Gabrotech.io
Democratise loyalty rewards using Blockchain

Gabrotech

Democratise loyalty rewards using Blockchain

TECHNICAL PAPER

Gabrotech.io

Gabro wallet

To allow versatile access to the user's various loyalty points, GBO tokens and fiat money - we designed easy-to-use mobile native application wallet (initially developed for iOS and Android devices using Swift and Kotlin respectively for the best end-user experience in each of the distinct mobile platforms). It will allow users to have trust-less access (our Gabro platform will not have access to users' cryptocurrency funds) to their crypto assets. For this scheme to work we will employ standard of BIP-321[1] to generate as many subwallets per currency as user wishes to use and also standard of BIP-392 to implement simple and secure way of backing up the randomness used to generate private keys for all the supported cryptocurrencies. User will be allowed to see the BIP-39[2] compatible mnemonics set encrypted with user's password. That same mnemonics set encrypted using AES algorithm with the user's password hardened with the algorithm PBKDF2 and fragmented to many pieces using Shamir's Secret[3] sharing protocol will be also securely stored across many data centers/locations (including different providers like Amazon AWS[4], Google Cloud[5] and Microsoft Azure[6]). This way our platform will never have access to the users cryptocurrency funds. Even in case of our infrastructure breach the users' funds will be always secured. And in the case of some of our data centers being inaccessible or plagued with temporar inaccessibility other data centers would have their own Shamir's Secret shares from which the original user's BIP-39 mnemonic can be recovered with the aid of user's password.

As there are distinct use cases and users with their habits of using browser-based web applications for any services offered out there we anticipate there will be also users not willing to utilize mobile native application to have access to the GabroTech wallet and instead they would prefer to use their browsers for that purpose. In light of these requirements the same functionality as laid out in this document with at least same level of security consideration would be also offered as HTML5 responsive[7] web-based application. We have extensive experience with building such applications using React[8] library, so that's what we will utilize. Generally the backend and blockchain processes would be shared and only different user interface would be used for different needs of different user profiles.

Access to the wallet will be guarded not only by the user's password or PIN code but also with the user's permission by the sophisticated biometric factors, mainly facial recognition algorithms. Technologies like Face++[9] or ZoOm[10] are no longer

---

[1] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
[2] https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
[3] https://dl.acm.org/citation.cfm?doid=359168.359176
[4] https://aws.amazon.com
[5] https://cloud.google.com
[6] https://azure.microsoft.com
[7] http://thinkapps.com/blog/development/responsive-web-vs-native-apps/
[8] https://reactjs.org
[9] https://www.faceplusplus.com
[10] https://www.zoomlogin.com

used only by the technology geeks and experimentators. These technologies matured over years (especially its spoof-proof protection mechanism - which prevents bad actors from simply using user's social media profile photos and videos and use it to try to circumvent the liveness detection mechanisms) and reached the level of accuracy that make them now trusted by the reputable financial institutions and organizations as a means of user's authentication of access to their private financial products and services. Using technologies like that our users will conduct registration process in which his/her biometric factors (with the user's approval) will be scanned, digitized and hashed to be usable as the factor for the comparison and authentication in the future login attempts to the application. Hashed data like that can be safely stored in the encrypted form, digitally signed by the user (using for the signing process the same private key as was used to hold the crypto funds) on the Gabro server for the future usage in the authentication process.

Gabro token

GBO tokens are an ERC20-compliant token that will be created during the token generation event period (another compatible standard of ERC-677[11] is still being assessed, as it presents superior security properties leaving backward-compatibility of the token standard, but as the standard is still in the Draft form we do not commit to implement it yet). Up to 1,000,000,000 GBO tokens will be issued during that period.

GBO tokens will be used in Gabro Wallet and Liquidity Market as the native token for all interactions between users and merchants. GBO tokens can be accessed by using any wallet service that supports ERC20-compliant tokens, such as MyEtherWallet, Parity, and the official Gabro Wallet. GBO Tokens design will be based on the ultra-secure and respected by the security community OpenZeppelin[12] framework for smart contracts development. For the integrated development and QA environment we will use latest industry standard of Truffle Suite[13] . We will also utilize the latest version of smart contracts programming language - Solidity[14].

ERC-20 compliant wallets:

Name	Link	Can user add external tokens?	Platform
MyEtherWallet	https://www.myetherwallet.com	Yes	Web
MyCrypto	https://mycrypto.com	Yes	Web
MetaMask	https://metamask.io	Yes	Browser extension

[11] https://github.com/ethereum/EIPs/issues/677
[12] https://openzeppelin.org
[13] https://truffleframework.com
[14] https://solidity.readthedocs.io

Name	Link	Can user add external tokens?	Platform
Mist	https://github.com/ethereum/mist/releases	Yes	Desktop
Parity Wallet	https://www.parity.io	Yes	Desktop
imToken	https://token.im	No (business deal required)	Mobile wallet
Coinomi	https://coinomi.com	No (deal with Bancor required)	Web
Trust Wallet	https://trustwalletapp.com	Yes	Mobile wallet
Cipher Browser	https://www.cipherbrowser.com	Yes	Mobile wallet

Prepaid card

KYC/AML compliance in the payments and financial industries is of vital importance. Fraudulent transactions if executed on the wider scale by the cards issued by the given issuer can trigger the card-schemes (Visa, Mastercard) restrictions on the cards from that issuer. Funds from stolen cards and in other way misappropriate transactions can be a source of wide chargeback demands from the valid card holders. For that reason we will be conducting KYC checks on all of our clients. To execute that operation on the scale of operations we plan that checks would be initially conducted by the 3rd party external KYC/AML check service providers, like Trulioo[15] for example.

But because we are operating in the cryptocurrencies space the funds we are collecting from our users (coming in the form of cryptocurrency deposits from other exchanges and wallets) can be also suspicious in some instances and if that cases would not be handled correctly and in line with the regulator's compliance guidelines could cause financial or reputational damages to the GabroTech brand and platform.

For that reason we are planning to partner with the cryptocurrencies and blockchain analysis and investigative platforms like Coinfirm[16], Elliptic[17] and Chainanalysis[18] to better understand the source of crypto funds and the risks associated with each and every crypto transfers and user.

[15] https://www.trulioo.com
[16] https://www.coinfirm.io
[17] https://www.elliptic.co
[18] https://www.chainalysis.com

MultiCurrency Exchange Engine

For the platform to have access to the liquid source of the GBO loyalty points, we introduce the exchange engines integration. Purpose of this exchange is to convert loyalty points to the GBO Tokens and later to fiat money. We can accomplish this by utilising power of the Bancor Network[19] with ShapeShift[20] or Changelly[21] (or other similar multi-crypto exchanges with the API for the external integration).

Bancor Network allows you to convert between any two supported ERC-20 tokens (and/or Ether) with no counterparty (in fully decentralized and trustless manner), at an automatically calculated price. GBO tokens can be also added to the Bancor Network protocol immediately creating liquid market for them without asking any centralized exchanges for permission (which is costly and requires their approval).

Bancor Protocol uses so called "Smart Tokens". These tokens are compliant with ERC20 standard but include additional logic which enables trading on the Bancor Network. Smart Tokens have liquidity mechanism built-in that allows exchanging for other ERC20 tokens and hold balances of different ERC20 tokens in a smart contract. The Bancor Formula recalculates prices constantly as a way to maintain the balance between connectors and smart contracts. For example Bancor Token (BNT) has connector to ETH, which holds ETH balance.

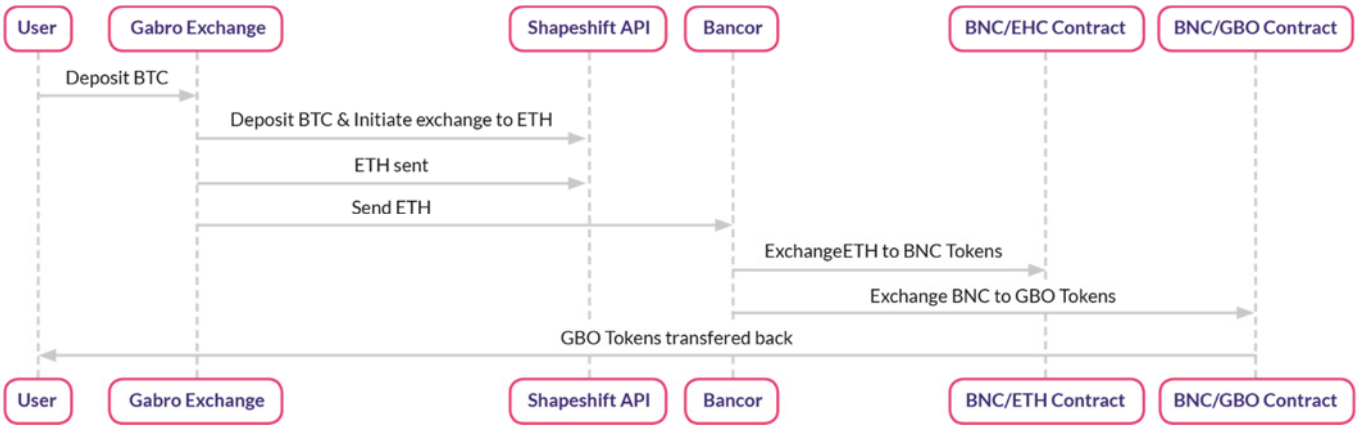
In our case the way the conversion would work is along this scheme:

- **There will be some smart contract deployed in the Ethereum mainnet that would hold two pools of assets:**
    - BNT token
    - GBO token
- **There is also another smart contract on the same network that would hold pool of BNT and tokenized ETH (wrapped in ERC20 compliant smart contract).**
- **Whenever user wants to convert GBO tokens to ETH he effectively executes chain of two operations:**
    - Selling GBO for BNT in the first mentioned smart contract
    - Buying ETH using BNT in the second mentioned smart contract

[19] https://www.bancor.network
[20] https://shapeshift.io
[21] https://changelly.com

All of these operations are atomic, which means these operations are happening in one single step and are fully seamless and transparent to the end user. Naturally it is also possible to convert ETH to GBO by reverting the above steps. Having ETH user can convert them to any other cryptocurrency using the external exchanges integration as described below or even our own exchange platform as described even further below. The exact venue where the exchange is happening in insignificant to the end user as from their perspective it is also a single-step transparent operation. Example how that operation would work for the scenario of acquiring GBO tokens for the holding of BTC coins can be analyzed below:

MULTICURRENCY EXCHANGE ENGINE



ShapeShift is an exchange platform which enables instant exchanges between supported cryptocurrencies like BTC, LTC, ETH, DASH and many more (whole list can be found https://info.shapeshift.io/about). ShapeShift supports wide variety of coins, Gabro Tokens can be purchased via most popular crypto tokens. Shapeshift made their JS API publically available and anyone can integrate their instant exchange. We don't expect ShapeShift to add direct support for the GBO tokens soon, hence we envision to utilize it to convert ETH to other cryptocurrencies and whenever the ETH/GBO conversion is needed to utilize Bancor Network protocol for that purpose.

Purchasing GBO Tokens can be achieved using the same tools but the process will be reversed. With the ShapeShift and Bancor Network, many coins can be used to purchase GBO Tokens.

MULTICURRENCY EXCHANGE ENGINE

Initially as the platform would have very little natural liquidity for the transaction exchanges to the other major currencies like ETH or BTC we would relay on the external exchanges relationship as laid out above. In time, when the number of white-labeled tokens increases and activity between users and merchants goes up the natural demand for external currencies exchanges would obviously go up too. That would allow us to slowly build our own internal liquidity pool and we would be able to gradually phase out and cut the ties with the external exchanges and relay on the internal supply of the exchange orders. There might be naturally arbitrage opportunities occasionally as the exchange rates can fluctuate freely on our exchange and on any other external exchanges, we would naturally intervene on that occasions and secure the profit opportunity and rebalance the market and internal order book.

Having multitude of supported cryptocurrencies (various clones of BTC, ETH but also ERC-20 tokens and other currencies like Stellar Lumens, EOS, Ripple etc.), each of them having different technological needs and the way the value is being handled with their specific blockchain technologies initially we would be offering centralized order book exchange to cover the initial needs. But over time we would be building on the growing pool of research efforts in the space of decentralized exchanges[22] and especially atomic-swaps between separate blockchains[23].

Integration of these technologies would mean that GabroTech platform would not need to directly hold any users' assets. That liability burden could be changed into user's own asset. That decreases security attack vectors on the platform but also gives end user greater experience where they don't need to rely on the platform's honesty in executing their trades in most efficient manner, that could be changed into provably-fair trades executing peer-to-peer directly between the users or with the facilitation of the dedicated but still decentralized facilitation engines (being it in the form of smart contracts or loosely connected network of agents with their specialized order books).

Centralized and decentralized trading venues and submodules can in fact coexist within the same ecosystem as each of them has some dicting features and tradeoffs (pace of orders execution vs efficient spreads; trust-dependability vs provable-fairness; various degree of arbitrage opportunities).

[22] https://hackernoon.com/understanding-decentralized-exchanges-51b70ed3fe67

[23] https://en.bitcoin.it/wiki/Atomic_cross-chain_trading

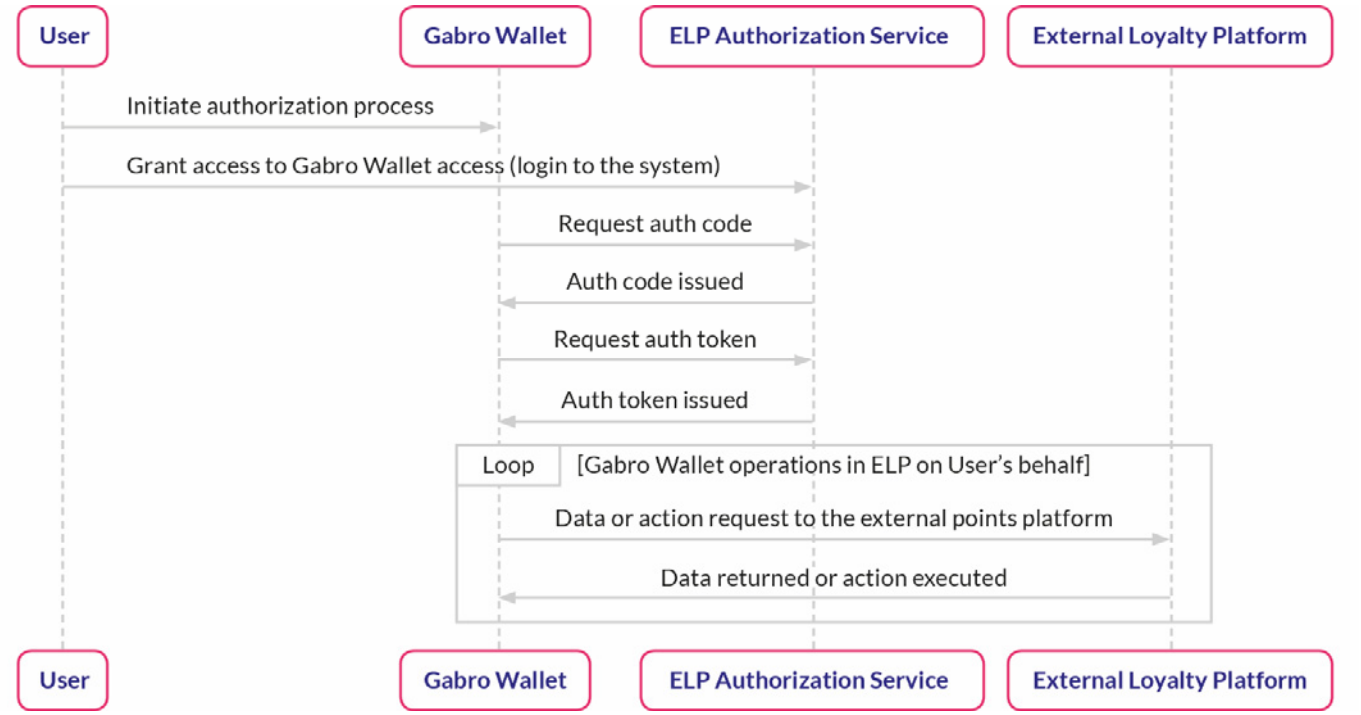
Loyalty central

Loyalty central is the core of the system. Tightly coupled with the Gabro Wallet as its user-facing interface offers seamless access to all of the platform features, including hasslefree management of users loyalty points within the Gabro Platform but also any other loyalty points platform integrated into the Gabro Platform.

1) External Loyalty Points system integration

For the end user to allow access to any loyalty points platform directly from the Gabro Wallet we will design REST-based integration API which every other loyalty point system that wants to allow their users to have the access to their points would need to implement and integrate. The authorization and authentication process between the Gabro Wallet and the External Loyalty Points systems (ELP) would follow the standardized OAuth2[24] protocol.

GABRO WALLET ACCESS AUTHORIZATION TO USER'S EXTERNAL LOYALTY PLATFORM POINTS (OAUTH2 BASED)

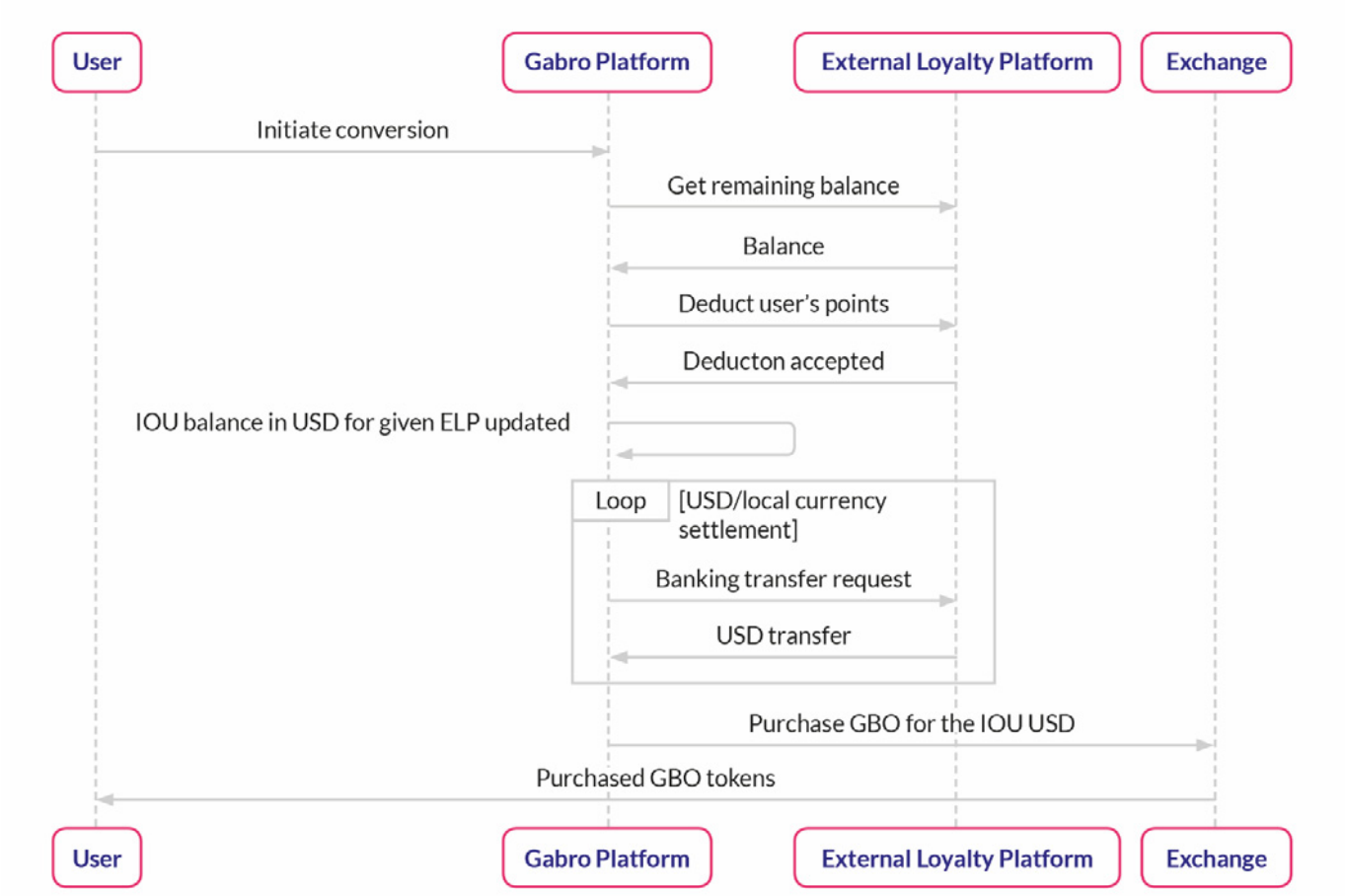


[24] https://oauth.net/2/

2) Converting ELP points into GBO

For the end user the smoothest experience is offered by the GBO loyalty tokens itself, as these tokens could be spend directly at any participating merchant site hence it is envisaged that users would readily convert their proprietary loyalty points at external loyalty points system into the GBO. To allow that operations to happen we designed the exchange protocol that employs the integration protocol between the ELP, external exchanges where the GBO will be traded and also the financial/fiat integration flow. The overview of that integration mechanism can be observed on the diagram below:

CONVERSION OF THE EXTERNAL LOYALTY POINTY TO GBO

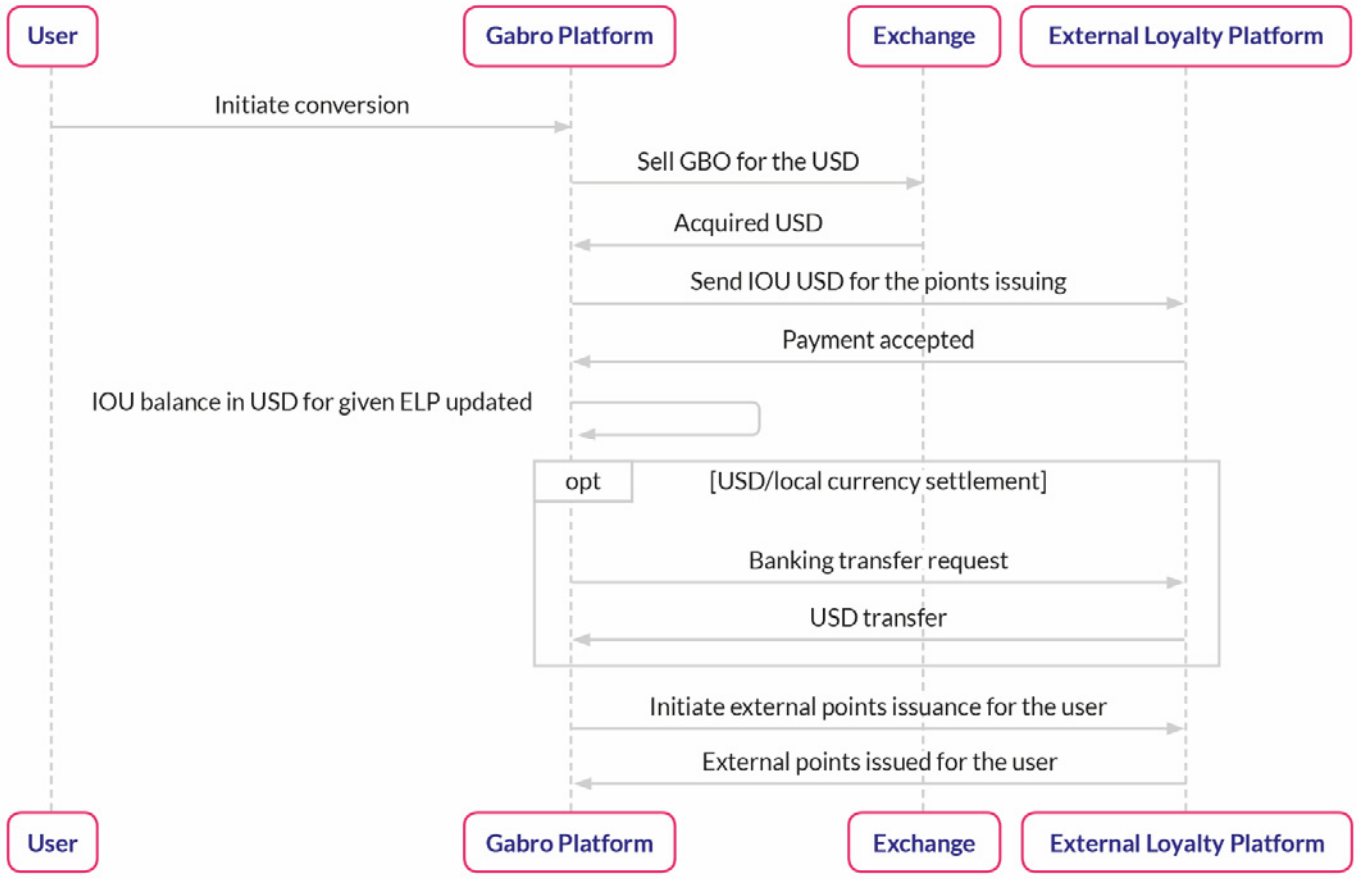


It is worth noting that some merchants would like to accept GBO as a means of payment or as a means of the bonuses redemption but they would not like to be exposed to the exchange rate risk, hence would prefer to convert these GBO to the local currency or USD. As the multicurrency exchange engine developed as part of the Gabro Wallet platform offer quick conversion between crypto tokens and the fiat currencies we can and we will offer that service to our merchants.

3) Converting GBO into ELP points

It is also envisioned that some users would like to convert their GBO holdings into the external loyalty proprietary points, for example if there are special promotions at the given merchant for the holders of that merchant own points. For that process to happen smoothly directly from the Gabro Wallet we also designed the protocol and operations reversing the above mentioned flow. The details of this protocol can be reviewed on the below sequence diagram:

CONVERSION OF THE GBO TO EXTERNAL LOYALTY POINTS



4) Gabro Wallet usage in off-line Point-of-Sale scenarios

A lot of points-of-sale where the loyalty points are being accepted are still brick and mortar shops where the traditional POS terminals prevail. Venues like that most of the time lack the on-line terminals hence to redeem the GBO loyalty points we would need to design the technology where even offline points redemption is possible and secure. To solve that problem we are working on the protocol that would employ couple of existing technologies:

- Bluetooth or NFC communication between user's smartphone and the merchants terminal (which could be also a smartphone). The devices would be able to communicate with each other directly.

- Cryptographic protocol based on the State Channel[25] where the GBO tokens would be locked in the smart contract and only those locked tokens could be used for the off-line redemption. Any process of locking down the GBO in smart contract would generate a cryptographic proof/certification from the platform that the lockdown happened. User would be able to lock and redeem only smaller number of the GBO points, greatly reducing risk of double-spending these points. In terms of security model this process would have very similar characteristics of the contactless payment[26] cards technology.

5) White labeled external points crypto tokens (called WL for short)

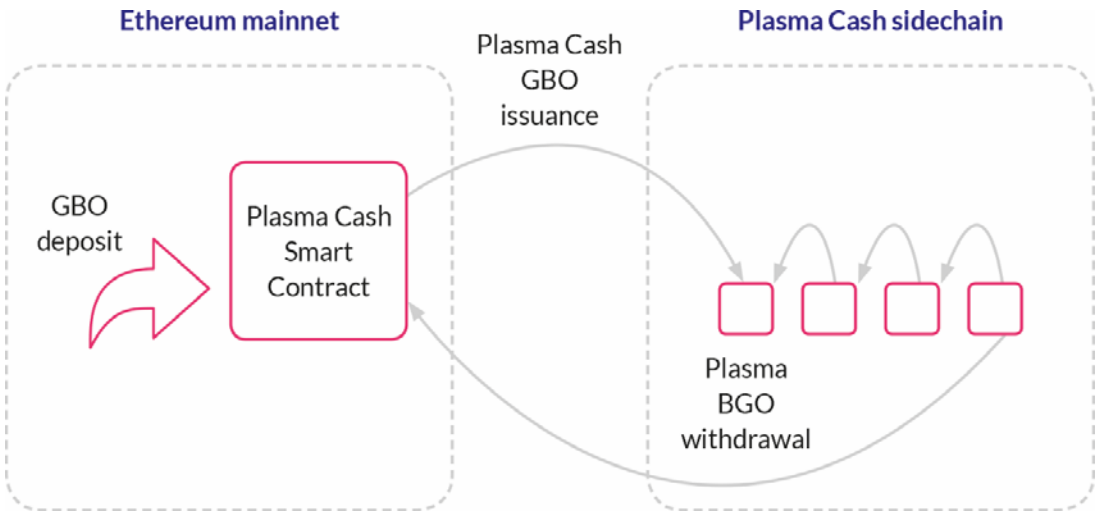
A Variant where GabroTech and the merchant agrees by means of the business agreement what is the fixed conversion rate between the existing merchant's loyalty points and the GBO tokens (or the local currency/USD). For example the exchange rate could be fixed at a level of 100 merchant tokens to be worth of 1 GBO token (or HKD$10 or US$1). There is also spread specified for the WL issuance and the WL redemption/withdrawal. These tokens will not be offered to be tradeable on the open market as the exchange rate is fixed on the business level, hence we plan to issue them on our private PoA blockchain as specified in the section g) below and there are no bridges or cross-chain transfers offered for these tokens back to the main Ethereum network (this way the platform can control the tokens exchange and their valuation pegged to the GBO value or local currency/USD). For each merchant deployed on the PoA[27] private blockchain there will be a merchant-specific smart contract that would objectively control execution of the business-level contract -- the main objective of this smart contract would be to issue appropriate number of WL tokens for the deposited GBO tokens (or local currency/USD) and also redeem WL tokens for GBO (or local currency/USD) when the user wants to sell the former tokens.

[25] https://www.jeffcoleman.ca/state-channels/
[26] https://en.wikipedia.org/wiki/Contactless_payment#Security
[27] https://github.com/poanetwork/wiki/wiki/What-is-POA

B The other wariant of WL tokens is similar to the above with the difference that once issued the WL tokens would be freely tradable and exchangeable for the GBO or other assets using the exchange rate established by the free market. There will still be PoA private blockchain where these WL tokens will be initially issued and there will still be issuance/redemption smart contract with the exchange rates as specified on the initial business agreement. But there will be also bridges deployed and other cross-blockchain transfer mechanisms that would allow users to freely transfer these tokens to main Ethereum network and trade them for other assets and other tokens without any pricing restrictions.

6) Efficient GBO tokens passing between Gabro Wallet users and merchants

When the acceptance for the tokens increases over time and the majority of the transactions processed within the Gabro Wallet would be the GBO transfers itself, less of the operations of ELP points redemption or issuance (and connected to them exchange operations of the GBO, USD and possibly other cryptocurrencies in the same atomic operation) we would need to introduce cheap way of changing the GBO ownership. After thorough analysis we decided for the technology that is being exceled within the Ethereum developers ecosystem: Plasma Cash[28]. It was initially conceived as the trustless blockchain scaling solutions for the exchanges. It does not require any federation of nodes, single operator of the Plasma sidechain is equally trustworthy as the cryptographic safeguards embedded into that protocol compel him to play by the rules, and if the rules are maliciously broken the operator or other fraudulent users can be easily challenged using objective smart contracts. This gives us all we need: near zero cost of the tokens passing between the platform participants and guarantee the complete trust between the operator of the platform and all its users.



[28] https://plasma.io

To elaborate a bit more how the Plasma Cash integration can work, we can identify these elements:

Plasma smart contract

deployed on the Ethereum main network. This is the place that controls all the operations of the GBO tokens issuance on the Plasma side chain and also all the operations of withdrawal of these tokens.

Plasma server

This would be a fault-tolerant highly available server application developed in Node.js. It would be responsible for:

- gathering all the transactions and building merkle trees for them
- creating blocks with the set of transactions
- monitoring transactions and challenging malicious actors
- defending fraudulent challenges from other malicious actors

Plasma and Plasma Cash as a standards are not uniformly defined. One project's implementation of Plasma does not need to be and rarely is compatible with other projects Plasma implementation. For that reason to increase the trust in our own implementation we are planning on open-source releasing Plasma Cash monitoring node. The node that would be used by use to monitor behavior and transactions in our own Plasma sidechain. It would be part of our own infrastructure, but users do not need to trust it, everybody would be free and even encouraged to install their own monitoring services.

7) Private blockchain for the white labelled merchants tokenized loyalty points

As it was already hinted in the section e) above for the purpose of issuing white-labelled tokenized loyalty points for the merchants we are cooperating with we are planning on releasing our private blockchain which would be guarded and secured by the consensus in which our participating merchants also take part. We were thoroughly reviewing various consensus algorithms and protocols that could safely and efficiently power such an installation (we were considering classical PoW, PoS, dPoS and PoA, more on it in Appendix A).

	PoW	PoS	PoA	dPoS
Costs	Requiring a lot of computing power to perform mining	Energy efficient as it does not require a lot of computing power	Energy efficient as it does not require a lot of computing power	Energy efficient as it does not require a lot of computing power
Finality	Slow transaction confirmation time	Faster transaction confirmation times	Fast transaction confirmation times	Fast transaction confirmation times
Accountability	Miners are Pseudo Anonymous	Validators are Pseudo Anonymous	Validators identity is known	Witnesses are Pseudo Anonymous
Decentralization	Due to creation of mining hubs, possibility for a centralization	Decentralized	Centralized	Partially centralized
Scalability	Not well scalable	Scalable	Scalable	Scalable
Applicability	Most fitted for Public Blockchain	Public and Private Blockchain	Public and Private Blockchain, but mostly fitted for private blockchains	Mobile Public and Private Blockchainwallet
Prevalence	Most cryptocurrencies are using PoW.	DASH, NEO implemented PoS	Ethereum Kovan Network	EOS

After this analytical exercise we finally settled on choosing PoA (and POA.Network[29] as its implementation based on the Parity Ethereum technology) as the algorithm that would suit our needs. The reason being that it allows reasonable number of potential merchants to join the network, no additional/wasted costs of the consensus (unlike PoW) and reasonable controllability of the whole network on the business level (authority to new merchants delegated based on the rules decided up-front, initially by the GabroTech and going forward by the whole group of merchants that together form the participating network alliance). The balanced, future-proof economical incentives for the group of merchants to willingly participate in securing network like that requires prices analysis, cryptoeconomic incentives alignment and multi-factor simulations but can be definitely modeled around the set of some or all of the schemes from the list below:

[29] https://poa.network

- Every merchant who participate in any form of WL tokens generation would need to pay their yearly renewal license in GBO tokens directly to the private blockchain (pool)

- All the private blockchain validating nodes would be compensated for their work with the GBO tokens from the pool (assuming block would be produced on average every 5 seconds and assuming production of one block would be compensated with 1 GBO token operation like that would require 6'307'200 tokens to be paid into the network every year)
- Tokens being held in the compensation pool are incentivising GBO price to go up over the year

- Merchants that decided to participate in the blocks validation scheme are charged with smaller yearly renewal license fees then those merchants who does not participate in the validation protocol

- Every operation of token issuance/redemption from the smart contract on the private blockchain can generate additional GBO fee that would be transferred to the common pool for the redistribution for the validating nodes

SUMMARY OF THE REASONING AND COMPARISON OF PRIVATE AND PUBLIC BLOCKCHAIN SOLUTIONS:

	Public Blockchain	Private Blockchain
Read Access	Anyone in the world can read the transaction data	Right to read the blockchain might be restricted
Write Access	Anyone can make transactions to the blockchain	Right to make transactions to the blockchain is restricted to trusted party
Consensus Access	Anyone can participate in the consensus	Consensus process is handled by selected nodes e.g. 12 nodes of different banks
Examples	Bitcoin Ethereum	Hyperledger Fabric Corda
Pros	• Public blockchains are open, everyone can participate • Developers have little power of changing the rules of the application, self governing	• Consortium can easily change the rules of a blockchain, revert transactions etc when software bug is noticed. No need for hard fork • Validators are known in the network • Transactions are cheap • Privacy • More suited for Enterprise applications
Cons	• High transactions fees • Probability of 51% attack • 3Lack of privacy/very hard to achieve	• More centralized/concentrated • Requires trust in the validators • Can be potentially censored

Analytics, AI, Big Data

With the vast amount of users' data to which GabroTech has access to (spending habits and patterns, geographical locations, wealth levels, gender, age group etc), these data could be utilized and put to work for the purposes beneficial to both data-holders, merchants and also other platform stakeholders. On the other hand GabroTech with its interconnectivity with various external exchange platforms and also its own internal exchange capabilities is able to monitor and discover interesting arbitrage and other trading opportunities that could be offered also own platform users.

To be able to handle these huge volumes of BigData and on the other hand to use machine learning and other Artificial Intelligence techniques on the BigData and also coming in real-time transactional data (exchange rates, trades executed in real-time etc) strong and reliable technology stack is a must. One of the tech stack that is able to handle both type of demands at the same time and is accessible as an open-source, hence for very reasonable pricing and with huge community of developers behind it is Elastic Stack[30] with its components of: Elasticsearch[31] (search and analytics engine), Logstash[32] (data enrichment, cleansing, real-time transformation, aggregation and mutation), Kibana[33] (visualization tool, drill down data explorer and discoverer) and Machine Learning[34] (artificial intelligence engine that can spot the insights and patterns that casual human observer might miss). More elaborate introduction to each of these components[35] can be reviewed following the links from the footer.

What is worth noting here is that big cloud companies like Amazon AWS have dedicated cloud services based directly on the Elasticsearch and the related components hence the server-side infrastructure setup can be both cheap and reasonably easy and time-efficient to implement and for petabyte-scale data sources.

[30] https://www.elastic.co/elk-stack
[31] https://www.elastic.co/products/elasticsearch
[32] https://www.elastic.co/products/logstash
[33] https://www.elastic.co/products/kibana
[34] https://www.elastic.co/products/x-pack/machine-learning
[35] https://aws.amazon.com/elasticsearch-service/

What is exactly stored in the blockchain and what is centralized in the blockchain

01 All transfers of tokens and other cryptocurrencies between users

02 All transfers of tokens between users and merchants

03 Atomic swaps between tokens and cryptocurrencies

04 All token transfers executed on the Plazma Cash sidechain

05 Exchange of cryptocurrencies executed via Bancor Network plarform

06 User pseudonyms (addresses of their wallets)

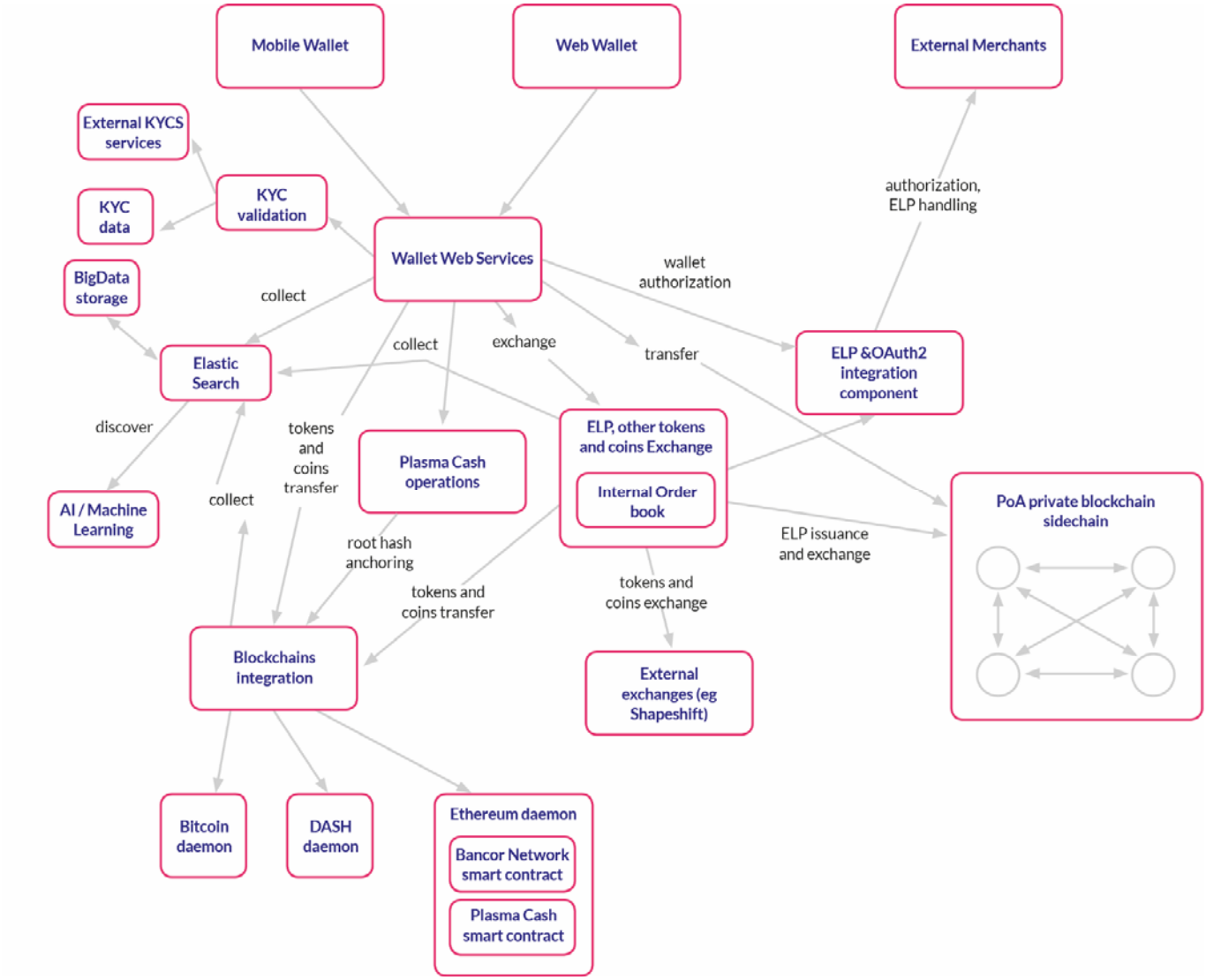
Stored on the separate centralized servers maintained by GabroTech:

01 KYC and AML related data (not public due to privacy and regulations compliance reasons).

02 Integration credentials for OAUTH2 and generally integration details of GabroTech infrastructure and the cooperating merchants.

03 Details of the deals betweeen GabroTech and merchants (what kind of tokens are being issued, what are the spreads for buying/selling tokens).

Overall high-level architecture diagram



How Plasma Cash and PoA private network could help business

to ensure transactions are genuine and token issuance is legitimate and in-line with the agreed upon contracts between GabroTech and the merchants

A

The technology behind Plasma Cash secures the tokens passing in the way that on the Plasma Cash sidechain does not require the operator of that sidechain to form any consortia or federations of the nodes with other entities. It can be easily structured as a single-node operator (or two to three nodes single operator for the technical resilience and fault-tolerance purpose) and still maintain high standard of security and transparency. The reason is that the security as such is guaranteed by the smart contract installed on the Ethereum mainnet which purpose is to guard the passing of the tokens between mainnet and the sidechain (but not within the sidechain, that is orchestrated solely by the single operator).

Users having the assurance that no matter what their tokens can be always withdrawn from the sidechain directly back to the Ethereum mainnet chain can transact freely and without worry of the fraudulent behaviour of any other user or operator on the sidechain. Naturally every transaction that happens on the side chain and on the Plasma Smart contract on the mainnet chain have to be observed and if suspicious activity is discovered it has to be challenged straight away (and possibly the mass withdrawal of the tokens also executed). Nevertheless following the protocol as specified is enough to make sure the funds and tokens hold and transferred are secure.

B

On the other hand the PoA private blockchain is going to be used for securing the as-agreed white label (WL) loyalty points issuance contracts within the GabroTech network. Contractual terms will differ from merchant to merchant but nevertheless merchants want to be assured that the execution of these terms does not deviate from what was agreed. All these contractual terms will be modeled as a Solidity smart contracts for the WL tokens issuance. Because merchants with substantial GBO holdings will have the opportunity to form also part of the validators network within the PoA private blockchain, as a whole they will have peace of mind that the network and the execution logic of the smart contracts deployed on that network runs in accordance to the contractual business terms.

Depending on the actual terms of the contractual agreement (if the WL token pricing is fixed and if GabroTech would offer that token exchangeability for other cryptocurrencies and fiat money) WL tokens can be transferred from PoA network to the main Ethereum network and also to the Plasma Cash chains for rapid and cheap value passing within the wider GabroTech technical ecosystem and landscape.

Consensus protocols analysis

PoW

A piece of data that requires significant computation to find. In bitcoin, miners must find a numeric solution to the SHA256 algorithm that meets a network-wide target, the difficulty target. This means that miners compete with each other by calculating hashes and miner that calculates the correct one first, wins. Their block gets to be the next in the blockchain.

This work is incentivized, with each block creation new coins are created and those coins are going to the miner that found the correct hashes. This is the most known approach to mining (block creation). It is mostly used when we do not trust the other parties.

This approach is considered the old way, Ethereum is slowly moving away from this consensus mechanism.

Pros: It is currently the most implemented and used solution, and considered the safest one for the public blockchains;

Cons: Slow transactions, requiring specialized mining equipment.

PoS

Proof-of-Stake (PoS) is a method by which a cryptocurrency blockchain network aims to achieve distributed onsensus. Proof-of-Stake asks block producers to prove ownership of a certain amount of currency (their "stake" in the currency).

The common argument against proof-of-stake is the Nothing at Stake problem. The concern is that since it costs validators almost no computational power to support a fork unlike PoW, validators could vote for both sides of every fork that happens. Forks in PoS could then be much more common than in PoW, which some people worry could harm the credibility of the currency.

Pros: Attacks more expensive; More decentralized; Faster transactions confirmation times; No wasted computation;

Cons: Nothing at Stake attack.

PoA

PoA consensus is a straightforward and efficient form of Proof of Stake with known Validators and governance-based penalty system. This means that only trusted nodes can participate in a network as block producers. If their behavior will indicate that they are misbehaving, the trust in them is broken and they get banned from participating in the consensus.

A list of block validators is managed by a smart contract with governance by Validators. First validators are chosen by the centralized, trusted authority, which distributes keys to some static number of independent block validators.

Basically, for this to work efficiently, each block producer's identity has to be known (PoW and PoS do not require this).

The most well-known cryptocurrency that uses variant of this approach is Ripple. The PoA protocol is also used on Ethereum's testnets Kovan and Rinkeby.

Pros: High throughput; scalable, identity known of the validators we put the trust in;

Cons: Centralized system.

dPoS

In Delegated-Proof-of-Stake (dPoS) , token holders don't vote on the validity of the blocks themselves, but vote to elect delegates to do the validation on their behalf. Voting can occur in many ways. The most basic approach is having one node equals one vote. This may lead to "Sybil attack" problem, where someone can have thousands of nodes and take over the network.

Second approach is to weight the vote based on how many coins a node has: a stake.
All the nodes in the dPoS network system vote on which nodes will become block producers or Witnesses. The voting power is based on a stake—nodes with more (native) cryptocurrency have more voting power. Once the block producers are chosen, they create blocks in a predetermined way. This approach means that the community is allowed to choose which nodes have the power to produce transaction blocks.

Each time witnesses produce a block, they are paid for their services. How much they will get paid is set by the stakeholders via their elected delegates. If a witness fails to produce a block, then they not receive payment, and later may be voted out.
The state of active witnesses is updated once every maintenance interval (1 day) when the votes are gathered. The witnesses are then shuffled, and each witness is given a turn to produce a block at a fixed schedule of one block every 2 seconds. After all witnesses have had a turn, they are shuffled again. If a witness does not produce a block in their

turn, then that turn is skipped, and the next witness produces the next block. Anyone can monitor network health by observing the witness participation rate.

Delegates are elected in a manner similar to witnesses. A delegate becomes a co-signer on a special account that has the privilege of proposing changes to the network parameters. This account is known as the genesis account. These parameters include everything from transaction fees, to block sizes, witness pay, and block intervals. After the majority of delegates have approved a proposed change, the stakeholders are granted a 2 week review period during which they may vote out delegates and nullify the proposed changes.

Pros: Cheap transactions; scalable;

Cons: Partially centralized.