aeries BLOCKCHAIN CORPORATION

Building Blockchain Enterprise Solutions

Rahul Golash
Chief Blockchain Architect

13th June, 2018

Content

1 About ‘Aeries Blockchain Corporation’

2 Our Offerings

3 Technology Stack

4 BAeTH Blockchain Solution

5 How to take MVP to Production

- 5.1 Upgradable Contracts
- 5.2 Non Functional Requirement Considerations
- 5.3 Deployment and Administration

6 BAeTH App Screenshots

7 Q&A

About Aeries Blockchain Corporation

Business Profile

Aeries Blockchain Corporation (ABC) is a Blockchain focused technology company. ABC's senior leadership has held key positions in corporates like IBM, Oracle, HP, Broadridge, Siemens, & CA,

Headquartered in US with a global development centre in Bangalore, India.

Focused in providing Blockchain consulting and development services to ISVs, SaaS, Medium and large Enterprises.

Value Proposition

ABC has developed Blockchain based accelerator framework which enable us to quickly build secure and scalable solutions faster.

ABC empowers businesses to digitise your transaction workflow through a highly secured, shared and replicated ledger.

Experienced in delivering Smart Contract, Crypto token based financial derivatives, Supply Chain, eKYC & Digital Signature.

Our Offerings - Service Portfolio

What we do

Partner with customer towards their business goals:

- DApp Development, Testing and Support on private and public blockchain
- Decentralised exchange protocol development on Crypto currencies
- Ethereum and Hyperledger Fabric
- ICO crypto tokens

Smart Contract

DApp

ICO

Enterprise Solutions

Our Offerings - Smart Solutions

What we do

Leverage blockchain capability to Improve:

- Supply Chain Traceability
- Transaction and Verification
- Process Efficiency
- Transparency

Smart Credentials

Smart Logistic

Smart Procurement

Smart Underwriting

Technologies Stack

Distributed Ledgers	ETHEREUM HYPERLEDGER
Languages	ANGULAR Solidity TRUFFLE node JS python™
Frameworks	remix uport oraclize METAMASK 0x INFURA
CI/CD	docker CHEF™ CODE CAN Jenkins
NO SQL/ Storage	cassandra mongoDB Couchbase IPFS GridFS

BAeTH Blockchain Solution

Personal Instant Loan App on Blockchain

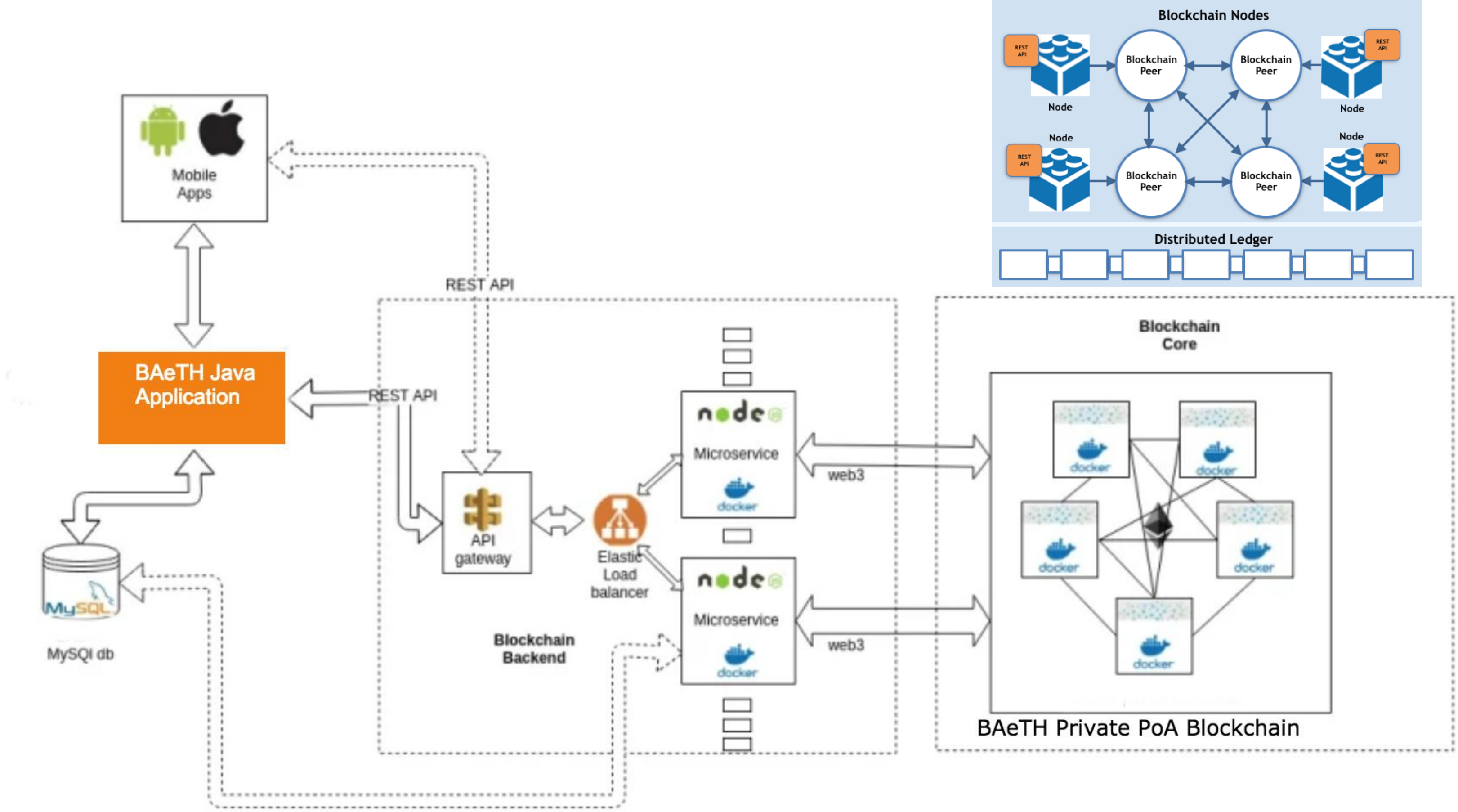
Executive Summary

- BAeTH is the masked project name of an Global fin-tech company which has instant personal mobile app for millennials.
- $50m total loans lent and repaid with 127,000 total no of loans
- Client wants to implement Distributed Ledger (Blockchain) enabled Digital Tokens using Smart Contracts on its lending platform
- Smart Contract based Distributed Ledger records all lending transactions in an open and transparent manner, thus allowing BAeTH and the borrower to execute a trusted lending transaction that is transparent and tamper proof.
- ABC is building and productionizing BAeTH Blockchain Solution.

BAeTH Blockchain Solution - Salient Points

- Open source Ethereum platform (latest release) with solidity, web3 as core-tech stack
- Private testnet and mainnet will be used for blockchain network
- Proof of Authority - PoA used for blockchain consensus mechanism
- Each user, merchant, bank, admin (/operators) will be given blockchain account
- ERC 20/223 standards to use for BAeTH tokens
- Mapping of loans and funds to actual token values
- Implement multi-sig wallet for collateral lock-in
- Blockchain Indexed log events to support **User, Merchant, Bank** wise filter

BAeTH Blockchain Solution Architecture



BAeTH Blockchain Solution - Proposed Entities

Microservice - Node.js, Front end + web3

- User login
- Banks
- Regulators
- Credit Rating Agency
- Administrator’s operations & reporting console

Nodes

- BAeTH Core nodes
- Banks
- Merchants
- Regulators
- Credit Rating Agency

Roles

- User
- Banks
- Merchants
- Regulators
- Credit Rating Agency

Data

- Token(s)
- Loan
- User Profile & eKYC
- User interactions

Used Technology Stack

Distributed Ledgers	ETHEREUM
Languages	ANGULAR Solidity TRUFFLE node JS python™
Frameworks	remix uport MyEtherWallet METAMASK INFURA
CI/CD	docker CHEF™ CODE CAN amazon web services Jenkins
NO SQL/ Storage	mongoDB Couchbase

How to take MVP to Production

Core Considerations

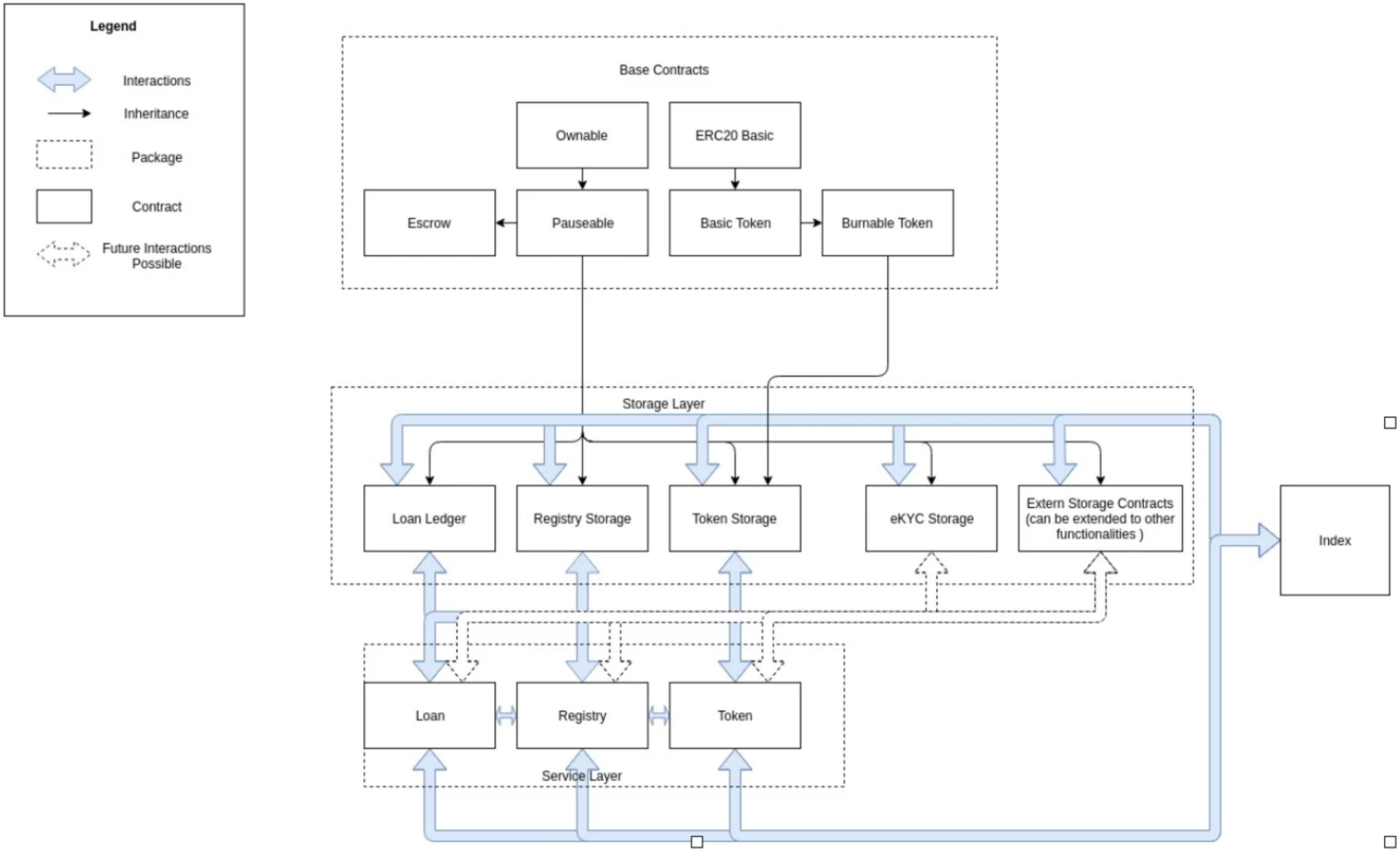
- Right Consensus Mechanism e.g. choice between PoW, PoS, PoA
- Upgradable Contracts
- Follow Solidity/Ethereum Coding Best Practices
- Follow Engineering best practices e.g.
  - Code Repo & BugTracking Tool
  - CI/CD Pipeline
  - Docker/Swarm setup
  - Deployment in scalable and secured environment
- Non Functional Requirement e.g.
  - Security,
  - Scalability,
  - Performance and
  - Robustness

Why choose Proof of Authority - PoA?

- Suitable for all private blockchain
- Transactions and blocks are validated by approved accounts, known as validators or sealers
- Validators identity is approved ahead of time and hence allow only selected (authorised) nodes to join network
- No need to mining incentive
- Manage consensus with more than one authorized node
- Signer can sign at most one of a number of consecutive blocks (floor(SIGNER_COUNT / 2) + 1).
- The same consensus is applied when an authority node is removed from the network.
- Each banker will have one blockchain account

Upgradable Contracts

BAeTH Upgradable Smart Contracts



Upgradable Contracts – Best Practices

- Ethereum contracts are immutable so once deployed, can not be changed
- Contract Registry - Smart contract that assembles all other contracts we use
- Contract Manager - Smart contract enables us to not hardcode the address and look for registry before each function call
- Each contract will have a Storage-Implementation (Library) design to separate data from logic
- Managing data migration in chunk
- Index will maintain the latest version of each smart contract
- Use libraries to encapsulate logic

Solidity/Ethereum Coding Best Practices

Followed the best practices of security & solidity code from https://consensys.github.io/smart-contract-best-practices/

- **Race Conditions** – This can result into major bug and result into DAO's collapse.
- **Reentrancy** – This can result into different invocations of the function to interact in destructive ways.
- **Cross-function Race Conditions** – This is similar to race conditions using two functions that share the same state.
- **Transaction-Ordering Dependence (TOD) / Front Running -** Can be avoided using batch transaction or pre-commit
- **Timestamp Dependence -** Business logic based on Timestamp should be carefully considered, since a node can change the local timestamp.
- **Integer Overflow and Underflow -** Smaller data-types like uint8, uint16, uint24...etc: can even more easily hit their maximum value, there are around 20 cases for overflow and underflow.
- **DoS with (Unexpected) revert and DoS with Block Gas Limit**
- **Token loss** due to contract misbehaviour
- **Availability loss:** external contracts e.g. regulators can not interact with the token contract due to its errors

Non Functional Requirement

Non Functional Requirements - (1/3)

Security

- All communications of mobile to BAeTH backend to BAeTH microservice using HTTPS (TLS 1.2) with a Level 3 SSL certificate
- The entire system is hosted within AWS cloud infrastructure with microservice API access only from whitelisted IPAddress and port control using EC2 security group.
- Application Seed and Customer Seed

Performance

- Asynchronous by design so as to allow maximum number of operations to take place including logging operations
- Using compiled libraries for encrypt/decrypt operations
- Using inbuilt libraries to perform tasks as opposed to using an external module
- Using HTTP 2.x (if required)
- Using Cluster module to make the Node.JS application use more than one core if available

Non Functional Requirements - (2/3)

Scalability

- The node application is deployed using Docker containers making the application horizontally scalable.
- Packages like PM2 also allow node applications to run on clusters while having an inbuilt load balancer to control number of instances.
- Using PoA as the consensus algorithm to **increase block times**.
- Increasing the block gas limit to facilitate more transactions per block

Non Functional Requirements - (3/3)

Highlighted Geth commands options which are used:

--datadir : Points to the data directory for storing ethereum data
--port : tells geth to use the port provided for inter node communication
--rpc : to enable the rpc communication with Web3.JS
--rpcaddr : allows to set the address on which the client will listen
--rpcport : The port on which the client rpc will run
--rpcapi 'personal,eth,web3,' : restricts the exposure to web3 and eth
--networkid : custom network id
--gasprice '1' : limit the minimum gas price to decrease number of ether spent
--unlock : optional unlock of the coinbase account
--password : password for the coinbase account
--mine : start mining
--**targetgaslimit** 90000000: increases the number of transactions capable in a block
console "*" : enable the console interface to make admin changes
--nodiscover : disable peer discovery (adding peers manually the first time)
--rpccorsdomain : limit the usage of RPC to a particular ip/domain
--ws : enable the web socket interface to receive events faster
--**wsorigins** : set the web socket domain to control access

Additional - Clique block ‘**period**’ - 1 sec and ‘**epoch**’ being the default value

Deployment and Administration

CI/CD Pipeline

- Bitbucket tools for code repo

Static Analysis:

- **Mythril** - Reversing and bug hunting framework for the Ethereum blockchain
- **Oyente** - Analyze Ethereum code to find common vulnerabilities, based on this paper.

Test Coverage

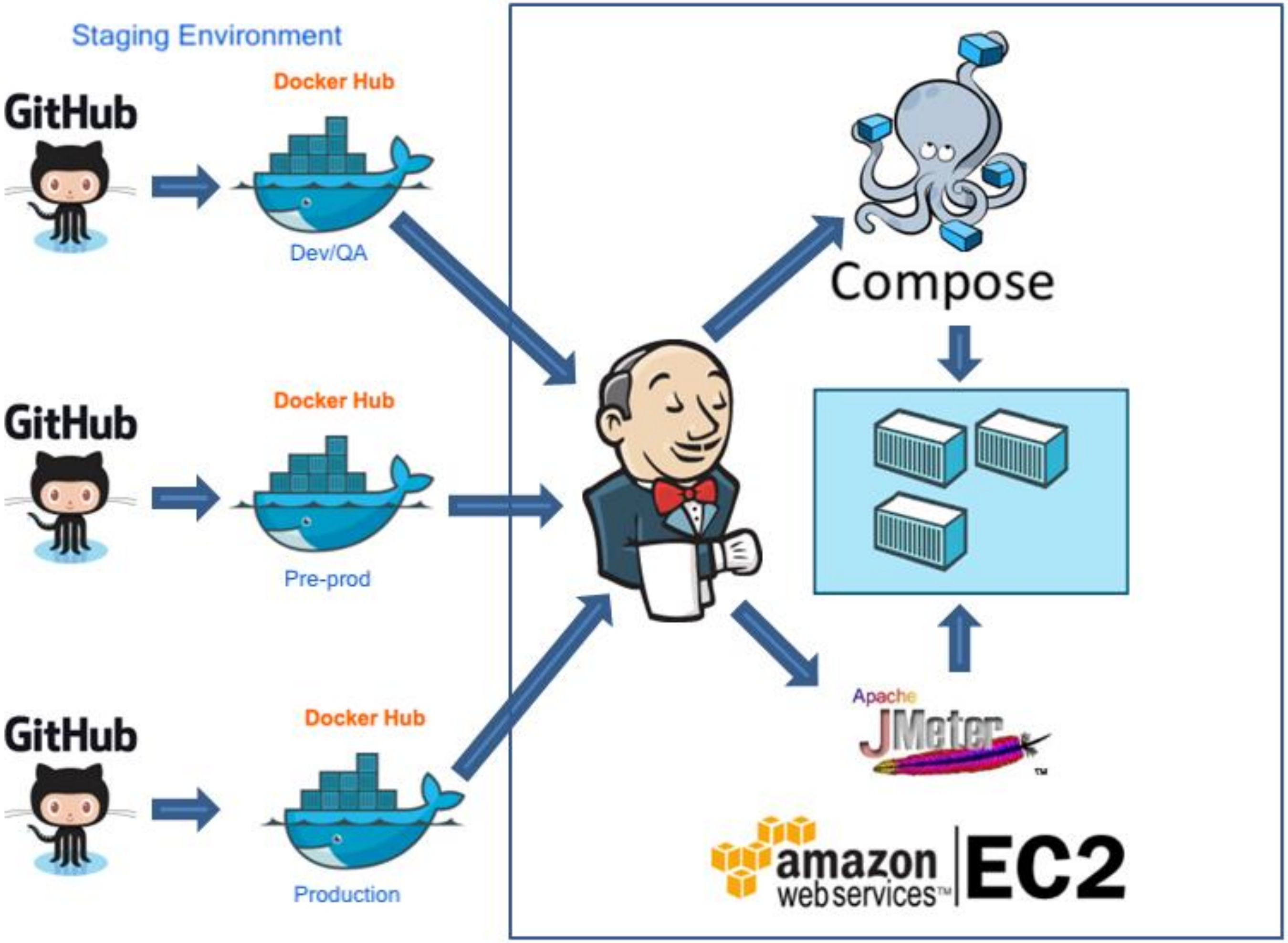
- Solidity-coverage - Code coverage for Solidity testing.

Linters

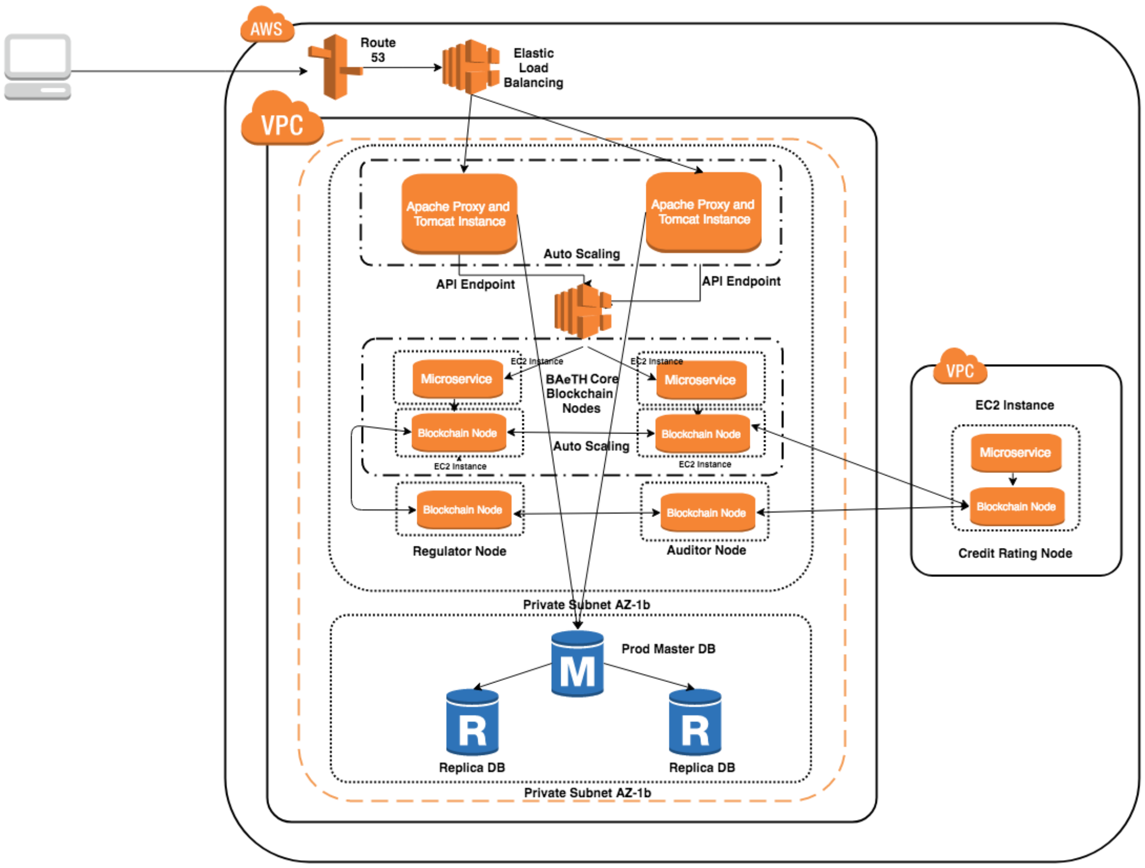
Linters improve code quality by enforcing rules for style and composition, making code easier to read and review.

- **Solint** - Solidity linting that helps you enforce consistent conventions and avoid errors in your Solidity smart-contracts.
- **Solium** - Yet another Solidity linting.
- **Solhint** - A linter for Solidity that provides both Security and Style Guide validations.

Deployment Staging Environment



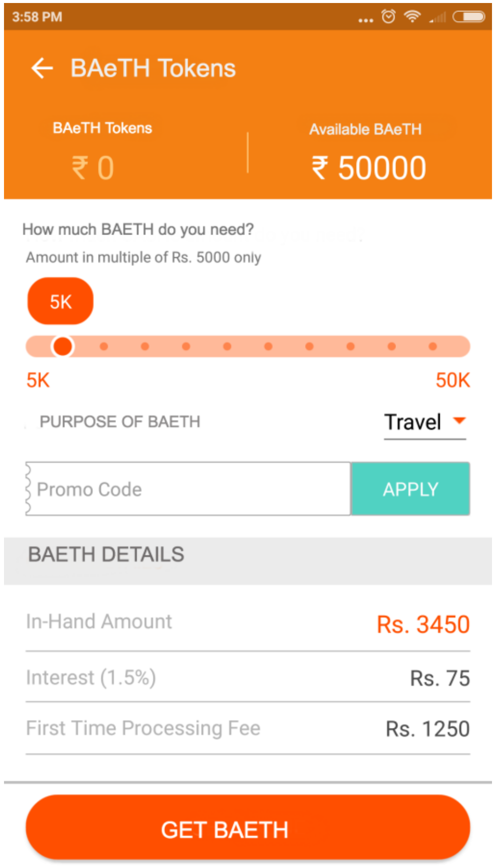
BAeTH AWS Deployment



- One Elastic Load Balancer
- Two instances of micro-services under autoscaling group
- Credit Rating Node on different VPC
- Regulator and Auditor Nodes on the same private subnet

BAeTH App Screenshots

Apply Loans and Award BAeTH Tokens



3:58 PM

← BAeTH Tokens

BAeTH Tokens	Available BAeTH
₹ 0	₹ 50000

How much BAETH do you need?

Amount in multiple of Rs. 5000 only

5K

5K 50K

PURPOSE OF BAETH Travel

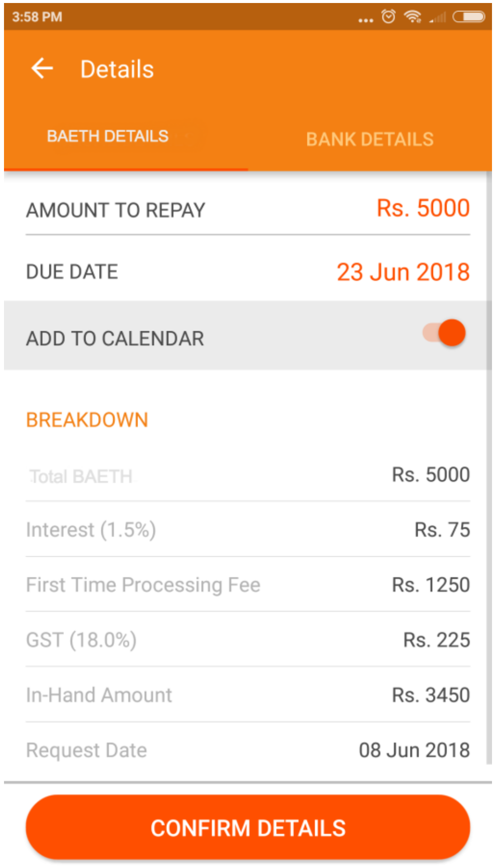
Promo Code APPLY

BAETH DETAILS

In-Hand Amount	Rs. 3450
Interest (1.5%)	Rs. 75
First Time Processing Fee	Rs. 1250

GET BAETH

User has 0 tokens and no loan



3:58 PM

← Details

BAETH DETAILS BANK DETAILS

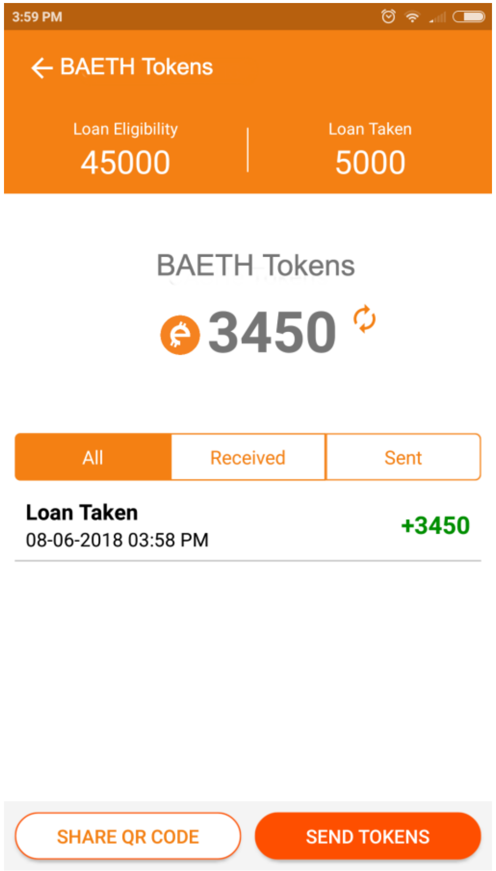
AMOUNT TO REPAY	Rs. 5000
DUE DATE	23 Jun 2018
ADD TO CALENDAR	●

BREAKDOWN

Total BAETH	Rs. 5000
Interest (1.5%)	Rs. 75
First Time Processing Fee	Rs. 1250
GST (18.0%)	Rs. 225
In-Hand Amount	Rs. 3450
Request Date	08 Jun 2018

CONFIRM DETAILS

User asks loan of INR 5000



3:59 PM

← BAETH Tokens

Loan Eligibility	Loan Taken
45000	5000

BAETH Tokens

3450

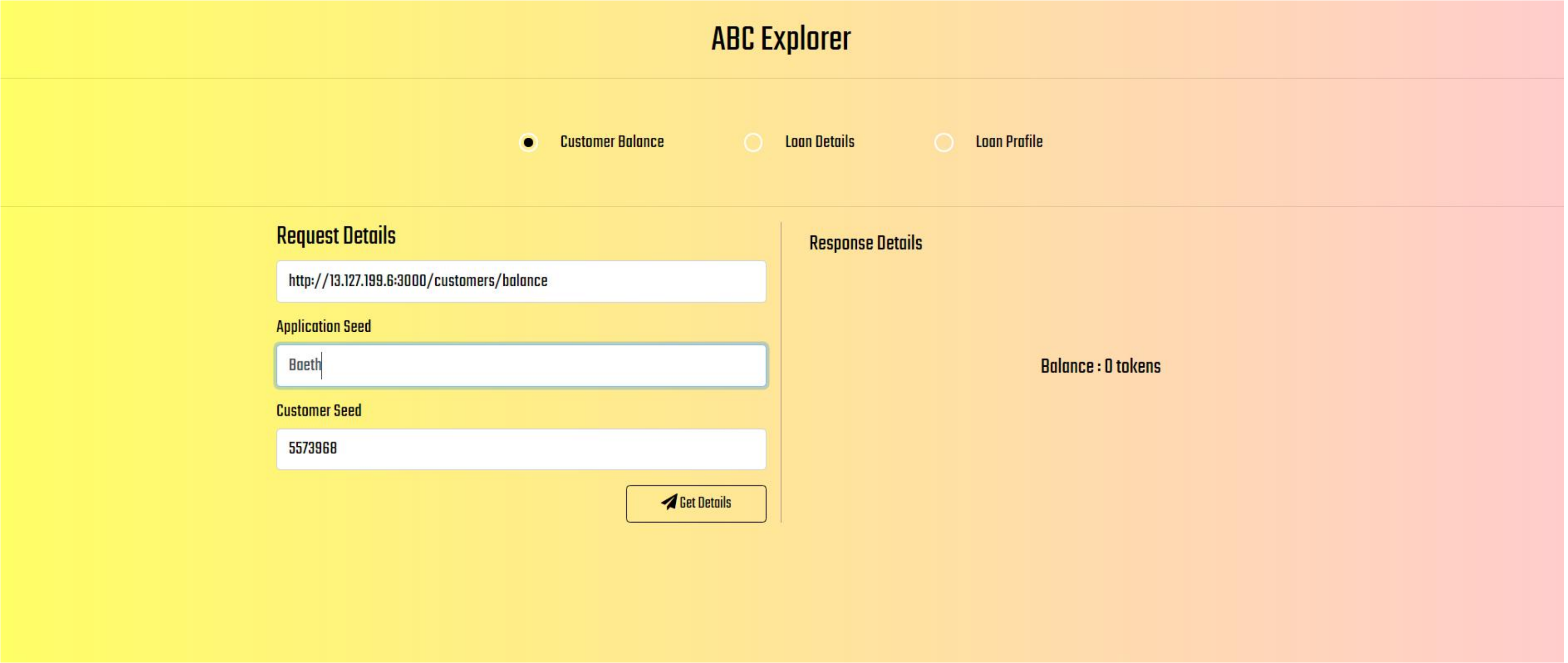
All Received Sent

Loan Taken 08-06-2018 03:58 PM	+3450

SHARE QR CODE SEND TOKENS

3450 BAeTH tokens in Wallet

Apply Loans and Award BAeTH Tokens



ABC Explorer

● Customer Balance ○ Loan Details ○ Loan Profile

Request Details

http://13.127.199.6:3000/customers/balance

Application Seed: Baeth

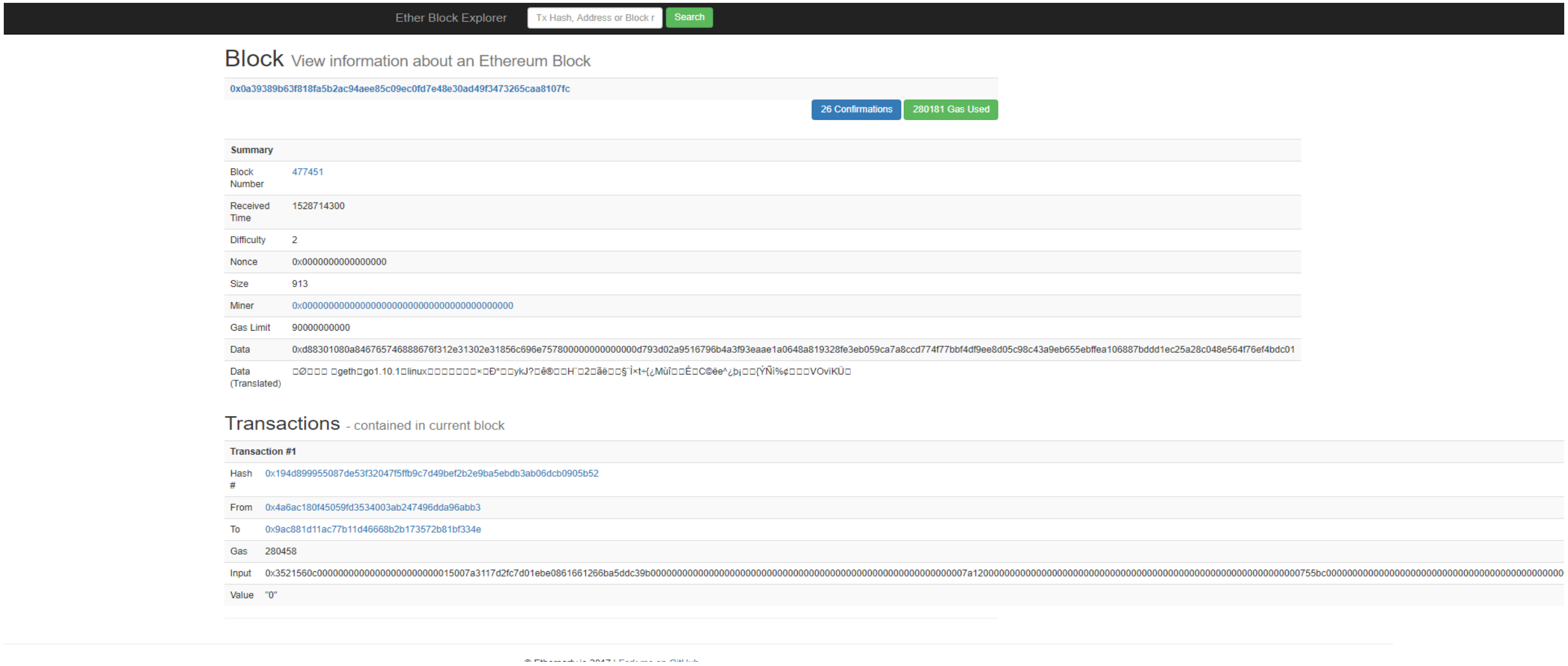
Customer Seed: 5573968

Response Details

Balance : 0 tokens

Stage 0 - User has 0 tokens in the wallet

Apply Loans and Award BAeTH Tokens



Block View information about an Ethereum Block

0x0a39389b63f818fa5b2ac94aee85c09ec0fd7e48e30ad49f3473265caa8107fc

26 Confirmations | 280181 Gas Used

Summary	
Block Number	477451
Received Time	1528714300
Difficulty	2
Nonce	0x0000000000000000
Size	913
Miner	0x0000000000000000000000000000000000000000
Gas Limit	90000000000
Data	0xd88301080a846765746888676f312e31302e31856c696e757800000000000000000d793d02a9516796b4a3f93eaae1a0648a819328fe3eb059ca7a8ccd774f77bbf4df9ee8d05c98c43a9eb655ebffea106887bddd1ec25a28c048e564f76ef4bdc01
Data (Translated)	□Ø□□□ □geth□go1.10.1□linux□□□□□□□×□Ð*□□ykJ?□ê®□□H¨□2□ãë□□§¨Ì×t÷{¿Mùî□□É□C©ëe^¿þ¡□□{ÝÑì%¢□□□VOvïKÜ□

Transactions - contained in current block

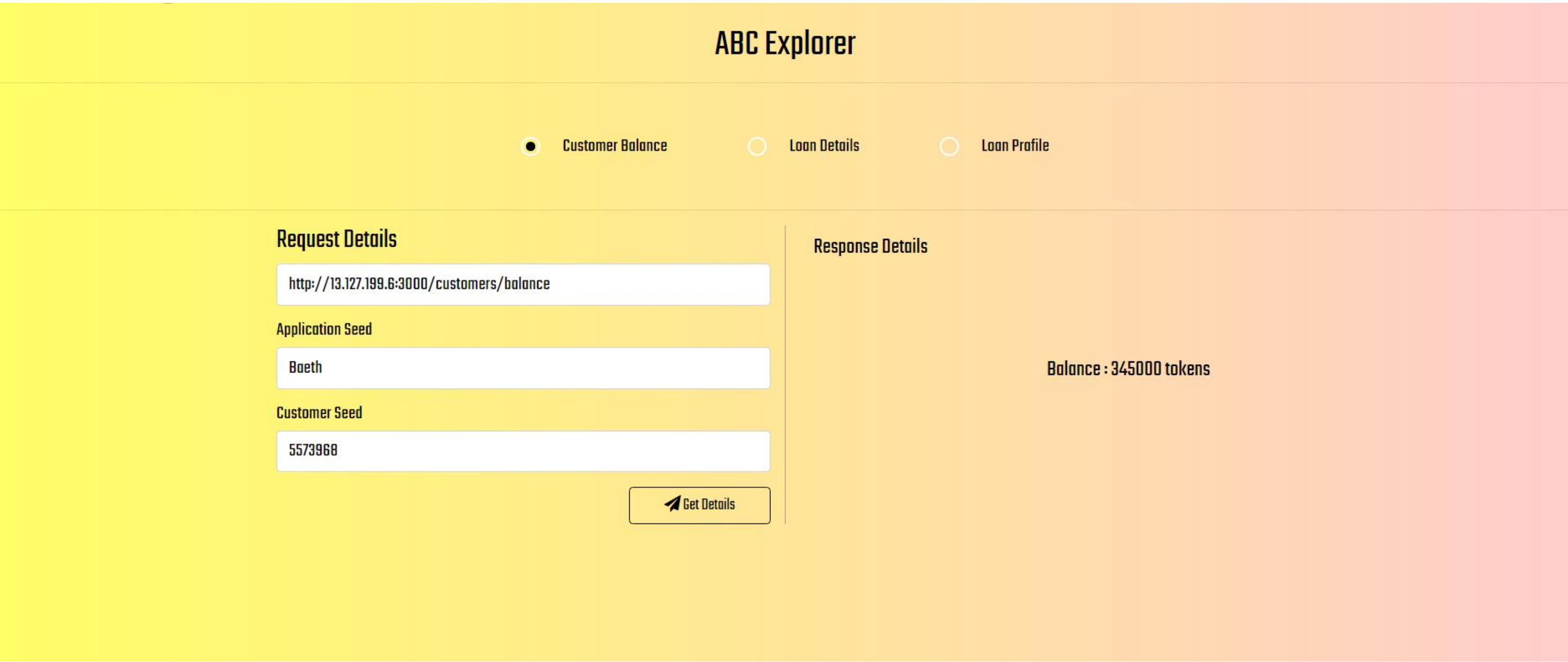
Transaction #1	
Hash #	0x194d899955087de53f32047f5ffb9c7d49bef2b2e9ba5ebdb3ab06dcb0905b52
From	0x4a6ac180f45059fd3534003ab247496dda96abb3
To	0x9ac881d11ac77b11d46668b2b173572b81bf334e
Gas	280458
Input	0x3521560c00000000000000000000000015007a3117d2fc7d01ebe0861661266ba5ddc39b0000000000000000000000000000000000000000000000000000000000007a1200000000000000000000000000000000000000000000000000000000000755bc00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Value	"0"

© Ethernart.io 2017 | Fork me on GitHub

```
0x3521560c000000000000000000000000015007a3117d2fc7d01ebe0861661266ba5ddc39b
0000000000000000000000000000000000000000000000000000000000007a12   <-- 500000 Loan Applied
000000000000000000000000000000000000000000000000000000000000000543A8 <-- 345000 Disbursed Amount
0000000000000000000000000000000000000000000000000000000000000000f  <-- 15 day loan
0000000000000000000000000000000000000000000000000000000000044AA20  <-- 4500000 Eligibility
0000000000000000000000000000000000000000000000000000000000098b692  <-- LoanId
```

Transaction shown in EthExplorer

Apply Loans and Award BAeTH Tokens



ABC Explorer

● Customer Balance ○ Loan Details ○ Loan Profile

Request Details

http://13.127.199.6:3000/customers/balance

Application Seed

Baeth

Customer Seed

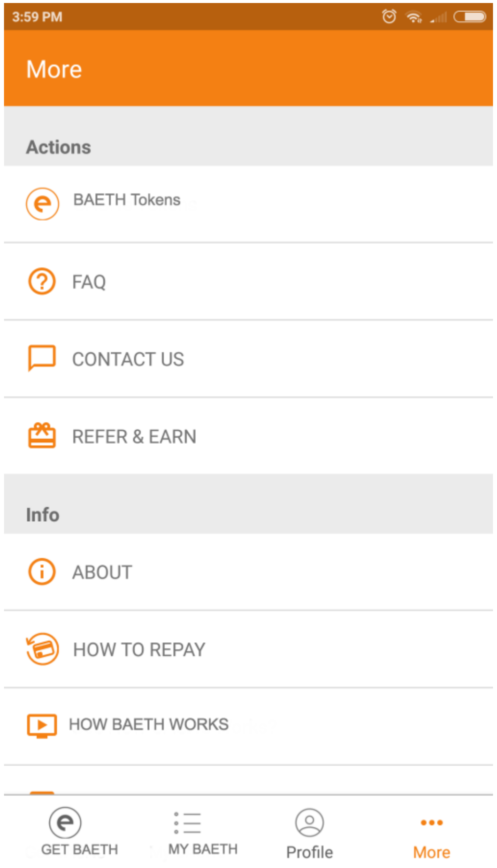
5573968

Response Details

Balance : 345000 tokens

Stage 1 - User has 3450(00) tokens in the wallet

Transfer BAeTH Tokens to a friend



3:59 PM

More

Actions

BAETH Tokens

FAQ

CONTACT US

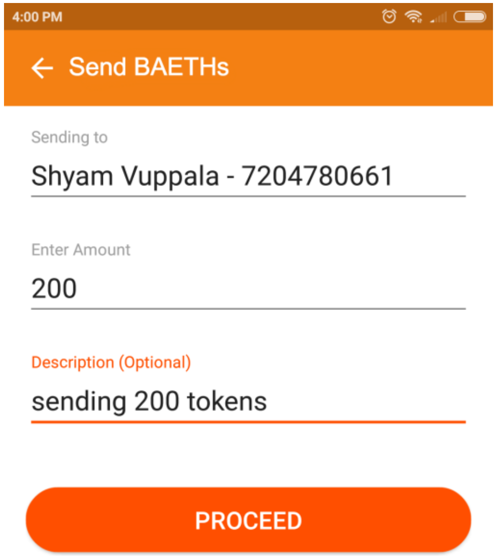
REFER & EARN

Info

ABOUT

HOW TO REPAY

HOW BAETH WORKS



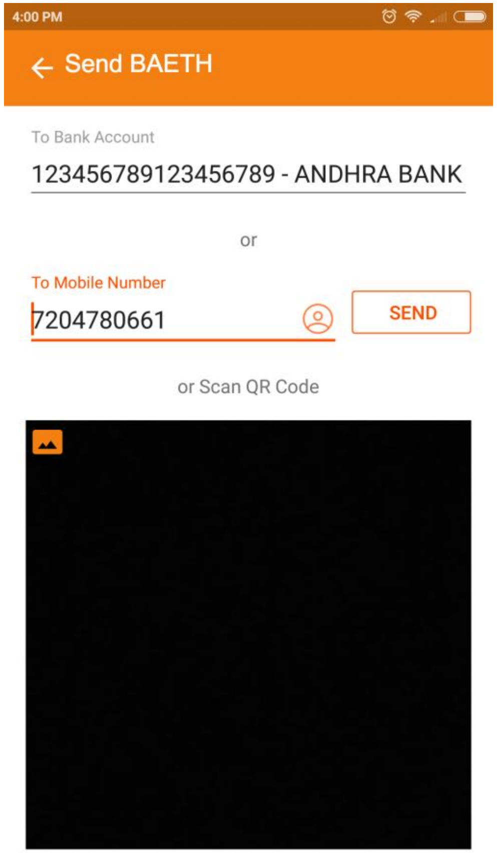
4:00 PM

Send BAETHs

Sending to
Shyam Vuppala - 7204780661

Enter Amount
200

Description (Optional)
sending 200 tokens



4:00 PM

Send BAETH

To Bank Account
123456789123456789 - ANDHRA BANK

or

To Mobile Number
7204780661

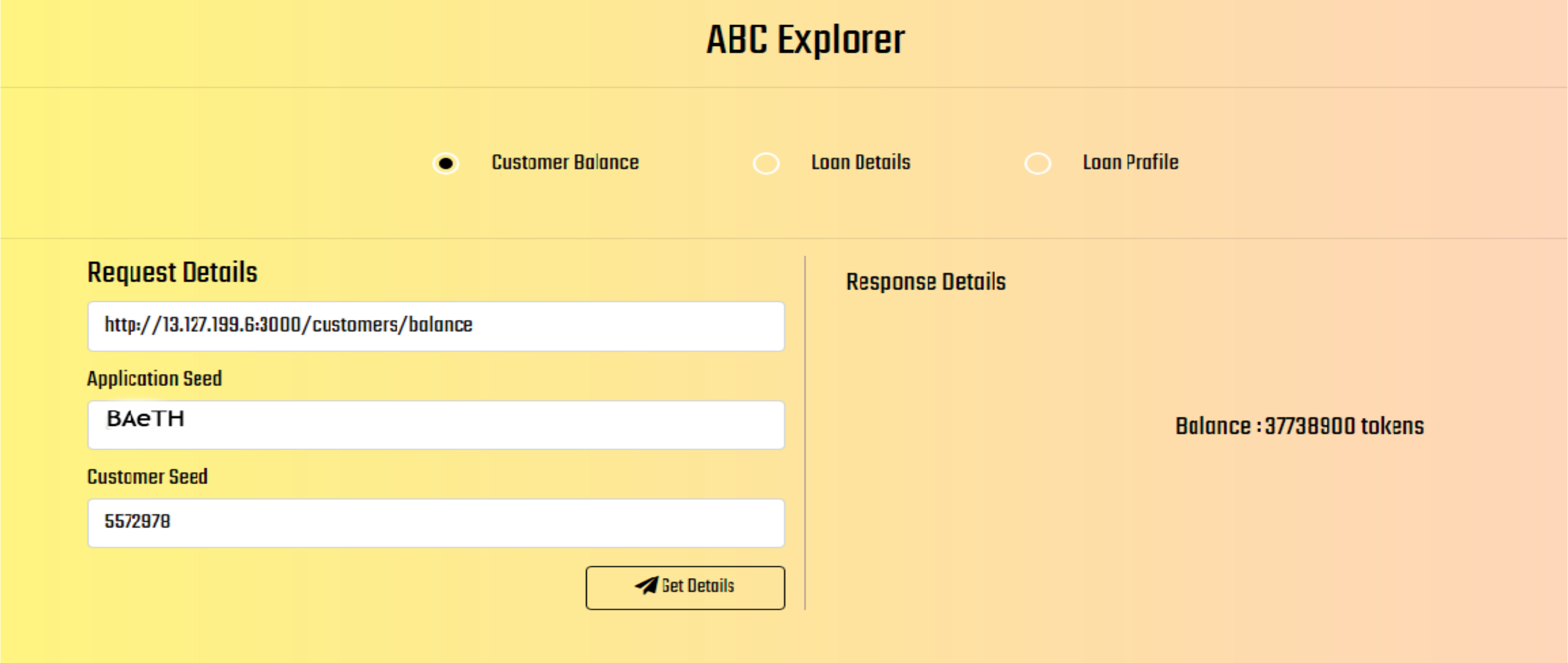
or Scan QR Code

User screen

User to transfers 200 BAeTH

User enters the details of recipient

Transfer BAeTH Tokens to a friend



ABC Explorer

● Customer Balance ○ Loan Details ○ Loan Profile

Request Details

http://13.127.199.6:3000/customers/balance

Application Seed

BAeTH

Customer Seed

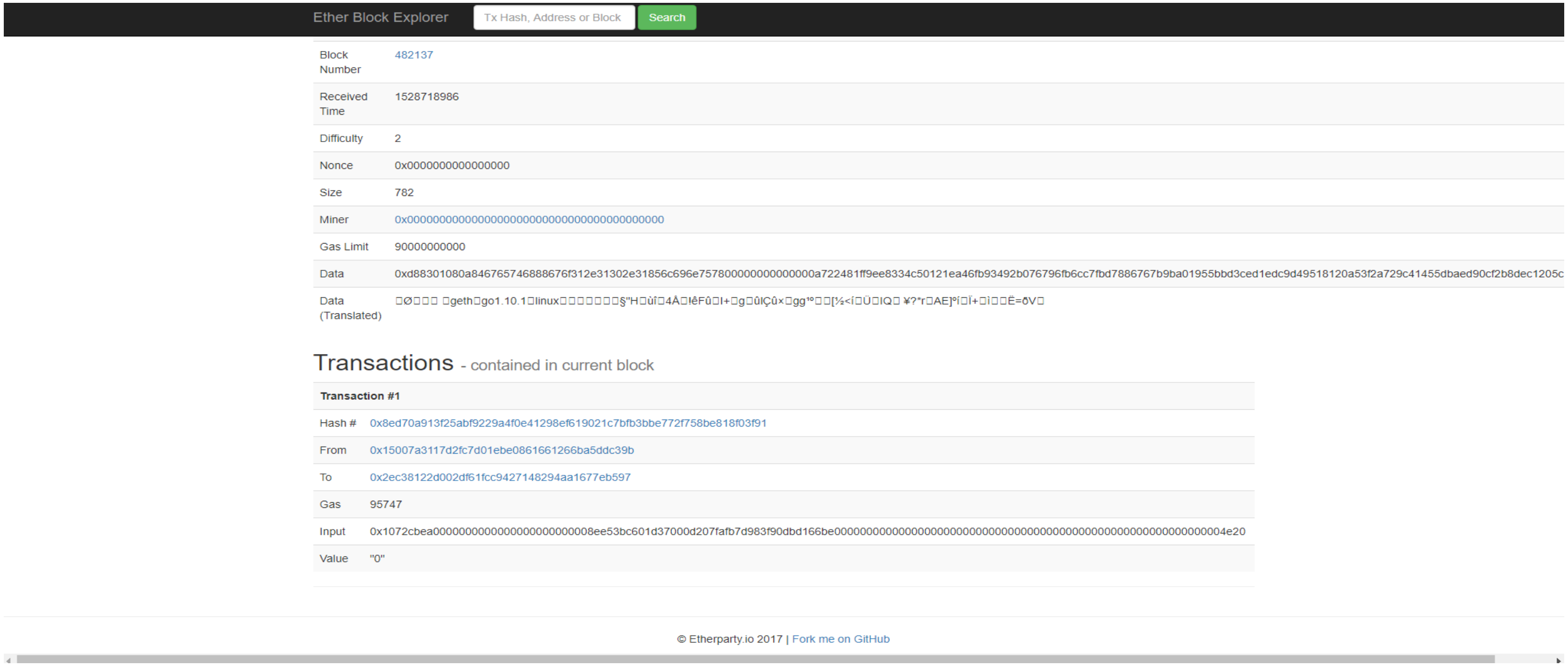
5572978

Response Details

Balance : 37738900 tokens

Stage 0 - Recipient has 377389(00) tokens in the wallet

Transfer BAeTH Tokens to a friend

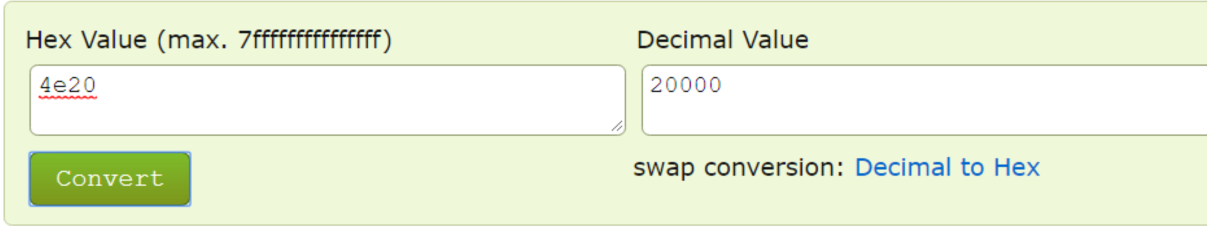


Block Number	482137
Received Time	1528718986
Difficulty	2
Nonce	0x0000000000000000
Size	782
Miner	0x0000000000000000000000000000000000000000
Gas Limit	90000000000
Data	0xd88301080a846765746888676f312e31302e31856c696e757800000000000000a722481ff9ee8334c50121ea46fb93492b076796fb6cc7fbd7886767b9ba01955bbd3ced1edc9d49518120a53f2a729c41455dbaed90cf2b8dec1205c
Data (Translated)	□Ø□□□ □geth□go1.10.1□linux□□□□□□□§"H□ùî□4Â□!êFû□I+□g□ûlÇû×□gg¹º□□[½<í□Ü□IQ□ ¥?*r□AE]ºí□Ï+□ì□□Ë=ðV□

Transactions - contained in current block

Transaction #1	
Hash #	0x8ed70a913f25abf9229a4f0e41298ef619021c7bfb3bbe772f758be818f03f91
From	0x15007a3117d2fc7d01ebe0861661266ba5ddc39b
To	0x2ec38122d002df61fcc9427148294aa1677eb597
Gas	95747
Input	0x1072cbea0000000000000000000000008ee53bc601d37000d207fafb7d983f90dbd166be0000000000000000000000000000000000000000000000000000000000004e20
Value	"0"

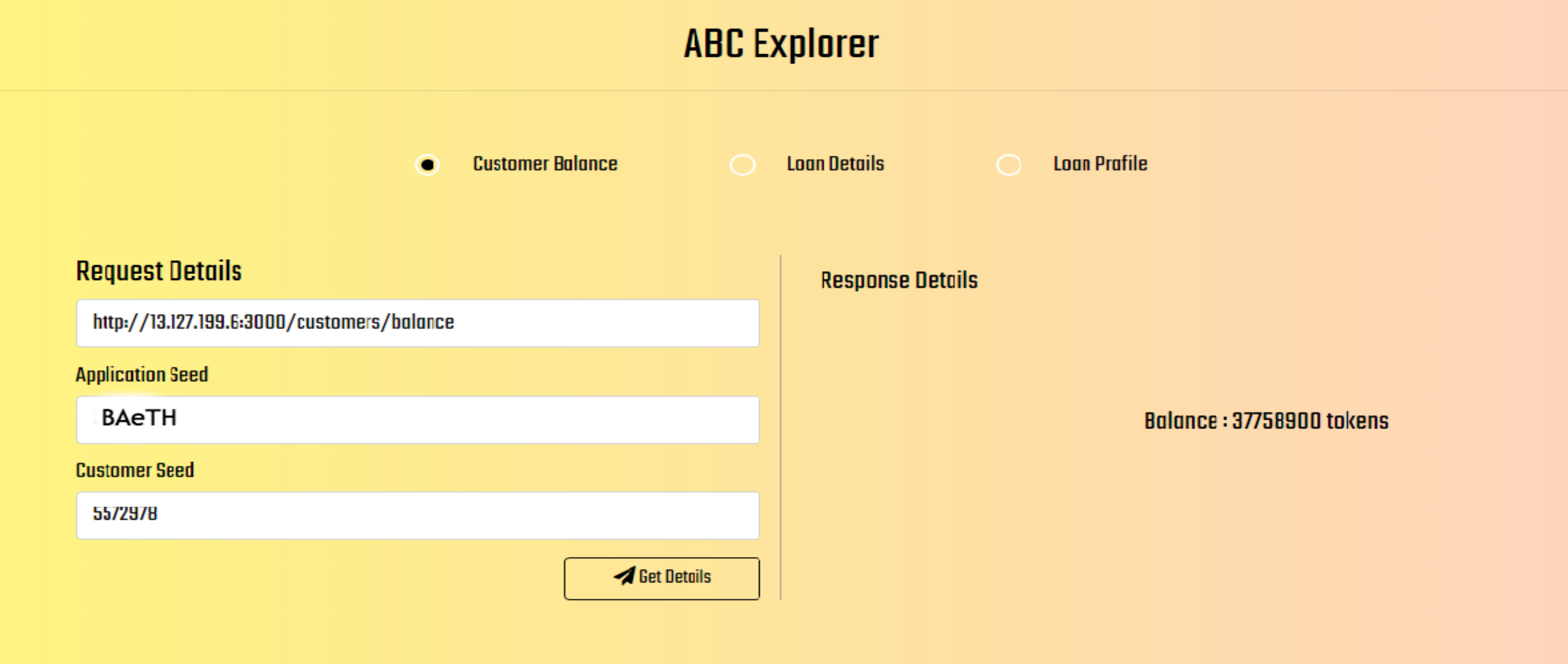
© Etherparty.io 2017 | Fork me on GitHub



Hex Value (max. 7fffffffffffffff)	Decimal Value
4e20	20000

Transaction shown in EthExplorer

Transfer BAeTH Tokens to a friend



ABC Explorer

● Customer Balance ○ Loan Details ○ Loan Profile

Request Details

http://13.127.199.6:3000/customers/balance

Application Seed

BAeTH

Customer Seed

5572978

Response Details

Balance : 37758900 tokens

Stage 1 - Recipient has 377589(00) tokens in the wallet

Thank You

Q & A

Contact :

Rahul Golash
rahul@aeries.io
+61 435 228670