USPTO Provisional Patent Application Number : 62/646,930 62/797,648

InfraBlockchain

Scalable enterprise blockchain technology that combines the strengths of a private and a public blockchain

No Native Cryptocurrency

programmable fiat-pegged stable tokens
(e.g. USD, KRW, CNY) as base currencies used for transaction fee

Proof-of-Transaction (PoT)

reasonable and fair blockchain consensus mechanism
incentivizing blockchain service providers

General Financial Platform

smart-contract based blockchain system designed for enterprise uses

Optional On-Chain Privacy Tech.

privacy-protecting transactions applicable for small amount money transfer (like cash) and blockchain-based full privacy voting system

Technical White Paper

Feb. 2018 (v1) / Jan. 2019 (v2) / Aug. 2020 (v2.4)

InfraBlockchain is rebranded from YOSEMITE Blockchain

Abstract

InfraBlockchain provides innovative blockchain system architecture overcoming the obstacles of private and public blockchains which prevent enterprises and public institutions from utilizing the full potential of blockchain technology. Public blockchains having their native cryptocurrencies (e.g. BTC, ETH, EOS) cannot be adopted by enterprises/public-institutions due to the regulatory uncertainty, extreme volatility and unfair distribution of cryptocurrencies. Private/permissioned blockchain systems (e.g. Hyperledger Fabric, Corda, Quorum) applied to existing enterprise systems are very likely to be nothing but an inefficient high-cost distributed database providing system auditability.

InfraBlockchain introduces a new method of enterprise-oriented public/permissioned blockchain system design without issuing a native cryptocurrency minted by the blockchain itself. Any entities can issue their own tokens (e.g. digital USD fiat-pegged stable tokens backed by an equivalent fiat money reserve, asset-backed security tokens, …) using the built-in *InfraBlockchain Standard Token* model ensuring the token interoperability. The elected block producers can select some user-created tokens like fiat-pegged stable tokens issued by trusted entities as the *Transaction Fee Tokens* to be used as a fee for executing blockchain transactions. The block producers of the *InfraBlockchain* are elected by a unique consensus mechanism, the *Proof-of-Transaction* (PoT) implemented by the *Transaction-as-a-Vote* (TaaV), which incentivizes the application service providers, who are directly contributing to the blockchain ecosystem by generating blockchain transactions associated with real economic activity, to be elected as block producers. The *InfraBlockchain* is designed to be a smart contract based general financial platform providing the fiat-pegged stable tokens as base currencies which are programmable on custom smart contracts to meet the business needs, the delegable transaction fee payments, the built-in on-chain token exchange, the blockchain account recovery, the integrated KYC/AML support meeting the regulatory compliance and the enterprise level blockchain scalability enabled by the PoT-based BFT consensus with short block time and fast block finality, off-chain state-channel exchange technology and multi-blockchain (network of sister chains) architecture. Optional privacy-protecting on-chain transaction features leveraging privacy token technology (e.g. one-time stealth address, group sig, zkp) are supported to enable privacy-protecting blockchain services like cash-like private token transaction and full privacy-protecting voting service.

Table of Contents

1 Blockchain Design Without Native Cryptocurrency

The most common economic model for public blockchains holds that there should be a native cryptocurrency which is pre-minted through an ICO presale process and/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], Ethereum Casper, ...), 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 cryptocurrency holders cast weighted votes in proportion to their currency holdings or stake their crypto tokens to have more influence over blockchain governance.

The native cryptocurrency in a blockchain serves as the basic incentive system underlying the coordination mechanism among the stakeholders of that blockchain ecosystem (developers, investors, block producers, service providers, end users) and is typically used as the basic building block for blockchain system design, despite how native crypto-currencies have created serious obstacles to adoption in existing blockchain ecosystems. A public blockchain's native crypto-currencies, traded in public exchanges, are speculative assets which are constantly involved in pump-and-dump schemes, making the native crypto-currencies highly volatile in price. For ordinary people who are accustomed to stable fiat-currency like USD, it is uncomfortable and impractical to use unstable cryptocurrency 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 cryptocurrency by selling their fiat money through an external crypto exchange. This is the main obstacle to mass adoption of blockchain-based applications, aside from the scalability issue. Additionally, the financial benefits gained from these speculative crypto-currencies are unfairly concentrated among blockchain developers and early stage investors, who maintain large shares of cryptocurrency after ICOs. Meanwhile, those who seek to adopt the blockchain later, even if they are the service providers who are directly contributing value to the blockchain ecosystem by making applications generating meaningful transactions, are unfairly disadvantaged. In the same manner, blockchain governance power is also unfairly concentrated in the hands of a few large token holders, resulting in centralization of power and poor governance, where decision making power is not aligned with the best interests of most of the system participants nor with the parties and interests generating the most value. Moreover, it is impractical to attempt a

[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

simple fix to this problem by having a large proportion of blockchain users participate in an explicit voting process to democratically control blockchain governance (e.g. voting for electing block producers). The typical user is not nearly well-informed enough or engaged enough to implement sound governance by this mechanism.[5]

No Native Cryptocurrency	*InfraBlockchain* Standard Token Model	Fiat-Pegged Stable Tokens Asset-Backed Tokens	Transaction Fee Tokens Selected from User-Created Tokens
Proof-of-Transaction (PoT) Consensus Mechanism	Smart Contract Enabled General Financial Platform	Integrated KYC/AML Support Account Recovery	Scalable Blockchain Architecture

Figure 1.1 - Major Features of *InfraBlockchain*

In this paper, we introduce a new method of public/permissioned blockchain design that avoids issuing native cryptocurrency minted by the blockchain itself. The *InfraBlockchain* provides a unique *InfraBlockchain Standard Token* model. Instead of giving a distinguished cryptocurrency the special role of underpinning the incentives in the system, every account in the *InfraBlockchain* is inherently a built-in standard token issued and circulated freely by any blockchain account owner. There is no distinguished special token. Only user-created tokens exist in the *InfraBlockchain*. Among the user-issued tokens, the elected block producers can select some tokens to be used for blockchain transaction fee payment, whereas typically a pre-built native cryptocurrency is used in other blockchain systems. Whenever any blockchain transaction is executed on the *InfraBlockchain*, the block-producer-designated transaction fee tokens are collected as a transaction fee from users. Whereas the other public blockchain's native crypto-currencies are highly volatile in price, in the *InfraBlockchain*, fiat-pegged stable tokens (e.g. USD tokens backed by an equivalent amount of USD held in reserve) issued by trusted entities (e.g. enterprises, financial institutions, governments) are selected as the transaction fee tokens. Fiat-pegged stable tokens are not likely to be involved in speculation and most people and businesses are familiar and comfortable with stable fiat currencies. Asset-backed security tokens (e.g. company shares, gold backed tokens, cryptocurrency backed tokens, real-estate backed tokens, ...) can be also issued and traded through on-blockchain exchange smart contracts using fiat-pegged stable tokens as base currencies.

The block producers are the core blockchain operators who execute blockchain transactions from which transaction fees are collected as the shared profits for the elected block producers. Block producers hold governing power on the blockchain system, making decisions such as selecting transaction fee tokens and deciding transaction fee rates for blockchain operations. The block producers of the *InfraBlockchain* are elected by a unique consensus mechanism:

[5] https://www.longhash.com/news/eos-is-not-a-democracy

Proof-of-Transaction (PoT) using Transaction-as-a-Vote (TaaV). Every transaction can be a vote for a block producer candidate, and the vote amount is proportional to the paid amount of transaction fee. The block producers are continuously elected and evicted by the transparent and fair vote index, the proof of generating meaningful transactions. The Proof-of-Transaction (PoT) mechanism incentivizes the application service providers, who are directly contributing to the blockchain ecosystem by generating blockchain transactions associated with real economic activity, to be elected as block producers.

The *InfraBlockchain* is designed to be a general financial platform supporting smart contracts. Business entities can process their financial transactions on the *InfraBlockchain* using the fiat-pegged stable tokens and custom smart contract codes developed to meet the needs of their business process. The integrated KYC/AML process for *InfraBlockchain* accounts is provided by trusted *Identity Authorities* designated by block producers, which lays the foundation for the secure and reliable financial transactions maintaining regulatory compliance. The enterprise level blockchain scalability provided by the *InfraBlockchain* enables financial transaction processing at global scale.

2 *InfraBlockchain* as Smart Contract Based General Financial Platform

The *InfraBlockchain* includes a smart contract execution environment, fiat-pegged stable tokens, and an integrated blockchain account KYC feature, together comprising a blockchain-based general financial platform. Any customized smart contract code designed to meet the user's business needs can be deployed to operate a blockchain based financial application service on the *InfraBlockchain*. The smart contract based blockchain platform with the fiat-pegged stable tokens as base currency used by the users who has gone through identity authentication (KYC) process meeting the regulatory compliance has great potential as an alternative financial network system whereby fintech services can be implemented conveniently and cost-effectively on the secure and scalable blockchain based environment. In the *InfraBlockchain* ecosystem, fintech service providers who are planning to implement blockchain based service do not need to worry about the risk of high cost and high volatility of purchasing platform coins like ETH and EOS to pay for blockchain transactions. The fiat-pegged stable tokens issued by trusted entities and selected by block producers are used as transaction fee payment currencies which assure predictability of service operation costs, and fintech services themselves can use the fiat-pegged stable tokens as payment or as the base trading currency for their own financial services, just as businesses in the real world naturally use fiat currencies instead of volatile crypto-currencies. Whereas the blockchain service users also have to hold some amount of cryptocurrencies to execute the user's own blockchain transactions on other

smart contract enabled blockchains, the *InfraBlockchain* provides delegable transaction fee payment by which the service provider can pay the fiat-stable blockchain transaction fees for their user's blockchain transactions just as other internet based service providers pay the server cost to provide free web services for their users.

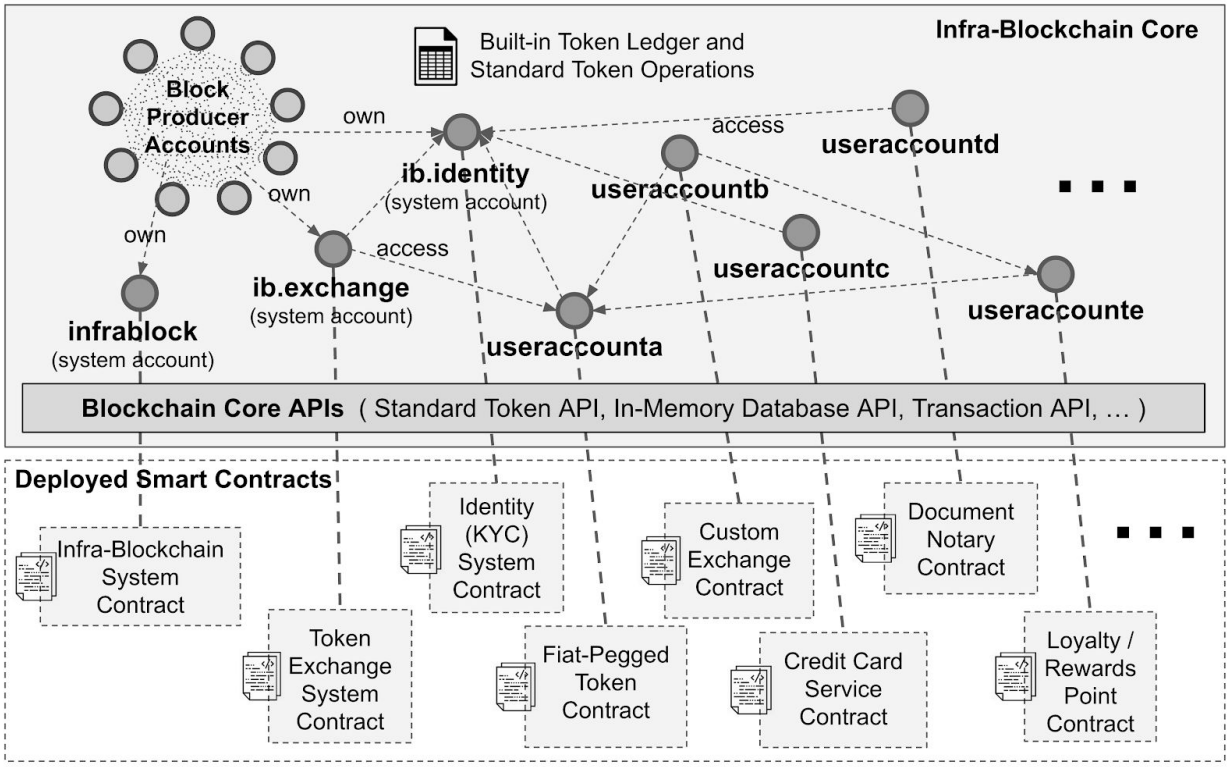

Figure 2.1 - Smart Contract Based *InfraBlockchain* System Architecture

There are two types of smart contracts on the *InfraBlockchain*: *system smart contracts* and *user-deployed smart contracts*. The system smart contracts are privileged smart contracts deployed on special system accounts owned and managed by the elected block producers. The *InfraBlockchain system contract* deployed on the special account *'infrablock'* handles system level blockchain operations such as blockchain account creation, account permission management, block producer related operations, and so on. The *InfraBlockchain* provides the *system identity contract* for blockchain account KYC feature and the built-in on-chain *system token exchange contract* (buy/sell *InfraBlockchain Standard Tokens*) in addition to the *InfraBlockchain system contract*. The *InfraBlockchain* core implements the *InfraBlockchain Standard Token* model. Every blockchain account has a token ledger and common token operations inherently built on blockchain core without a deployed smart contract code. All smart contracts other than the system smart contracts are user-deployed smart contracts deployed on each user's blockchain account implementing user-designed custom blockchain operations (actions). Examples of user-deployed smart contracts are fiat-pegged stable token contracts,

asset-backed token contracts, token exchange contracts, non-fungible token contracts (e.g. unique game items), document notary contracts, loyalty/rewards point contracts, and so on.

The *InfraBlockchain* also functions as a decentralized token exchange (DEX) platform. A built-in token exchange smart contract is deployed as a system contract managed by the elected block producers. Any token issued as a *InfraBlockchain Standard Token* can be easily traded through the transparent on-chain order books and the standardized buy/sell order transactions executed on the system token exchange contract. Asset-backed tokens like company share tokens, gold tokens, art-piece tokens, loyalty/rewards tokens, and so on, can be easily traded using the fiat-pegged stable tokens as the base trading currencies. Due to the *InfraBlockchain Standard Token* model enforced on the standard token interface at the blockchain core level, a token exchange smart contract can seamlessly interface with the various types of tokens being circulated on the *InfraBlockchain*. Any other entities also can deploy their own custom token exchange contracts using the standard token interface. Unlike a centralized crypto exchange services, 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 on the smart contacts. An immutable record of the trading transactions is transparently visible to the public and cannot be manipulated by a centralized actor.

3 *InfraBlockchain Standard Token* Model

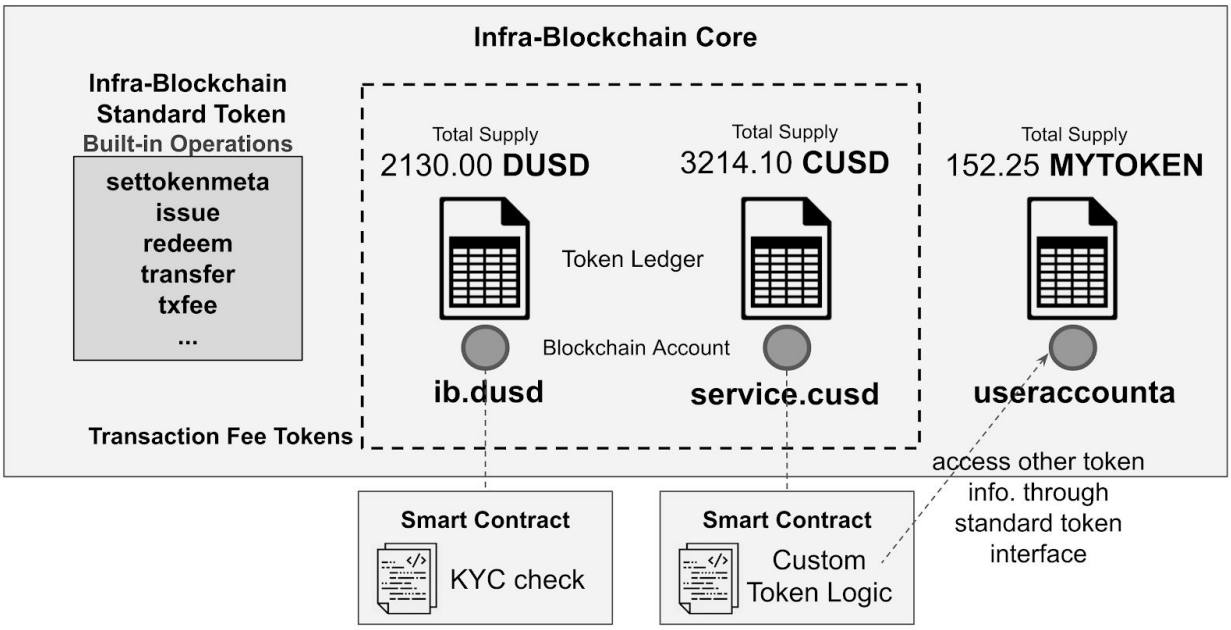

Figure 3.1 - *InfraBlockchain Standard Token* Model

3.1 Every Blockchain Account is a Built-in Standard Token

The *InfraBlockchain* provides a unique token model different from the other smart-contract enabled blockchains such as Ethereum and EOS which provide one built-in native crypto token (ETH, EOS) used for blockchain transaction execution at the core system level, and support user-created custom tokens at smart contract level. Unlike these, there is no single distinguished built-in native token in the *InfraBlockchain*. Instead, every account created can mint a *InfraBlockchain Standard Token* and inherently run standard token operations natively supported at the blockchain core level. Interoperability among the tokens on the *InfraBlockchain* is enforced and guaranteed by the blockchain core system. In other blockchains, to create a new token, custom smart contract code needs to be developed and deployed by users for each token (optionally implementing a de-facto standard token interface like Ethereum ERC-20[6], which is just a recommendation). Typically, the same token functionalities are redundantly implemented on each token contract. In the *InfraBlockchain*, it is not required to create and deploy custom token contract code for each new token. Every blockchain user can make his/her account act as a *InfraBlockchain Standard Token*, and *issue*/*transfer*/*redeem*(burn) its own tokens freely on the *InfraBlockchain*. Based upon this standardized token interface and implementation, *InfraBlockchain* also supports flexible

[6] Ethereum ERC-20 Standard Token Interface https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

polymorphic implementation of various token contracts. If custom token operations need to be implemented (for example, a token that can only be circulated among accounts that have gone through the KYC process, implementing custom coin offering logic and so on), then blockchain users have the option to develop and deploy their own custom token contract codes which still inherit the built-in standard token operations and which then may optionally implement new custom operations. Every token created as a *InfraBlockchain Standard Token* is accessible through the standard token interface from the blockchain core, from user-level smart contracts, and from external systems.

Each *InfraBlockchain Standard Token* is identified by its symbol name tagged by the blockchain account name of the issuer of the token. (e.g. DUSD/*ysmt.dusd*, MYTOKEN/*useraccounta*) Each token account can have its own token symbol name, but the same symbol name can be used by multiple token accounts.

- Notation for *InfraBlockchain Standard Token* :
  {TOKEN_SYMBOL}/{TOKEN_ISSUER}

  e.g) **DUSD/ib.dusd** : US-Dollar-pegged digital USD token issued by the blockchain account '*ib.dusd*'. The issued DUSD token amount should be equal to the USD fund amount transparently held by the account owner. (fiat-pegged stable token) DUSD tokens are only redeemable by the owner of 'ib.dusd' account. **1000.0000 DUSD/ib.dusd** denotes $1000 equivalent token issued by *ib.dusd* account.

3.2 Built-in Standard Token Operations

The common token operations such as creating / issuing / redeeming / transferring tokens are built-in on *InfraBlockchain* core inherently for every blockchain account. Every blockchain account can process below built-in operations without a deployed smart contract code.

- ***SetTokenMeta*** Operation
  A blockchain account owner can make its account act as a *InfraBlockchain Standard Token*. Token symbol name and precision, token meta information like website url of token issuer are set up by this operation executed on blockchain.
  (e.g. settokenmeta *'ysmt.dusd'*, 'DUSD,4', 'https://infrablockchain.com')

- ***Issue*** Operation
  A token account owner can issue its new tokens to a specific blockchain account. The tokens issued by token account owner can be circulated among the blockchain accounts.
  (e.g. issue 5000.0000 DUSD/*ib.dusd* to *useraccounta*)

- ***Transfer*** Operation
  A token holder can transfer its own tokens to another receiver account.

(e.g. transfer 150.0000 DUSD/ysmt.dusd from *useraccounta* to *useraccountb*)

- ***TxFee*** Operation
  If a token account is selected as a *Transaction Fee Token* by block producers (@see 3.3), *'txfee'* standard token operation is auto-generated from *InfraBlockchain* core after calculating the transaction fee amount for processing actions on a submitted transaction. The transaction fee is charged to the designated transaction fee payer account whose signature is also included in the transaction message. (@see 4.2)
  (e.g. txfee 0.0525 DUSD/*ysmt.dusd* charged to tx-fee payer *useraccountx*)

- ***Redeem*** (Burn) Operation
  Only the token issuer can redeem (burn) the tokens held by the token issuer account.
  (e.g. redeem 1000.0000 DUSD/*ysmt.dusd*)

- **Read-Only Operations**
  All information for *InfraBlockchain Standard Tokens* issued and circulated on the blockchain is transparent to everyone. Programmatic access to the token information is provided to blockchain core, smart contract codes deployed on any account and any external system accessing *InfraBlockchain* nodes through the chain information API.
  - ***GetTokenMeta*** - to get token meta information such as symbol name/precision and token issuer website
  - ***GetTotalSupply*** - to get current total supply of a token
  - ***GetTokenBalance*** - to get token balance of an account for a token

3.3 Transaction Fee Tokens Selected by Block Producers

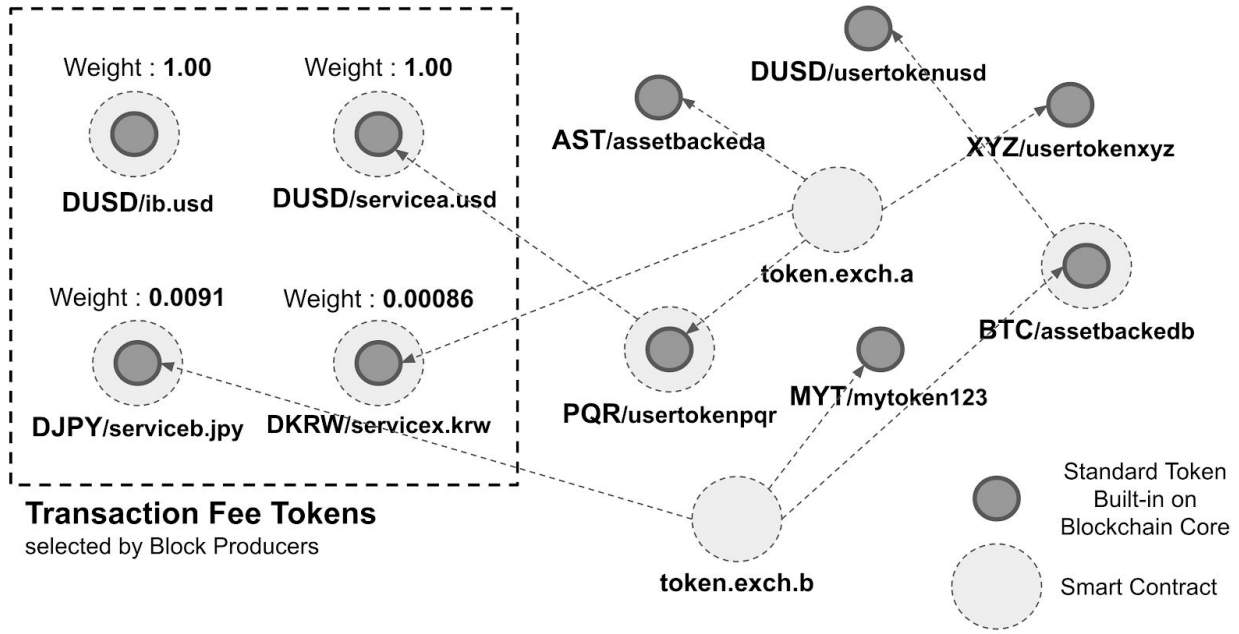

Figure 3.2 - *InfraBlockchain* Token Ecosystem and Transaction Fee Tokens Selected by the Block Producers

Figure 3.2 shows an example of a token ecosystem constructed on *InfraBlockchain* where anyone can freely make a *InfraBlockchain Standard Token*. Smart contracts have access to any *InfraBlockchain Standard Token* through the standard token interface. Any entity can develop and deploy an on-chain token contract interoperating with other tokens seamlessly.

Among the *InfraBlockchain Standard Tokens* issued and circulated on the blockchain, block producers elected by the blockchain ecosystem through the Proof-of-Transaction (PoT) / Transaction-as-a-Vote (TaaV) (*@see chapter 5*) can select multiple *InfraBlockchain Standard Tokens* as the *Transaction Fee Tokens* which can be used for blockchain transaction fee payment. When a blockchain transaction is executed, the selected *Transaction Fee Tokens* are consumed to pay the transaction fee, just as native cryptocurrencies (e.g. ETH) would be in other blockchain systems. The *InfraBlockchain* is a fee-based blockchain system: every blockchain operation is charged a transaction fee by default. Because there is no distinguished native token used for transaction fee payment (like ETH), stable tokens (usually fiat-backed stable coins) issued by some trustworthy entities can be selected by the block producers and used as the transaction fee payment token collected to pay the block producers. Block producers themselves decide which tokens they will accept for payment of transaction fees. When block producers make a token eligible as a *Transaction Fee Token*, a *weight* value is also chosen for each token. The *weight* of a *Transaction Fee Token* determines how many units of that token are equivalent to a standard transaction fee unit. The weight can be thought of as similar to the foreign exchange rate among the different fiat currencies. Suppose block producers have decided

to use USD as base currency for transaction fee payment, A USD-backed stable tokens is selected as a *Transaction Fee Token* with *weight* 1.00, and non-USD fiat-pegged stable tokens are selected with weight not equal to 1.00 (e.g. *weight* 0.00086 (USD/KRW foreign exchange rate) chosen for a KRW-backed stable token). The *InfraBlockchain* core determines the *Transaction Fee Token* amount charged for each transaction according to the block-producer-designated fee amount per operations, the consumed computing resources (cpu, network, storage) and the *weight* of the used *Transaction Fee Token*. The *InfraBlockchain* core system automatically generates and executes the ***'txfee'*** standard token operation which charges *Transaction Fee Tokens* to the transaction fee payer for the measured transaction fee amount imposed for executing blockchain operations in a user-sent original transaction message. *(@see chapter 4 for more details)*

As the blockchain ecosystem evolves, the continuously elected block producers of the *InfraBlockchain* can make tokens eligible and revoke the eligibility of tokens as *Transaction Fee Tokens* with the agreement of ⅔+ of the active block producers. In other smart contract based blockchains like Ethereum and EOS, custom tokens implemented as smart contracts are totally separate from the native cryptocurrency (ETH, EOS) used for executing blockchain transactions. In contrast, *InfraBlockchain* lets any custom user token conforming to the *InfraBlockchain Standard Token* interface become a *Transaction Fee Token* just as a native cryptocurrency can in other blockchain systems.

4 *InfraBlockchain* Transaction Fee Model

4.1 Transaction Fee Table Managed by Block Producers

InfraBlockchain is a fee-based blockchain system, charging *Transaction Fee Tokens* for each transaction executed on the blockchain to the transaction fee payer designated in the transaction message. A transaction can contain multiple operations which are targets for a transaction fee charge. Block producers manage the transaction fee table on-chain, transparently specifying the prices of specific blockchain operations, which can be *InfraBlockchain Standard Token* operations or custom smart contract specific operations. The transaction fee table can be continuously updated with the agreement of ⅔+ of the block producers, by which the blockchain transaction fee rates are governed in a transparent and decentralized fashion reflecting the needs of the blockchain ecosystem. If a smart contract operation whose price is not specified on the fee table is executed, the default transaction fee per operation is charged. Since a user-created custom smart contract could use a large amount of computing resources (cpu time, network bandwidth, storage space), a dynamic transaction fee amount determined by how much computing resources are consumed can be also applied. If the resource consumption based dynamic transaction fee measured for an operation is greater than the transaction fee price on the transaction fee table or the default transaction fee per operation, then the dynamic transaction fee is charged for the executed operation. The calculated transaction fee amount is by default in the base currency units as agreed by the block producers (e.g. if a USD pegged *Transaction Fee Token* is selected with weight 1.00, the base currency unit for transaction fee payment is USD), so finally the weighted amount of *Transaction Fee Tokens* to be charged for the transaction fee calculated by applying relative weights (exchange rates) among the selected *Transaction Fee Tokens*.

txfee_token_amount_charged_to_an_operation =
max{ (txfee_table(operation) | default_txfee), dynamic_txfee(operation) } / txfee_token_weight

Figure 4.1 is an example of a transaction fee table managed by block producers. *(Code, Operation)* designates a specific blockchain operation implemented on blockchain core or system smart contract code or user-created smart contract code. Block producers can set the default fixed transaction fee per operation, set transaction fees for built-in standard token operations (overridable for each specific token account) and for contract code specific custom operations. As an exception, transactions for which the fee payer is specified as the system account having signatures from ⅔+ block producers are exempt from paying transaction fee.

Code (Account)	Operation	Fee Value	Fee Type	
-	-	0.07 DUSD	Fixed	Default tx fee per operation (minimum fixed fee)
-	**issue**	0.03 DUSD	Fixed	Default tx fee charged for a *'issue'* standard token operation
-	**transfer**	0.02 DUSD	Fixed	Default tx fee charged for a *'transfer'* standard token operation
ib.dusd	**transfer**	0.01 DUSD	Fixed	different 'transfer' tx fee from default 'transfer' charged for *'ib.dusd'* contract
accountabc	**deposit**	0.1 DUSD	Fixed	Tx fee charged for *'deposit'* custom operation of *'accountabc'* contract code
accountxyz	-	2x	Dynamic	Dynamic tx fee depending on computing resources (CPU/NET/STORAGE) consumed by executing an operation on *'accountxyz'* contract. 2x fee rate
ib.identity	-	0	-	No transaction fee for every operation on *'ib.identity'*(KYC) system contract
...	...	...	...	...

Figure 4.1 - Example of Transaction Fee Table Managed by Block Producers

4.2 Delegable Transaction Fee Payment

For every blockchain transaction submitted to the *InfraBlockchain*, the *transaction fee payer* account name must be specified and the transaction message must include the signature of the transaction fee payer account in addition to the signatures required by the blockchain operations in the submitted transaction. If the transaction fee payer account has enough *Transaction Fee Tokens* to execute the transaction, then the auto-generated *'txfee'* standard token operation is executed on the payer account whose tokens are consumed, or else the transaction fails. Because the transaction fee payer is always specified separately from the accounts directly involved in a transaction, the transaction fee payment can be delegated to some other account. (e.g. when a token transfer from account A to account B is executed, a different account C can pay the transfer transaction fee.) Enforcing that every blockchain account holds some tokens to make blockchain transactions (like most public blockchains (Bitcoin, Ethereum, EOS, ...)) is a big hurdle for blockchain based applications to be broadly adopted. For the sake of a seamless and convenient user experience, blockchain service providers can pay blockchain transaction fees on behalf of the service's users. In the *InfraBlockchain*, delegated transaction fee payment is possible for every blockchain transaction.

5 Fiat-Stable Tokens and Security Tokens on *InfraBlockchain*

5.1 Token Backing Depository

A *Token Backing Depository* is an entity that issues tokens in the *InfraBlockchain* and ensures the value of issued tokens by holding assets of equal value to back the issued tokens. Whenever a token holder requests to redeem tokens, i.e. to withdraw the backing of their tokens, the *Token Backing Depository* who issued the token burns the requested amount of tokens on the blockchain and transfers the corresponding amount of the backing asset to the user. The *InfraBlockchain Standard Token* interface includes built-in operations for issuing and redeeming (burning) tokens. Token symbols are tagged by the blockchain account name of the *Token Backing Depository* who issued each token. A token can be redeemed by only the *Token Backing Depository* whose account name is tagged on the token symbol.

DUSD/D1 : USD-pegged digital UXD token issued by the *Token Backing Depository* D1, only redeemable by D1
BTC/D2 : Bitcoin-backed BTC token issued by the *Token Backing Depository* D2 holding the private keys controlling the issued amount of actual Bitcoin, only redeemable by D2

If multiple entities issue USD-pegged tokens, each token tagged by each *Token Backing Depository* should be redeemed by the corresponding Depository. Tokens can be issued by any blockchain account owner, but *Token Backing Depositories* need trust from other blockchain users for their tokens to be accepted by others in the system. The *Token Backing Depositories* are always required to prove transparently that they hold the backing of the outstanding tokens to maintain this trust.

5.2 Fiat-Pegged Stable Tokens (*dFIAT*)

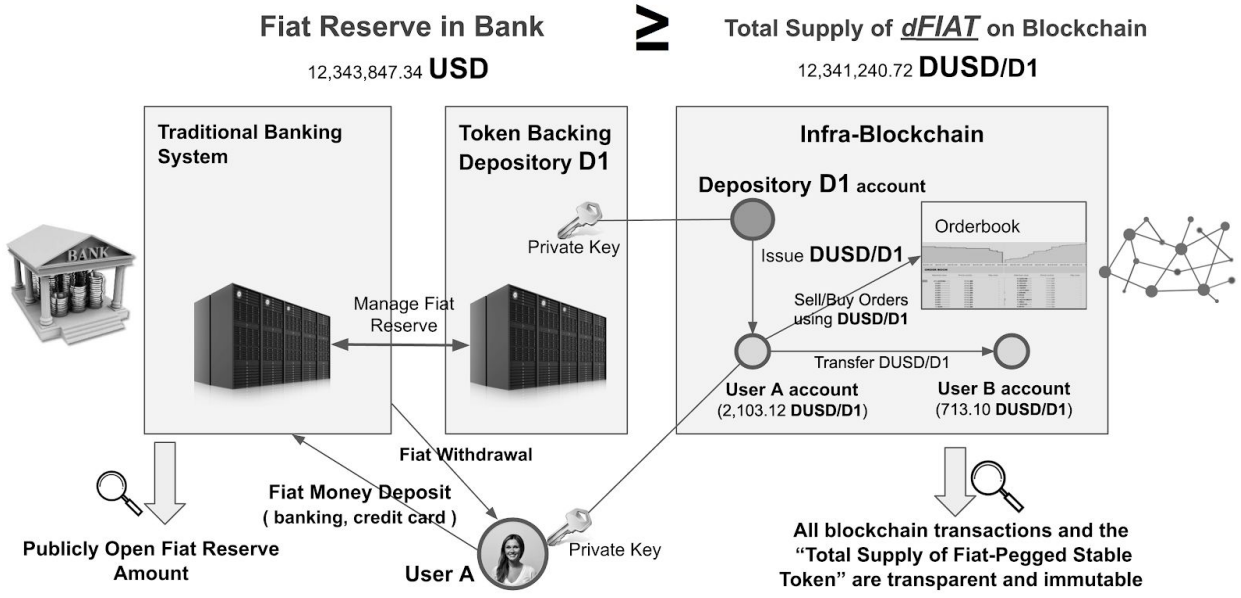

Figure 5.1 - Fiat-Pegged Stable Token (*dFIAT*) issued on the *InfraBlockchain*

A fiat-pegged stable token is maintained by one-to-one backing of fiat money held in reserve outside the blockchain. Any entity can issue a fiat-pegged stable token backed by a specific fiat currency reserve fund. If the elected block producers select a fiat-pegged stable token trusted by the blockchain ecosystem, the the fiat-pegged stable token can be used as a Transaction Fee Token like a native cryptocurrency on a blockchain. A blockchain account holding some selected *Transaction Fee Tokens* can execute blockchain transactions consuming the tokens for the transaction fee payment. Below are the examples of fiat-pegged stable tokens.

- **DUSD/TFI** : USD-pegged stable token, digital USD, issued by a trusted financial institution (TFI), which could serve as a *Transaction Fee Token* and a base currency for on-chain token exchanges on a blockchain operated in a country where people use USD as currency.
- **DKRW/BK1** : KRW-pegged stable token, digital KRW, issued by a trusted bank (BK1), which could serve as a *Transaction Fee Token* and a base currency for on-chain token exchanges on a blockchain operated in a country where people use KRW as currency.

...

dFIAT is only issued when the users of the blockchain deposit their fiat money into the *dFIAT Token Backing Depository*. If a user sends 100.00 USD worth of fiat money through an existing payment channel (e.g. wire-transfer, credit card payment) to the bank acting as a *Token Backing Depository* (TFI), then the same amount (100.00) of DUSD/TFI is issued to the user's

blockchain account. The *Token Backing Depository*'s off-chain system manages the fiat reserve by interfacing with traditional banking systems and handles *dFIAT* token issuance/redeeming by interfacing with the blockchain using the securely stored private key. Because the guarantee of redeeming *dFIAT* for actual fiat money is crucial, the existence of trusted entities issuing fiat-pegged stable tokens who receive widespread ecosystem support is indispensable to the *InfraBlockchain* design.

The public ledger of *dFIAT* token distribution for every blockchain account is maintained transparently and securely on the blockchain. All blockchain transactions such as issuing, redeeming (burning) *dFIAT* and transferring *dFIAT* among blockchain accounts are transparent and securely immutable since the transactions occur on the blockchain. Since all actions of a *dFIAT Token Backing Depository* are also transparent and traceable, the total supply of the *dFIAT* token being circulated on the blockchain is always public information. So, if the bank holding the fiat money deposited through the *dFIAT Token Backing Depository* allows public access to the current fiat money reserve balance in a reliable way, blockchain users can transact on the *InfraBlockchain* without fear that the *dFIAT* may not be backed by sufficient reserves for full redemption. The total supply of a *dFIAT* token on the blockchain should always be less than or equal to the fiat reserve amount in the bank connected to the *Token Backing Depository*.

5.3 Asset-Backed Security Tokens (*dASSET*)

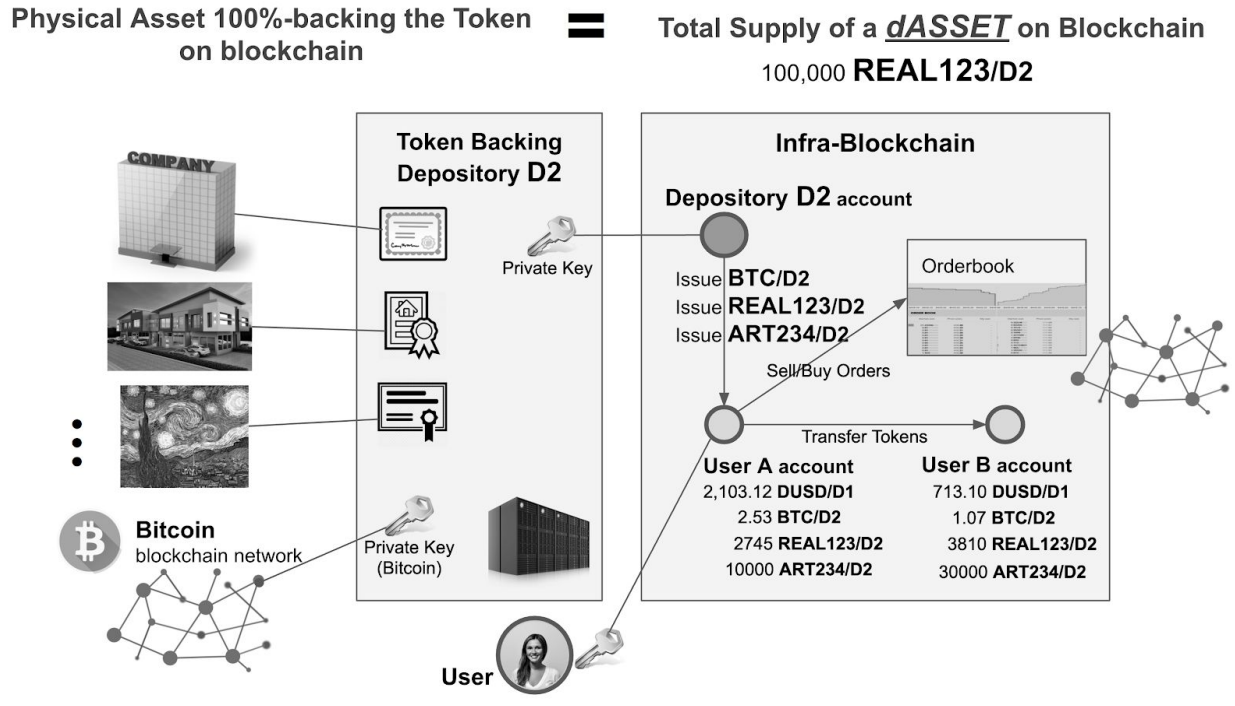

Figure 5.2 - Asset-Backed Security Tokens (*dASSET*) issued by Token Backing Depositories

Depositories can also issue real asset-backed security tokens (*dASSET*, digital ASSET token) on the *InfraBlockchain*. The real assets, such as company shares, real estate, art pieces, gold, diamond, crypto-currencies on the other public blockchains and so on, can be tokenized through trusted *Token Backing Depositories* connecting the real assets and the *dASSET* tokens. For example, REAL123/D2 is a real estate backed security token issued for a building managed by a *Token Backing Depository* D2, and can be used to trade shares of the tokenized building. A *Token Backing Depository* issuing *dASSET* is required to securely manage the ownership of the tokenized real assets and keep the real asset safe physically and legally. The asset is owned in its entirety by the *Token Backing Depository* off-chain, but partial ownership shares of the tokenized asset can be traded on the *InfraBlockchain* via the token representing these shares. The open market determines the price of the assets through the on-chain token trading. If there is revenue generated from the tokenized asset, e.g. getting monthly rent, the dividends 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 a 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 the 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 can be implemented as custom token smart contracts inheriting the *InfraBlockchain Standard Token* operations.

The external cryptocurrency pegged tokens (e.g BTC/D2, ETH/D3) can be issued by *Token Backing Depositories* in the same way as the fiat-pegged stable tokens. A *Token Backing Depository* can issue the exact amount of crypto pegged token on the *InfraBlockchain* only when a blockchain user deposits the same amount of cryptocurrency to the *Token Backing Depository*'s external blockchain (e.g. Bitcoin, Ethereum) account. The redemption of the issued crypto-backed tokens owned by blockchain users on the *InfraBlockchain* to the user's external blockchain accounts in the corresponding external blockchains should be guaranteed by the Token Backing Depositories who issued the crypto-backed tokens.

6 Proof-of-Transaction (PoT) Consensus Mechanism

6.1 Transaction-as-a-Vote (TaaV)

The key idea that makes Proof-of-Transaction (PoT) 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 in or is already participating in the blockchain consensus process. In blockchain transactions which incur a transaction fee, there is an optional "*transaction vote*" field where a blockchain account name can be nominated. The entity generating the transaction thereby designates a blockchain account running a blockchain core node to be a block producer of the *InfraBlockchain*. The transaction message containing the vote for block producer is cryptographically signed by the private key of the blockchain account originating the transaction, so each transaction vote has its own cryptographic proof on-chain.

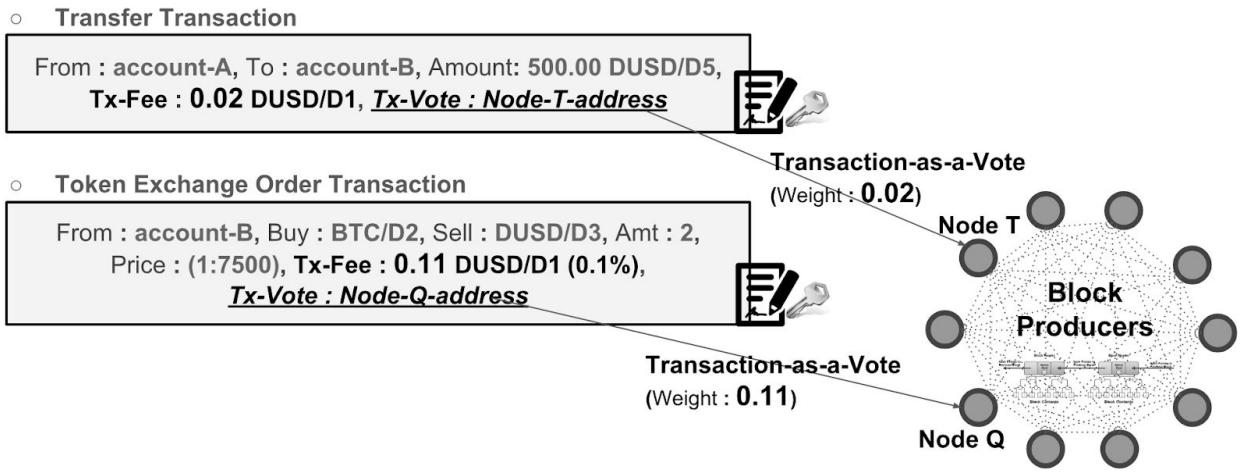

Figure 6.1 - Transaction-as-a-Vote examples

The blockchain core nodes who receive the most votes from the processed transactions are elected to the group of block producers that cooperatively make new blocks and collect transaction fees from blockchain activity. Only the transactions incurring transaction fees paid by blockchain users, i.e. transactions actually contributing to economic activity on the blockchain itself, will generate profits for block producers, the core blockchain operators. Each vote is not equally weighted; rather they are weighted in proportion to the transaction fee amount paid. In the example in Figure 5.1, the token transfer transaction incurring transaction fee 0.02 DUSD/D1 with a transaction vote signed for the Node-T-address is 0.02-weighted vote to Node-T. The token exchange sell order transaction with a transaction vote signed for the

Node-Q-address, which will incur 0.11 DUSD/D1 as transaction fee when the order is executed, is 0.11-weighted vote to Node-Q.

In other blockchains, the voting process for blockchain governance and profit sharing are usually governed by a process distinct from the normal transactions representing economic activity in the system, and an explicit, separate procedure is used to manage voting. Since most users do not take the time to explicitly vote, especially if fees are incurred while doing so, voting rates are typically low in such blockchain governance mechanisms. In the EOS blockchain, for example, the EOS token holders have to cast their votes explicitly for the block producers[7]. In the Stellar blockchain, the *Lumens* token holders have to designate a blockchain account address who will take a portion of the cryptocurrency inflation[8]. But in the *InfraBlockchain* 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 process.

6.2 Proof-of-Transaction as Incentivization for Service Providers

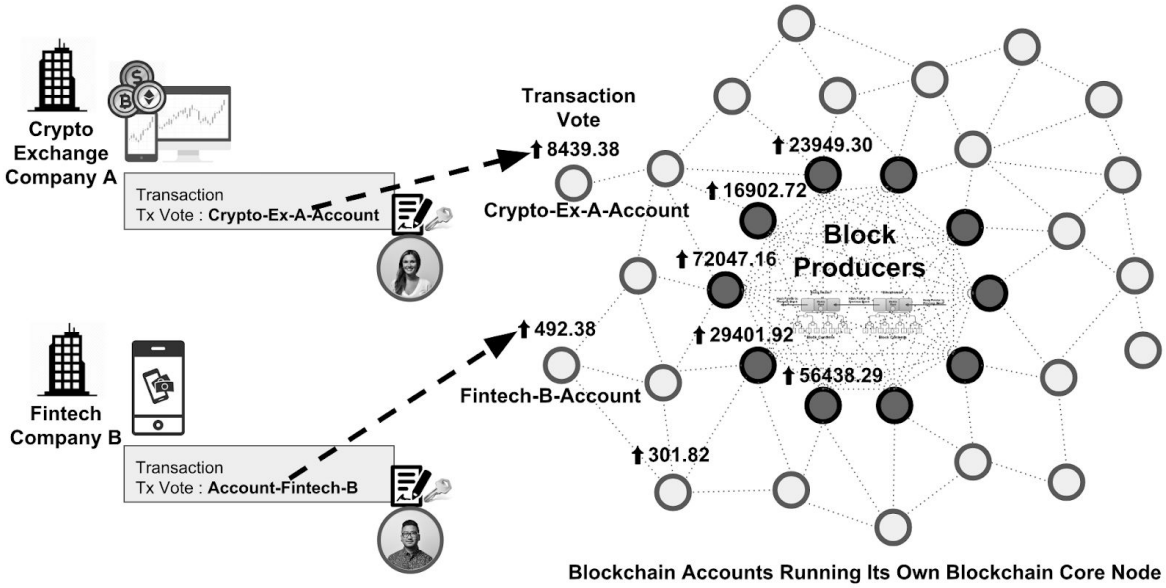

Figure 6.2 - Proof-of-Transaction as the incentivization for the blockchain-based service providers

The transaction votes for each blockchain account running a blockchain core node (all of whom are block producer candidates) are continuously accumulated as transactions are processed on the blockchain. The amount of transaction votes acquired represents the solid proof of how much that blockchain account has been involved in producing meaningful blockchain

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

transactions and creating economic activity in the blockchain ecosystem. The accumulated vote amount is used as the key criterion for block producer election in the *InfraBlockchain*. In contrast, Proof-of-Work (PoW) based blockchains reward those entities having a large hash power deriving from controlling a huge amount of computational resources and wasting them regularly, which contributes nothing to the blockchain itself besides defining an artificial competition for block production, and massive amounts of natural resources are consumed as an unwelcome side-effect. Alternatively, Proof-of-Stake (PoS) based blockchains reward entities owning a large amount of the blockchain's native cryptocurrency. The validators or block producers of PoS, who already possess a lot of cryptocurrency, will have more opportunities to earn newly-minted crypto-currencies generated as the block reward from the blockchain itself, creating a rich-get-richer dynamic which consolidates ownership of the system and undermines its governance. Both PoW and PoS produce incentives that provide further rewards to the players who already have the large vested interests, but who need not directly contribute to the creation of economic activity in the system. The Proof-of-Transaction (PoT) consensus mechanism of the *InfraBlockchain* instead incentivizes service providers who can bring the most real economic activity to the chain, that is, it rewards the parties directly contributing the most to the blockchain economy by creating real transactions, not just leveraging already vested computation power or financial wealth.

Though blockchain transaction messages must always be cryptographically 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 can be automatically filled in by the operator of the application that transacts on behalf of the user. So when the blockchain service provider creates blockchain transaction messages for the application users, the service provider's own blockchain account name can be specified in the transaction vote field for every transaction generated from that application. In the example in Figure 6.2, the crypto exchange company A is providing a service built on the *InfraBlockchain*. The crypto trading software built by the company A always inserts the company's own blockchain account name (*Crypto-Ex-A-Account*) in the transaction vote field of every blockchain transaction message made for the service user's sell/buy order. As the trading volume of the exchange service grows, the company A's blockchain account accumulates a significant amount of transaction votes that eventually enable the service provider to qualify as a block producer. The blockchain based service providers, such as exchange service providers, fintech companies, and so on, compete in a transparent and fair way to get as many transaction votes as possible by providing useful services to the users.

6.3 Blockchain Consensus and Transaction Fee Profit Distribution

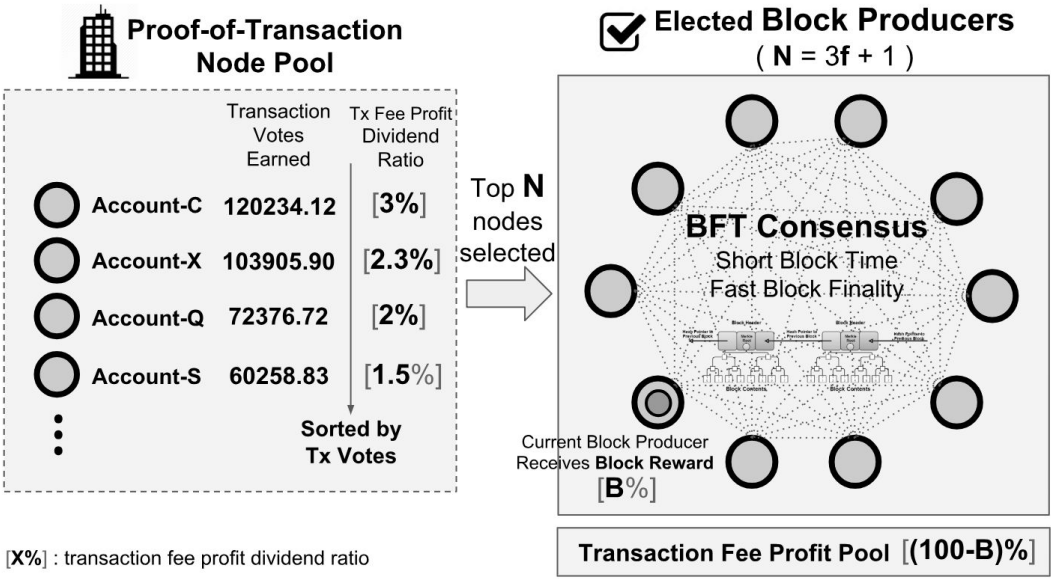

Figure 6.3 - Proof-of-Transaction based BFT blockchain consensus
(public blockchain setup with no seed trust node)

6.3.1 Proof-of-Transaction (PoT) Node Pool

The Proof-of-Transaction blockchain consensus mechanism has been designed to have ideal properties for a public/permissioned hybrid blockchain such as the *InfraBlockchain*. Any entity can be elected as a block producer, and can subsequently participate in the blockchain consensus process (i.e. making new blocks by validating and executing transactions) and collect the profits of maintaining the blockchain infrastructure. Entities compete for these rewards by earning sufficient transaction votes from blockchain users for whom the entity provides useful blockchain-based application services, aligning their incentives with the health of the blockchain ecosystem. The blockchain accounts of service providers running the blockchain core nodes, which earn a considerable amount of transaction votes are listed publicly on-chain in the *Proof-of-Transaction Node Pool*. The accounts in the *PoT Node Pool* are guaranteed to get a portion (dividend) of the transaction fee profits from the *InfraBlockchain*. The amount of transaction votes earned by each account is calculated by the elected block producers through a BFT[9](Byzantine Fault Tolerant)-based consensus in a secure and transparent manner, being utilized as the reliable and fair criteria to determine the beneficiaries of the blockchain system's operating fees. The number of accounts in the *PoT Node Pool* is limited and there is a threshold amount of transaction votes which must 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

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

earned. In the example of Figure 6.3, the top rated Account-C who earned *120234.12* points from weighted transaction votes can claim 3% of the transaction fee profits generated from a time window. The top accounts in the *PoT Node Pool* are also eligible to be elected as block producers, who can make new blocks and earn an additional block reward profit.

6.3.2 Seed Trust Node Pool

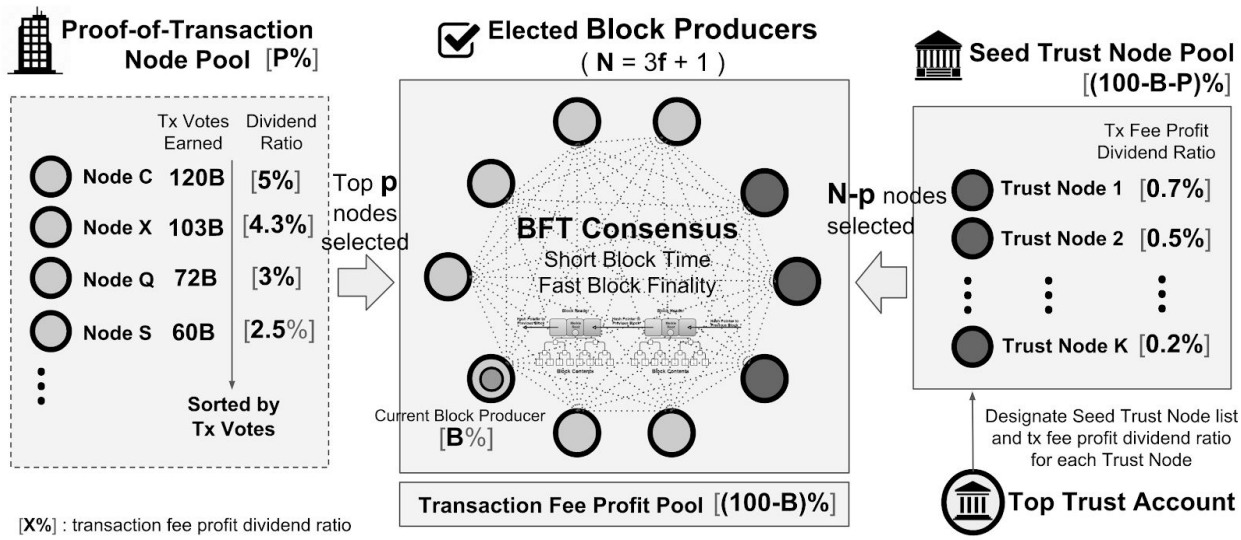

Figure 6.4 - Proof-of-Transaction based BFT blockchain consensus including Seed Trust Nodes (public/permissioned hybrid setup)

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 *InfraBlockchain*, trusted Depositories providing *dFIAT* 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 6.3.4 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 *InfraBlockchain* 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 *InfraBlockchain* 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.

6.3.3 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 number of consensus participants (i.e. validators, block producers) can be bounded. There is no predetermined bound on the number of consensus participants in existing PoW-based consensus systems (e.g. Bitcoin, Ethereum). In those, any node is able to competitively find the solution of the hash puzzle for the next block, and thus any node can be a block producer. Neither does the FBA (Federated Byzantine Agreement) consensus technique yield such a bound. It is based on the 'quorum-slice' concept and is used in the Stellar Consensus Protocol[10], in which the quorum set participating in the consensus can also become arbitrarily large as the quorum-slices of the consensus nodes expand. In that situation, high TPS is not guaranteed. In a practical setup, a blockchain with FBA consensus is instead managed by a small, fixed set of authority nodes constituting the consensus quorum set, which enables the system to achieve high TPS, but that in fact results in an effectively permissioned blockchain, in which new users have no direct incentive to run a blockchain node due to the lack of a guaranteed block reward and the low probability of inclusion in the top tier quorum set which participates in blockchain consensus. In the BFT-based consensus algorithms like PBFT[11] (Practical Byzantine Fault Tolerance), Tendermint [12], and the DPoS[13] (Delegated PoS) of Steem/BitShares/EOS, there is also a predefined number of elected consensus participants (i.e. validators or block producers) which yields high TPS because the elected set of nodes can cooperatively make fast consensus for new block creation with the agreement that the new blocks created through the consensus of the elected nodes are authoritative. The *InfraBlockchain* adopts the optimized modification of BFT-based consensus algorithms (@see 6.3.5) to achieve short block time (inspired by DPoS of Steem/BitShares/EOS) and fast 100% block finality (inspired by Tendermint), but adds the unique block-producer-election mechanism based on the Transaction-as-a-Vote (TaaV) and Proof-of-Transaction (PoT).

Block producers participating in the consensus protocol to generate new blocks in the *InfraBlockchain* are elected from the *PoT Node Pool*. Let *N* represent the number of the block producers to be chosen. The top *N* nodes based on the earned transaction vote amount are selected from the *PoT Node Pool* as block producers in each round. The parameter *N* is fixed in

[10] D. MAZIERES, Stellar Consensus Protocol - https://www.stellar.org/papers/stellar-consensus-protocol.pdf , 2015
[11] M. Castro, B. Liskov - Practical Byzantine Fault Tolerance and Proactive Recovery - http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf , 2002
[12] Jae Kwon - Tendermint : Consensus without Mining - https://tendermint.com/static/docs/tendermint.pdf , 2014
[13] D. Larimer - BitShares - Delegated Proof-of-Stake Consensus - https://bitshares.org/technology/delegated-proof-of-stake-consensus , 2014

the *InfraBlockchain*. Among the *N* nodes elected from the *PoT 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. to run a physical server, the block reward allotted to elected block producers who run core nodes strongly incentivizes the *PoT nodes* to run core nodes and to participate in blockchain consensus. If a *PoT Node* account elected as a block producer does not run a 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 the account of its rank in the block producer list. 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 *InfraBlockchain* is a Byzantine node can be regarded as very low because every elected block producer is a *PoT Node* making profit by operating a blockchain-based service which is in itself profitable, likely more so than the fee income is, and which depends on the health of the blockchain ecosystem for that profitability.

6.3.4 Transaction Fee Profit Distribution

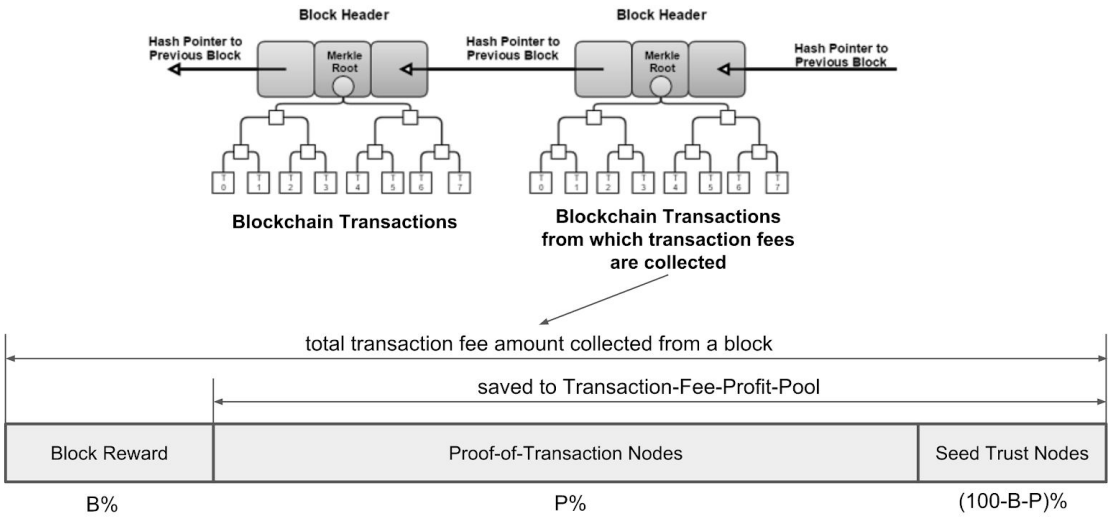

Figure 6.5 - Transaction fee profit distribution

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.

6.3.5 BFT Consensus with Short Block Time and Fast Block Finality

Low latency and high transaction throughput processing capacity are the key scalability traits lacking by the present generation of blockchain technology. The short block time (time interval between consecutive block creation events) and fast block finality (the time required for a new block to be immutable, guaranteeing no fork up to the block) are the crucial properties of a scalable blockchain.

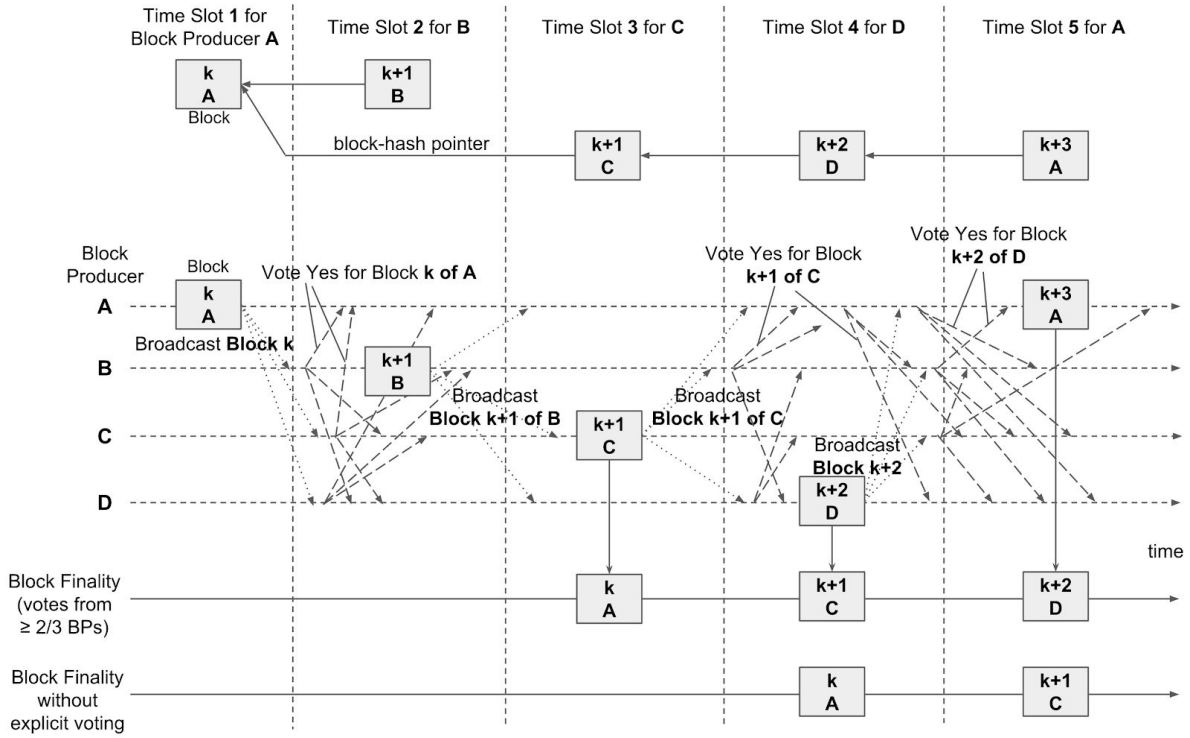

Figure 6.6 - BFT consensus protocol among the elected block producers

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 6.6, 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 temporary 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 recognized Byzantine block producer should be penalized. Remember that 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 would 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 broadcast, 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 *InfraBlockchain* accelerates the block finality time through explicit block validity voting, independent of the block production progress, with the trade-off of higher network communication cost. When a block producer receives a newly broadcast block from another block producer, the new block is validated and a validity vote for the block is broadcast 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 6.5 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 times).

7 Blockchain Accounts

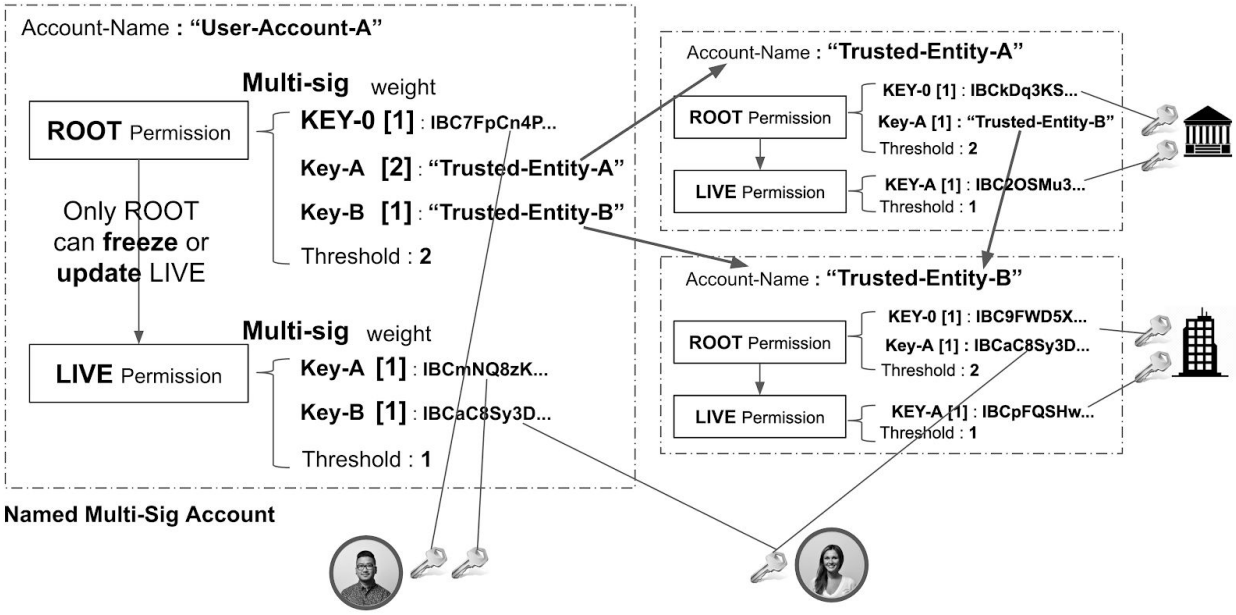

Figure 7.1 - Named Multi-Sig Blockchain Accounts of *InfraBlockchain*

7.1 Named Multi-Sig Blockchain Accounts

The *InfraBlockchain* natively supports named multi-sig[14] blockchain accounts. A blockchain account in the *InfraBlockchain* consists of a *ROOT* permission and *LIVE* permission pair by default. Every usual blockchain transaction includes the cryptographic signature of the *LIVE* permission that should be validated by the block producers. The *LIVE* permission can be updated on the blockchain only by the *ROOT* account when the *LIVE* permission is found to be compromised. The *ROOT* and *LIVE* permissions themselves have multi-sig structure, each having multiple weighted keys and threshold value. To make a valid transaction message signed by a multi-sig permission, 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* permission 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

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

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"* permission of *"Trusted-Entity-A"* must be collected. A blockchain account can have a human-readable alphanumeric identifier (name). 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 an explicit blockchain account creation transaction which is charged some transaction fee in *dFIAT* to prevent account creation spamming attacks.

7.2 Trust Network for Account Recovery

Because the *LIVE* permission can be replaced by the *ROOT* permission, when the blockchain keys are lost or compromised by malicious attackers, the *LIVE* permission and even the ROOT permission used to make blockchain transactions in normal situations can be recovered. Even in the case that some of the keys in the multi-sig *ROOT* permission are lost, the *LIVE* account can be recovered with the help of one or many 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 user to repeat the KYC/AML[15] authentication process to recover an account. 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 *InfraBlockchain*. Figure 6.1 shows an example of a *Trust Network* built by the *"User-Account-A"*, *"Trust-Entity-A"* and *"Trust-Entity-B"* accounts. The Trust Network makes the blockchain ecosystem solid and stable, mitigating the impacts of blockchain key loss.

7.3 KYC/AML Compliance and Account Anonymity

Tokens issued by Depositories in the *InfraBlockchain* 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 which organization carried out the validation is published on the *InfraBlockchain* transparently, but the personal information (e.g. email, phone number, bank account, passport info., ...) gathered from users is privately processed and maintained by the trusted entities. The integrated KYC/AML support by the *InfraBlockchain* 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 can be compromised. To maintain account anonymity, trusted entities like financial companies can

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

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 a financial company providing blockchain-based financial services can use the account ids issued by the company as if they were normal bank account credentials, 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 *InfraBlockchain* account serving all its customers using the tag or memo field in the blockchain transaction messages to distinguish its customers, with its private customer ledger running on its own 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. *InfraBlockchain* will provide standard protocols and open-source components for developers to implement KYC/AML integrated financial services built upon the *InfraBlockchain*.

8 Decentralized Issuance of *dFIAT* without Fiat Reserve

InfraBlockchain users can receive an issuance of *dFIAT* by escrowing their *dASSET* tokens. At a later time, the user can redeem *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 *dASSET* token being escrowed. A very similar decentralized stable coin (bitUSD) implemented by BitShares[16] has proven to closely hold parity with USD. Stable coin issuance via *dASSET* tokens is beneficial to the *InfraBlockchain* 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 *dASSET* tokens ,
n : the number of *dASSET* escrows locked for *dFIAT* issuance ,
$\mathbf{A_i}$: the amount of each *dASSET* token escrowed ,
$\mathbf{P_i}$: the current *dFIAT* price (changing over time) of each *dASSET* token escrowed

[16] 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 *dASSET* tokens must always remain strictly less than the sum of the total value of all escrowed *dASSET* tokens at current prices in *dFIAT*. To ensure this equation always holds, the blockchain will execute a margin call operation, liquidating *dASSET* into the market on the *InfraBlockchain*, at a price strictly higher than the total value of *dFIAT* issued from escrowing *dASSET* tokens at the time. (The elected block producers of *InfraBlockchain* automatically execute sell orders for the escrowed *dASSET* tokens according to the predefined protocol) Among the liquidated *dFIAT* tokens, the same amount of the issued *dFIAT* tokens when the liquidated *dASSET* tokens are escrowed, are burned on the blockchain, and the remaining *dFIAT* tokens are returned to the blockchain account which originally escrowed *dASSET* tokens, excluding the fee amount paid 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 dASSET* (A_i) *and the* $dFIAT^{i}_{AB}$ *is burned*

where ***AB*** *: ASSET-BACKED ,* $\boldsymbol{dFIAT^{i}_{AB}}$ *: the amount of dFIAT issued via each dASSET escrow,*
$\boldsymbol{P_i^E}$: the *dFIAT* price of an *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 *InfraBlockchain* 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 *dASSET* escrows.

9 Scalability of *InfraBlockchain*

9.1 Single Chain Scalability

The single chain scalability of the *InfraBlockchain* 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 second block time, can be realized. In the unique setup of the *InfraBlockchain* consensus, the service providers acting as *PoT Nodes* will be elected to become block producers running full core node servers. They are expected to provide high performance computing power efficiently and securely to the blockchain ecosystem, handling very large volumes of transactions. The probability for the nodes run by the service providers and trusted entities to be Byzantine is very low; 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.

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

Though the single chain throughput facilitated by the *InfraBlockchain* is enough for most blockchain service applications, including on-blockchain decentralized exchanges, for exceptional cases like high frequency trading or micropayments, *InfraBlockchain* has already provided on/off-chain hybrid state-channel/exchange technology. Some trading pairs needing high volume and high frequency trading can be serviced using the existing *InfraBlockchain* hybrid architecture. In this hybrid architecture, only 'deposit to exchange' and 'withdrawal from exchange' transactions are on-blockchain. All buy/sell order messages are cryptographically signed by *InfraBlockchain* user accounts and 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 IPFS[17] distributed P2P storage system in a transparent and immutable manner, regularly anchoring the cryptographic proof of recent transactions handled on off-blockchain servers to the blockchain. When a user requests withdrawal of tokens, 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 trading events, and makes the hybrid system fully auditable to any external parties and fully restorable even in the event of off-chain exchange server failure. Off-chain payment channels enabling high-frequency

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

micropayments can also be implemented in a similar way using the *InfraBlockchain* hybrid technology.

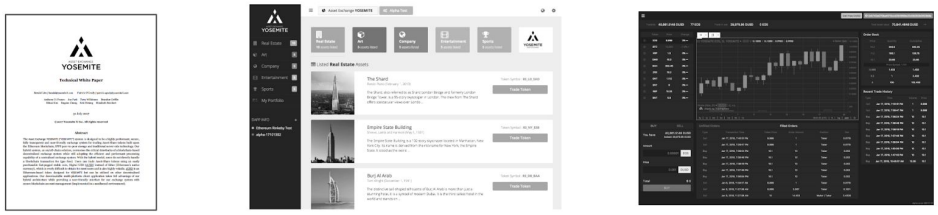

Figure 9.1 - *InfraBlockchain* hybrid exchange technology, Technical White Paper and asset/crypto exchange alpha version.

The technical white paper[18] and the working alpha system[19] of *InfraBlockchain* hybrid exchange technology were published in mid 2017. (previously named as *YOSEMITE*) The working alpha versions of asset/crypto exchange systems in Figure 8.1 were developed based on the Ethereum blockchain, but the hybrid technology can be implemented on any other blockchains including the *InfraBlockchain* Blockchain.

9.3 Scalable Multi-Blockchain Architecture

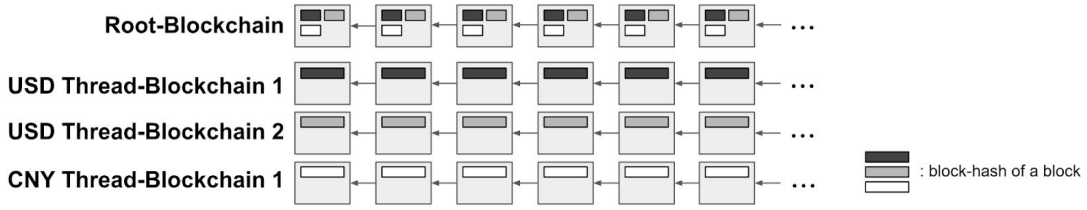

Figure 9.2 - Scalable multi-blockchain architecture with tightly coupled inter-blockchain communication

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 *InfraBlockchain*. There will be a single *Root-Blockchain* in each *InfraBlockchain* whose blocks contain the recent block-hashes of the blocks having block finality status from the multiple Thread-Blockchains running in the same *InfraBlockchain*. The *Root-Blockchain* is operated by its own block producers and acts as the inter-blockchain communication hub between the *Thread-Blockchains*. A *Thread-Blockchain* is a blockchain with its own domain-specific transaction types, *dFIAT* tokens used as basic currency

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

token in that chain, and its own blockchain consensus run by independent block producers or the same blockchain producers of the *ROOT-Blockchain*. With multiple Thread-Blockchains in a *InfraBlockchain*, each with a large capacity for blockchain transactions, a very high level of blockchain scalability (even millions of TPS) can be achieved.

10 Smart Contract Execution Environment

Instead of developing a custom-designed virtual machine and smart contract programming language such as the EVM[20] (Ethereum Virtual Machine) and Solidity[21], the *InfraBlockchain* adopts WebAssembly[22] (WASM) technology which was originally developed as the open web standard for the next generation of web browser application runtime environments. WASM, due to its fast and safe VM, has great potential to replace Javascript, currently the de-facto standard in web programming. The EOS blockchain also adopted WASM as its smart contract 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. A custom blockchain operation (action) implemented on a user-created smart contract can be charged a fixed transaction fee amount per an operation set by the elected block producers, or can be charged a dynamic transaction fee amount according to the computing resources consumed (cpu time, network bandwidth, storage space) by the custom operation. The transaction fees in the *InfraBlockchain* are always paid in the fiat-pegged stable tokens selected by the elected block producers, making DoS attacks prohibitively costly and ensuring the system's ability to resist them.

11 Optional Privacy-Protecting On-Chain Transactions

Privacy is a requirement for a viable financial system. Every fund(token)-transfer transaction of a blockchain account is transparently traceable on public blockchains. Once the identity of the blockchain account owner is revealed to the public or his/her friends, people can view the full history of the blockchain account owner's financial transactions causing privacy violation among the blockchain users. But the full privacy-protecting blockchain networks (e.g. Monero, ZCash) are discouraged by regulation because of the risk of money laundering. Privacy features can be implemented using a private blockchain network or just encrypting data on blockchain, but that approach leads to centralization issues. (Big Brother can still monitor/control all user data) Privacy-protecting token transaction features on *InfraBlockchain* are implemented

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

on-blockchain and complies with the crypto-currency travel rule regulations as much as possible. Privacy token transaction features are designed to optionally allow only small-amount token transfer transactions to be executed by the blockchain accounts for which KYC processes have gone through. As the paper fiat money system allows private cash transactions, InfraBlockchain can be set up to allow small-amount private token transactions.

Because the privacy-protecting token transactions are cryptographic-computation-intensive. *InfraBlockchain* provides built-in highly performant cryptographic operations on blockchain core for smart contract codes to utilize privacy-protecting features easily in out-of-the-box way.

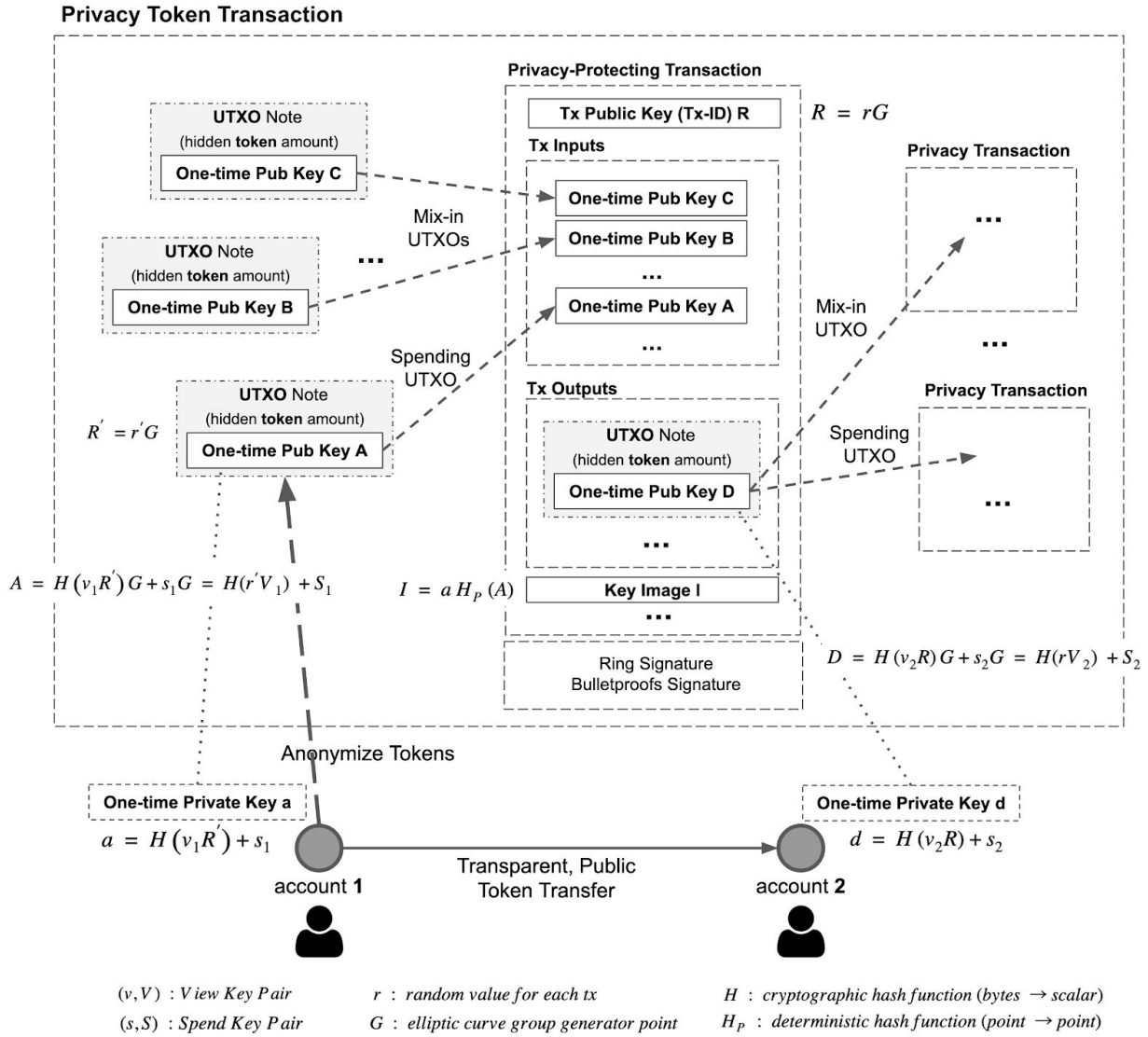

Figure 11.1 - Optional Privacy-Protecting Token Transaction Supported on *InfraBlockchain*

InfraBlockchain provides the ring-signature-based privacy token transaction technology on blockchain core software.

- UTXO(Unspent Transaction Output)-based token model for private transactions

- Using two public keys combined (View-Key, Spend-Key) as the public payee address for private transactions. The authorizations for viewing the incoming(token-receiving) private transactions and privately spending the received UTXO notes can be separate.

- One-time stealth-address using ECDH(Elliptic Curve Diffie–Hellman) key exchange technique to hide the token receiver. Each untraceable one-time public-key address is unique for each UTXO note, and only the token receiver can identify the ownership of the UTXO.

- Implementing MLSAG (Multilayered Linkable Spontaneous Anonymous Group signature) ring-signature for hiding token sender (mixing fake senders) and preventing double-spend (using linkable Key-Image)

- Small footprint Bulletproofs signature for hiding token transfer amount

- Private transaction relay to hide blockchain transaction sender consuming blockchain transaction fee. Receiving the privacy transaction message signed by the private UTXO note owners, the off-chain relay service adds its signature to the transaction message and submit transactions to *InfraBlockchain* network on behalf of the private token sender.

- secp256k1, secp256r1, ed25519, bn128 elliptic curve support

- Client wallet software (CLI, Desktop, Mobile) generating private transaction signatures and monitoring private transactions on *InfraBlockchain* network to identify incoming (token-receiving) private transactions

Privacy-protecting token transaction service of *InfraBlockchain* can be used to implement the blockchain-based full-privacy voting service. Like the payment use case, blockchain-based voting can be traceable revealing which account voted which candidate. Even though the identity of the voting account owner is not revealed to the public, the election administration agency can have a possible route to trace each voter's voting result. By using privacy-protecting token technology on a blockchain-based voting system, each voter's voting result can be fully secret. A right to vote is represented as a token on a voting smart contract which is minted and transferred from election administrator to eligible voter account. The vote-token holders can cast their votes privately to candidate accounts through the privacy-protecting token transfer transactions, not revealing their voting results to other people and even the election administration agency.