Crypto Exchange SRS

Computer Science (Anna University)

1 Scope of work

The idea is to develop Crypto based Exchange and tokens based on Ethereum(ERC 20 / ERC 721) which supports multiple Crypto currency and own coins. Exchange Wallet will be used to store all ERC20 tokens which are listed in Exchange. Users will be able to deposit / withdraw and trade supported coins or tokens with minimum trading fee or transaction charge. We will develop three layer security for our users for fund safety.

Instant trade and multiple order form supported:
Quick and fast trade matchmaking algorithm will be implemented in exchange so that the user does the trade as much as he can with a low transaction fee. Many order Form supports for creating bids as a wall as users have a number of pairs available for trade. Users are able to do the trade after initial confirmation of the deposit and there is no deposit fee but we have a deposit cap for all the coins or tokens. very minimum charge for withdrawing the coin or Tokens.

Wallet use to store all supported Coins / Tokens:
Users may not be able to send-receive tokens or ethereum to any exchanges. User only send – receive tokens or ethereum to ethereum compilable wallet. To send tokens / ethereum you just need to scan the QR code or enter the public key of the receiver and yeah your transaction is done. This transaction is hassle-free and does not require your personal information.

Users should be able to deposit/ withdraw and trade on other supported coins(BTC/ ETH/ LTC / USDT). Exchange wallet will support all wallet for deposit and withdraw crypto assets.
Exchange availability:
Our exchange will be available on Android and web , so that users use it on a system, Tab Mobile.

Instant trade Execution:
Exchange designed for instant trade execution features, unlike other cryptocurrency exchanges, our exchange is not dependent on third party wallet like Coinomi or Changelly or Shapeshift. The entire process takes place on its own network that reduces the time as compared to other wallets using third party exchanges.

Less Transaction fee:
Our wallet charges the lowest network fee or transaction fee. Many wallets claim that they charge only network fee but during the transaction through them, you need to pay high fees for the third party exchanges.
Assumption: Token will be used for paying the less transaction fee.

Security:
To ensure the safety of your assets we make use of strong encryption, non-custodial methods and advanced features that guarantee our users the highest level of security.

(IP verification/ Email Verification, SMS/ GAuth verification, Security questions, anti-phishing code)

Secure Withdrawal:
Transaction password required while withdrawing the token.

Easy KYC:
No KYC required for minimum caping of the coins / tokens for daily withdrawal. More the minimum capping withdraws required the user need to do KYC and users are able to do the KYC in very less time.

Fund Security (Non-custodial crypto wallet):
We don't keep a backup of your private keys to ensure you provide a completely decentralized crypto wallet that is safe from any type of hacks. Your assets are completely safe and secure in the non-custody environment.

Supported Coin for trade pairing :
BTC , LTC , BCH , ETH , EOS , Own Token

Listing coins depends on the algorithm provided by crypto-currency and we can list multiple coins / Tokens for trading.

1.1 Solution

Application will be developed to handle Frontend and backend operations.

- Full Node setup for wallet / Third Party wallet
- Authentication Module (Sign up / Login / Forgot)
- Deposit - Withdraw Wallet for Users
- Smart Contract for Token Generations
- Trade Engine
- Coin / Token Listing
- Advertisement Setup of ICO / STO
- Security Setup
- KYC
- Referral management
- Admin Controllers
- Hot wallet (Deposit)
- Warm Wallet (Withdraw)
- Cold Wallet
- White Paper
- Roadmap
- Token Distribution
- Fee setup

1.2 Modules and Features

1.2.1 Full Node Setup

- Full node setup to connect with genesis
- Block generations
- Generating Address

Authentication Module
Sign Up / Login
Forgot / Reset Password
IP validation while Login
2 factor authentication while Login (If enable)

1.2.1.1 Deposit - Withdraw wallet for User Wallet

- Send and receive tokens or coin
- Store Tokens or Ethereum
- Deposit and Withdraw coin or token

1.2.1.2 Smart Contract

- Number of Token development according to requirement
- Token distribution
- User can read the verified code of smart contract for fundamental work based on ERC20 (fungible token) and Nobel token based on ERC721 (Non- fungible token). User will get more Flexibility to use this token.

Security Setup
security for user verification fund security

1. SMS verification /IP whitelisting/ Email verification
2. Anti-fishing verification
3. Security Question verification while withdraw the token or amount
4. Transactional password
5. KYC

-

1.2.1.3 Admin

- Manage token distribution
- Manage Cold wallet for fund security
- KYC management of user
- Fund management

- User management

Trade Engine
1.Coin pairing
2. Order creation
3. Trade execution based on bid
4. Matchmaking algorithm
5. Trade History
6. Order history
7. Manage Order Forms
8. Trading cap based on user authentication
9. Trade TPS
10. Live price of the coins

Token Listing
Listing documentation for ICO / STO
Listing Token mechanism
Wallet setup for new listed token
Deposit and withdrawal management for tokens

Hot wallet(deposit)
When User do the deposit then every coin has a separate wallet for deposit only.

Warm Wallet(Withdrawal)
When User needs to withdraw the coin outside of the exchange then a warm wallet comes into the picture.

1.2.1.4 COLD WALLET

- When wallet reach threshold then admin got notification to plug in Ledger (Cold wallet) for fund safety.

WHITEPAPER

- We will create whitepaper according to concept and explain token behavior and functionality. We create whitepaper according to governance guidelines.

1.2.1.5 ROADMAP

- Progress plan of the exchange

Referral mangement

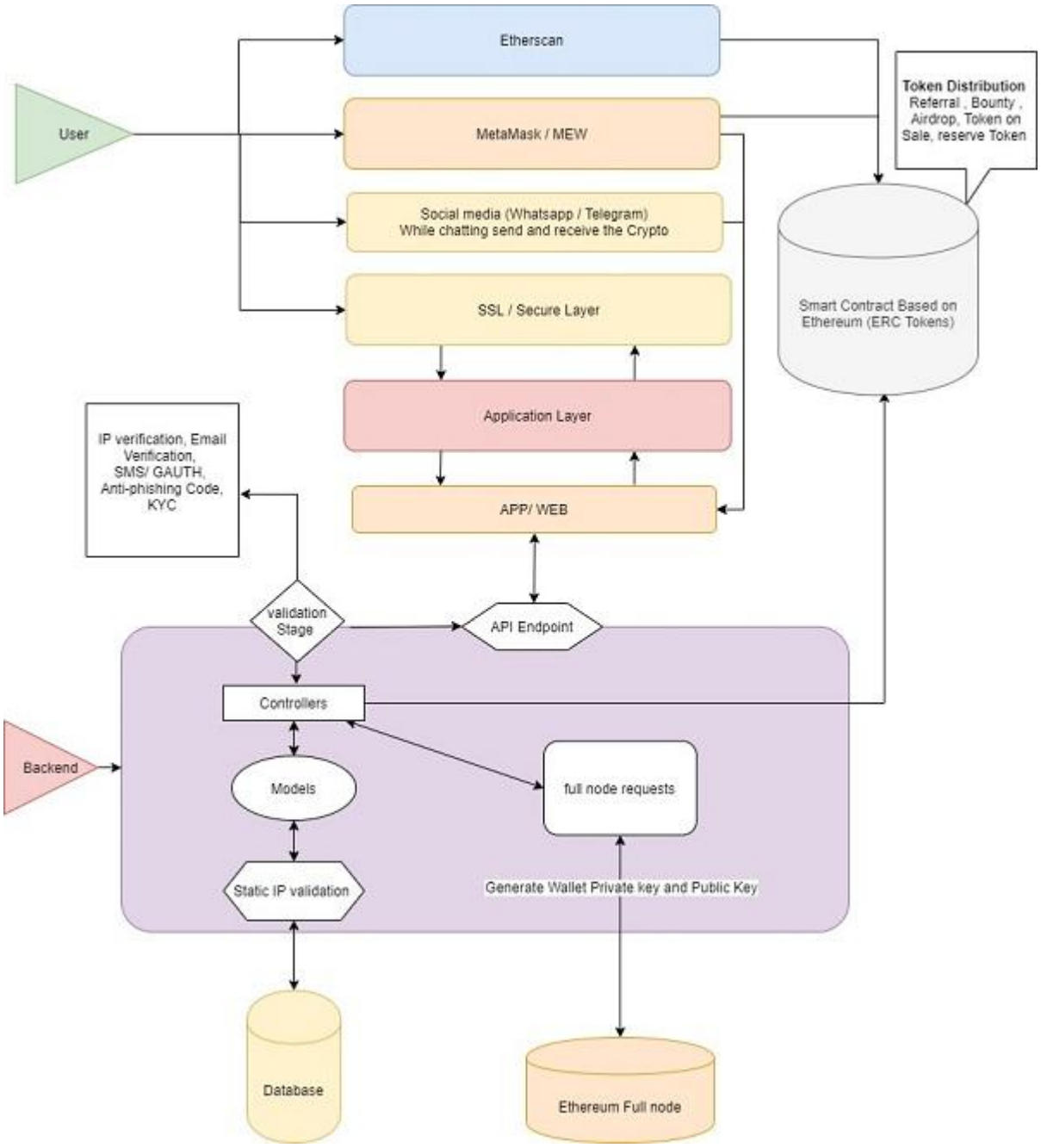
- User will get Sign up bonus tokens, Airdrop, Bug bounty, bounty, Social media promoter, User to user referrals.

2 TECHNOLOGY STACK

Below are the details of the **technology stack** that we propose for the solution:

Technology	Go, Solidity, NodeJS, Python
Framework	Express , Django
Mobile App	Android (Java or Kotlin)
Database	MongoDB, PostgreSQL
Frontend	HTML5, CSS3
Frontend Framework	Bootstrap

2.1 Architecture flow diagram



Explanation of Technical Architecture Flow Diagram

- Users will read the verified smart contract though etherscan. When the user will buy the token then the token will automatically transfer to the same ethereum address of the user (It should be an ethereum compatible wallet).As well as User can buy the token from

exchange. All user transactional records will be stored in our database. According to the smart contract, users will get a referral token, Bounty, bug bounty, etc.

- Users will use any third party wallet to deposit or withdraw all coins / Tokens which is supported over the exchange .
- SSL & Secure Layer User: A global standard security technology that enables encrypted communication between a web browser and a web server.
- When a user accesses the exchange(web / app), all requests and responses come through API endpoints.
    - On registration - Email and IP validation will be required.
    - On login - GAuth or SMS Auth will be required (If it is enabled)
    - For avoiding the fake mails user can enable Anti-Phishing Code
    - On transaction transaction-password will be required (If enable)
- All the requests will be getting responses through the controller (request, response) . We are using a segmented controller for real-time operation.
- Users have to do the simple KYC for fund security after the KYC user is able to get all the referral benefits (Like airdrop, Bounty).
- Separate trade engine will be implemented for executing the Bids(Orders) and fetching the live price from exchange. Matchmaking algorithm is responsible for every order execution.
- Separate Wallet we are using for providing instant response for deposit(HOT wallet) and withdrawal(Warm wallet). For fund safety, every coin we will set up a separate wallet for deposit and withdrawal.
- Hot wallet and cold wallet treach the threshold level then the fund is transferred to the cold wallet.
- Users will get a crypto address instantly.
    - When a user requests a Crypto address then it will come through the controller and call a full node for generating private and public keys for the user (No third party involved).
- Database models will be used for scalability and fast response.
- To send crypto users just need to scan the QR code or enter the public key (Crypto Address) of the receiver to complete the transaction.
- For the connection between database and backend static IP will be used to avoid any kind of security breach.
- All the records will be stored and fetched through the database.

3 Milestone & Deliverables

The total duration of the project will be approximately 3.5 months including UAT testing. Major milestones have been explained below.

Milestone Number	Milestone Details	Tentative Delivery Timeline (Week Number)
Milestone 1	Backend: Full Node setup, Private and Public key setup	End of Week 2
Milestone 2	Website & App(Android : User authentication, KYC , Security settings, Referral, Roadmap	End of Week 4
Milestone 3	Deposit - withdraw wallet setup for every coin and own Coin.	End of Week 8
Milestone 4	Trade Engine (match making algo, Order Details, Trade history, Order History, Fee management,) Listing other coins/tokens on the exchange	End of week 14
Milestone 5	Backend(Admin): Dashboard, Manage wallet, Manage User, Manage KYC	End of Week 17
Milestone 6	Backend : Smart contract	End of Week 19
Milestone 7	UAT Testing	End of Week 22