Trusted-Entity-A"* blockchain account, the valid multi-signatures of enough weighted keys from the *"LIVE"* account of *"Trusted-Entity-A"* must be collected. A blockchain account can have a human-readable alphanumeric identifier (name).

[13] Multi-signature - https://en.wikipedia.org/wiki/Multisignature

The public key address of the *ROOT* account's default key (*KEY-0*) can be used as a account identifier alternatively. A Single-Key account with only one public/private key pair can also be used as an independent blockchain account in the YOSEMITE Blockchain, using the same key for both the *ROOT* and *LIVE* account without the multi-sig scheme. A Single-Key account can be created implicitly in the client side offline from the blockchain. Whereas, a Named Multi-Sig account must be registered on the blockchain, with the selected account name, the weighted multi-sig keys and the threshold value, by a explicit blockchain account creation transaction which is charged some transaction fee in *dFIAT* to prevent account creation spamming attacks.

6.2 Trust Network for Account Recovery

Because the *LIVE* account can be replaced by the *ROOT* account, when the blockchain keys are lost or compromised by malicious attackers, the *LIVE* account used to make blockchain transactions in normal situations can be recovered. Even in the case that the default key (*KEY-0*) of the *ROOT* account is lost, the *LIVE* account can be recovered with the help of a single or multiple trusted entities which the account owner registered as key recovery partners in his/her multi-sig setup. The trusted key recovery partner should require the KYC/AML[14] authentication process to be done by the blockchain user. Recursively, the blockchain account of the trusted key recovery partner also can be recovered by its own chosen trusted partners, and so on. These links form the Trust Network of Blockchain Account Recovery in the YOSEMITE Blockchain. Figure 6.1 shows an example of a Trust Network built by the *"User-Account-A"*, *"Trust-Entity-A"*, *"Trust-Entity-B"* and a Single-Key account. The Trust Network makes the blockchain ecosystem solid and stable, highly mitigating the vulnerability of blockchain key loss.

6.3 KYC/AML Compliance and Account Anonymity

Tokens issued by Depositories in the YOSEMITE Blockchain can be configured to be held, transferred, and traded only by blockchain accounts that have already gone through the KYC/AML process provided by trusted entities. Information about whether a blockchain account has undergone the KYC/AML process and through what organization is published on the YOSEMITE Blockchain transparently, but the personal information gathered from users is privately processed and maintained by the trusted entities. The integrated KYC/AML support by the YOSEMITE Blockchain will be a great help to regulatory compliance issues faced by existing blockchain systems.

Since any number of blockchain accounts can be created anonymously and the personal identity authentication information gathered through the KYC/AML process are privately handled by the trusted entities, basic account anonymity can be achieved, while the transactions generated by blockchain accounts are transparent in the blockchain. However, once the owner of a blockchain account is known (e.g. someone receives tokens from his/her friend), the account anonymity is

[14] Know Your Customer / Anti Money Laundering - https://en.wikipedia.org/wiki/Know_your_customer

compromised. To maintain account anonymity, trusted entities like financial companies can build their own systems to manage blockchain accounts on behalf of their customers. A financial company would provide blockchain account mapping services operated under its trusted public internet domain, e.g. a web service operated under the url *https://fintechX.com/YSMT,* which maps a company-specific user account address such as *user-account-1234#fintechX.com* to an anonymous blockchain account managed by the financial company. The customers of financial company providing blockchain-based financial services can use the account ids issued by company as usual bank accounts, and through the blockchain account mapping services the actual blockchain transactions can be processed anonymously. It is possible for a company to manage only one YOSEMITE Blockchain account serving all its customers using the memo field in blockchain transaction message to distinguish its customers, with its private customer ledger running on its backend system. Alternatively, a company can manage multitudes of blockchain accounts, whose private keys are securely held in its internal system on behalf of its customers, which are anonymously mapped to its customers and regularly shuffled to maintain account anonymity of the blockchain transactions. YOSEMITE will provide standard protocols and open-sourced basic building block components for developers to implement KYC/AML integrated financial services built upon the YOSEMITE Blockchain.

7 Decentralized Issuance of *dFIAT* without Fiat Reserve

YOSEMITE blockchain users can receive an issuance of *dFIAT* by escrowing their *dCRYPTO* or *dASSET* tokens. At a later time, the user can redeem *dCRYPTO*/*dASSET* tokens by returning the corresponding amount of *dFIAT*. The issued amount of *dFIAT* is always less than the *dFIAT* price of escrowed tokens by some margin. The exact rates and ratio of issuance will largely be determined by the historical performance of the *dCRYPTO*/*dASSET* token being escrowed. A very similar decentralized stable coin (bitUSD) implemented by BitShares[15] has proven to closely hold parity with USD. Stable coin issuance via *dCRYPTO*/*dASSET* tokens is beneficial to the YOSEMITE Blockchain ecosystem because this style of issuance relies exclusively on crypto-token-assets held on the blockchain without the need for a centralized reserve of fiat funds.

$$dFIAT_{ASSET\text{-}BACKED} < \sum_{i=1}^{n} (A_i \times P_i)$$

where $dFIAT_{ASSET\text{-}BACKED}$: the total value of *dFIAT* issued via escrowing *dCRYPTO*/*dASSET* tokens ,
n : the number of *dCRYPTO*/*dASSET* escrows locked for *dFIAT* issuance ,
$\mathbf{A_i}$: the amount of each *dCRYPTO*/*dASSET* token escrowed ,
$\mathbf{P_i}$: the current *dFIAT* price (changing over time) of each *dCRYPTO*/*dASSET* token escrowed

[15] D. Larimer, C. Hoskinson S. Larimer - BitShares White Paper - https://www.scribd.com/document/173481633/BitShares-White-Paper

The total value of *dFIAT* issued from escrowing *dCRYPTO*/*dASSET* tokens must always remain strictly less than the sum of the total value of all escrowed *dCRYPTO*/*dASSET* tokens at current prices in *dFIAT*. To ensure this equation always holds, the blockchain will execute a margin call style operation, liquidating *dCRYPTO*/*dASSET* into the market on the YOSEMITE Blockchain, at a price strictly higher than the total value of *dFIAT* issued from escrowing *dCRYPTO*/*dASSET* tokens at the time. (The elected block producers of YOSEMITE Blockchain automatically execute sell orders for the escrowed *dCRYPTO*/*dASSET* tokens according to the predefined protocol) Among the liquidated *dFIAT* tokens, the same amount of the issued *dFIAT* tokens when the liquidated *dCRYPTO*/*dASSET* tokens are escrowed, are burned in the blockchain, and the remaining *dFIAT* tokens are returned to the blockchain account who originally escrowed *dCRYPTO*/*dASSET* tokens excluding the fee amount saved to the Transaction Fee Profit Pool.

$$dFIAT_{AB} = \sum dFIAT^{i}_{AB} = \sum (A_i \times P_i^E \times r_i) < \sum (A_i \times P_i^E \times m_i) \leq \sum (A_i \times P_i)$$

if the token price drops below the maintenance margin, $P_i < P_i^E \times m_i$*, the blockchain automatically liquidates(sells) the escrowed dCRYPTO/dASSET* (A_i) *and the* $dFIAT^{i}_{ASTB}$ *is burned*

where ***AB*** *: ASSET-BACKED ,* $\boldsymbol{dFIAT^{i}_{AB}}$ *: the amount of dFIAT issued via each dCRYPTO/dASSET escrow,*
$\boldsymbol{P_i^E}$: the *dFIAT* price of an *dCRYPTO*/*dASSET* when it is being escrowed ,
$\boldsymbol{r_i}$ *: the rate at which dFIAT is issued based on the price* P_i^E *,* $\boldsymbol{m_i}$ *: the maintenance margin rate,* $\boldsymbol{0 < r_i < m_i < 1}$

The YOSEMITE Blockchain provides a hybrid-style stable coin model supporting both reserve-backed and token-backed pegging methods.

$$\text{Total supply of } dFIAT = dFIAT_{RESERVE\text{-}BACKED} + dFIAT_{ASSET\text{-}BACKED}$$

The total supply of *dFIAT* tokens in circulation is the sum of *dFIAT* tokens backed by fiat fund reserves held by the Depositories and *dFIAT* tokens backed by *dCRYPTO*/*dASSET* escrows.

8 Scalability of YOSEMITE Blockchain

8.1 Single Chain Scalability

The single chain scalability of the YOSEMITE blockchain depends mainly on the consensus mechanism, namely, a novel PoT-based BFT consensus with short block time and fast block finality. With the Optimistic-Block-Production and the optimized block validity voting protocol, high speed and high throughput on-blockchain transaction processing, ranging from thousands to tens of thousands transactions per second with 1~3 seconds block time, can be realized. In the unique setup of the YOSEMITE Blockchain consensus, the service providers acting as PoT Nodes and the trusted institutions acting as Seed Trust Nodes will be elected to become block producers running full core node servers. They are expected to provide high performance computing powers efficiently and securely to the blockchain ecosystem, handling very large volume of transactions. The probability for the nodes run by the service providers and trusted entities to be Byzantine is very low, and there is more room to reduce the number of elected block producers compared to the usual public blockchain environment. Single chain scalability is the foundation of extended scalability, like off-chain state channels, on/off-chain hybrid exchange architecture and the ultimate multi-blockchain architecture with fast inter-blockchain communication.

8.2 Extended Scalability with On/Off-chain Hybrid Exchange Technology

Though the single chain throughput facilitated by the YOSEMITE Blockchain is enough for most blockchain service applications, including on-blockchain decentralized exchanges, for exceptional cases like high frequency trading or micropayments, YOSEMITE has already provided on/off-chain hybrid exchange technology. Some trading pairs needing high volume and high frequency trading can be serviced using the existing YOSEMITE hybrid architecture. In this hybrid architecture, only 'deposit to exchange' and 'withdrawal from exchange' transactions are on-blockchain. All buy/sell order messages crypto-signed by YOSEMITE Blockchain user accounts are submitted to the off-blockchain exchange servers which match the signed buy/sell orders and publish the trade transactions signed by the off-chain server's account through the distributed P2P storage IPFS[16] in a transparent and immutable manner, regularly anchoring the cryptographic proof of recent transactions handled in off-blockchain servers to the blockchain. When a user requests the withdrawal of the tokens, the verified cryptographic proof of the whole history of the off-chain trading transactions and the current token balances for the user is also recorded in the on-blockchain withdrawal transaction. This prevents the external off-chain exchange servers from manipulating the trading event, and makes the hybrid system fully auditable to any external parties and fully restorable even in the event of the off-chain exchange

[16] Juan Benet, IPFS - Content Addressed, Versioned, P2P File System
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf

server failure. Off-chain payment channels enabling high-frequency micropayments can also be implemented in a similar way using the YOSEMITE hybrid technology.

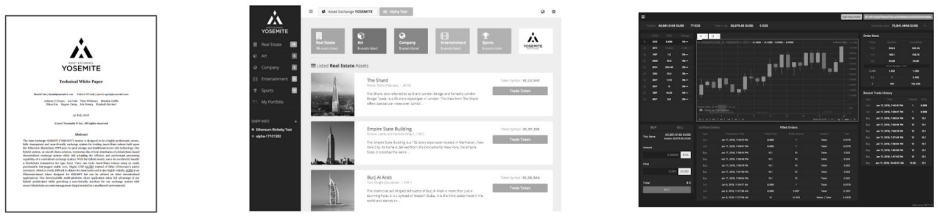

Figure 8.1 - YOSEMITE hybrid exchange technology, Technical White Paper and asset/crypto exchange alpha version.

The technical white paper[17] and the working alpha system[18] of the YOSEMITE hybrid exchange technology were published in mid 2017. The working alpha versions of asset/crypto exchange system in Figure 8.1 were developed based on the Ethereum blockchain, but the hybrid technology can be implemented on any other blockchains including the YOSEMITE Blockchain.

8.3 Scalable Multi-Blockchain Architecture

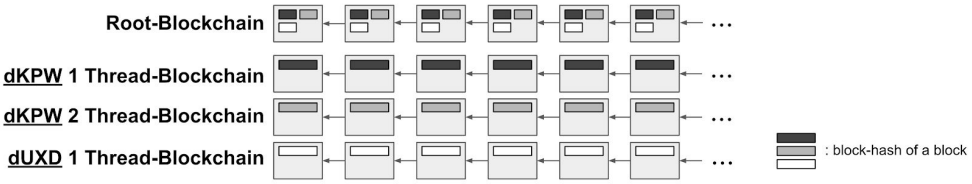

Figure 8.2 - Scalable multi-blockchain architecture with tightly coupled inter-blockchain communication

With the well-designed single chain scalability characterized by fast block finality and tightly-coupled inter-blockchain communication protocol, a scalable multi-blockchain architecture can be implemented. The scalable multi-blockchain architecture is planned to be implemented in a future upgrade of the YOSEMITE Blockchain. There will be a single Root-Blockchain in each YOSEMITE Blockchain whose blocks contains the recent block-hashes of the blocks having block finality status from the multiple Thread-Blockchains running in the same YOSEMITE Blockchain. The Root-Blockchain operated by its own block producers acts as the inter-blockchain communication hub between the Thread-Blockchains. A Thread-Blockchain is a blockchain with its own transaction types, native *dFIAT* tokens used as basic currency token in that chain, and its own blockchain consensus run by independent block producers. With

[17] YOSEMITE On/Off-Blockchain Hybrid Exchange System Tecnical White Paper, 2017
https://yosemitex.com/documents/YOSEMITE_Hybrid_Exchange_Technical_White_Paper_20170731a.pdf
[18] YOSEMITE Asset Exchange alpha (http://alpha.yosemitex.com) and Crypto Exchange alpha (http://crypto-alpha.yosemitex.com) hybrid exchange system built upon Ethereum

multiple Thread-Blockchains in a YOSEMITE Blockchain, each with a large capacity for transactions, a very high level of blockchain scalability can be achieved.

9 Smart Contract Platform

The YOSEMITE Blockchain, basically designed as a decentralized exchange platform, provides tokenization and token-trading operations as built-in blockchain transaction types, so that useful killer applications like crypto exchanges can be developed on the YOSEMITE Blockchain without utilizing smart contract technology provided by the blockchain. To support customized blockchain transactions designed by developers building their Dapp (Decentralized Application) on top of the YOSEMITE Blockchain, smart contract execution will be provided in a future upgrade of the YOSEMITE Blockchain. Instead of developing a custom-designed virtual machine and smart contract programming language such as the EVM[19] (Ethereum Virtual Machine) and Solidity[20], the YOSEMITE Blockchain adopts WebAssembly[21] (WASM) technology which was originally developed as the open web standard for the next generation of web-browser-side application runtime environments. WASM, due to its fast and safe VM, has great potential to replace Javascript, currently the only de-facto standard in web programming. The EOS blockchain also adopted WASM as its smart contracts execution technology. Currently, developers can use C/C++/Rust programming languages to produce secure and high performance smart contract codes compiled to WASM binary. DoS (Denial of Service) attacks consuming resources such as computing power and storage of the blockchain must be prevented. The operations callable from the WASM codes modifying the blockchain state (e.g. token operations, storage operations) will charge a transaction fee paid in ***dFIAT***. The YOSEMITE Blockchain also restricts the execution time of a smart contract execution transaction in proportion to the ***dFIAT*** holding of the blockchain account who initiated the smart contract execution. The smart contract platform with a fiat-pegged stable coin as the native crypto-currency will have a huge impact on practical blockchain-based application development, attracting existing financial institutions and fintech startups to utilize the YOSEMITE blockchain.

[19] G. Wood, Ethereum Yellow Paper - https://ethereum.github.io/yellowpaper/paper.pdf
[20] Solidity Programming Language official documentation - https://solidity.readthedocs.io
[21] WebAssembly official website - http://webassembly.org