THE CAASIOPE NETWORK
The first Cryptocurrency-as-a-Service blockchain

Guillaume Bonnot
www.caasiope.net
July 15th, 2018

Abstract. A simple blockchain which supports multiple external blockchain assets would help blockchain business easily transact with multiple assets using a single protocol. Acting as a layer 2 solution, the blockchain helps external blockchains scale and interoperate by allowing distinct assets to be exchanged without the need for these assets to be transacted on their native external network. While cryptographic fully decentralized mechanisms are appropriate for layer 1 solutions, they are not suitable for a universal layer 2 protocol to interoperate between distinct blockchains. Trusted central parties like cryptocurrency exchanges are being used to transact between distinct blockchain assets but require a high degree of trust. We propose a hybrid model which requires a certain level of trust for on-chain transactions, and uses using off-chain consequences to mitigate trust required. Tokenized assets issued on the network are fully collateralized by native blockchain assets by using multi-signature custodian wallets which are also secured by the proposed hybrid model.

Definition. Cryptocurrency-as-a-Service offers third parties the possibility to process payments in different cryptocurrencies using a dedicated infrastructure.

1. Introduction

Rise of Blockchain

Cryptocurrency and blockchain contain technological breakthroughs which could replace traditional centralized trust models, and in recent years have been thoroughly studied by the very financial institutions (FI) they are meant to replace. The base functionality of a blockchain is to facilitate an action on a digital ledger, such as a payment or transfer of value, between multiple parties without the need for a trusted third party. The blockchain itself is a ledger which tracks the state of balances across its network, and is held not by one party but by all users of the network. Centralized FI controlled database transactions are fast, have a high trust barrier, and the cost structure depends on the FI. Decentralized blockchains controlled by nodes are slower than centralized databases, however they remove the trust requirement for a transaction, and their cost is determined by market forces in the network.

In traditional finance the FI is a centrally controlled, trusted counterparty. The FI is responsible for validating transactions such as processing payments. It is responsible for governing its operations and relationship to customers and other FIs. Finally, it is a custodian of its clients' assets, responsible for maintaining, crediting, and debiting a client's, and ensures the safety of its clients' funds it holds in custody. An FI may be considered credible as it is an established legal entity with shareholders, regulatory compliance, shareholders, and a balance sheet. An FI may also be evaluated by subjective measures such as reputation, brand equity, and trust. These hard and soft business assets can positively or negatively affect a client's trust in the FI, and exist off-chain.

In blockchain based systems this centralized model is replaced by a decentralized model where no central entity holds power over validation, governance, and custodianship. Instead these powers and responsibilities are decentralized, held by the users of the network itself. In most blockchains, transaction validation is performed by nodes. Governance and decision making is performed by choosing to run a node or by employing a decentralized voting mechanism. Finally the user is the ultimate custodian of their assets. A blockchain based asset can only be accessed by a user who has control of the private keys to their wallet. The user is in full control of their assets, and also has ultimate responsibility for safeguarding their assets. Blockchain based systems are fully digital and do not have a central authority. The also differ greatly from FIs for legal protection in the physical world as legal definitions of blockchain based systems remain unclear in many jurisdictions and blockchains lack a central counterparty that is responsible for network fraud or failure. Blockchain mechanisms are fully on-chain.

Rise of Crypto

Crypto assets (assets), assets represented on blockchains, have grown in popularity with the market capitalization of all assets reaching as high as $829 billion USD in January of 2018. Speculation has driven trading activity of assets and led to a growing number of crypto exchanges (exchanges) where users can exchange one asset for another asset, or for fiat currency. While rising trading volume and asset price has created viable economic activities for many crypto users and exchanges, it has also created new sets of challenges.

According to coinmarketcap.com at time of writing more than 2,000 assets are being traded on exchanges. Increased usage has uncovered scaling issues on many blockchains which are unable to meet rising transaction volume with adequate speed, frequency, and low cost of transactions. This has also led to challenges for exchange IT infrastructure, particularly to support new assets. To accept deposits and withdrawals of a new asset, an exchange must integrate, support, and secure a new wallet per asset. Multiple wallets require a high degree of technical specialty and are a target for hackers presenting security risks for clients' assets held in custody by exchanges. This problem will continue to grow as more assets means more wallets, greater asset liability, and greater security risk.

(De)centralized Paradox

Blockchain based assets provide full decentralization and control for users, however exchanges must hold custody of assets that are being traded in order to provide the exchange service. Users are currently using exchanges as multi asset wallets because of the lack of convenient ways to store multiple assets. By using an exchange as a wallet, the user loses control of their assets and is forced to trust the exchange which becomes a crypto FI and returns the user to a fully centralized model. Exchanges also currently exist in a regulatory gap without staunch legal and compliance oversight making consumer protection unclear. Finally, operations and custodian practices of many exchanges are opaque, leaving users no choice but to fully trust the exchange. Exchange users may be in a worse position than operating with tradition FIs which are subject to strict oversight, and are instead at the sole mercy of the crypto FIs.

Exchanges are centrally controlled marketplaces where users trade one decentralized asset for another. The use of exchanges highlights the demand to trade different assets, but also shows that these assets cannot be traded between each other without the use of a trusted third party.Rise in trading volume proves there is economic opportunity for a simple technical solution to transact between assets.

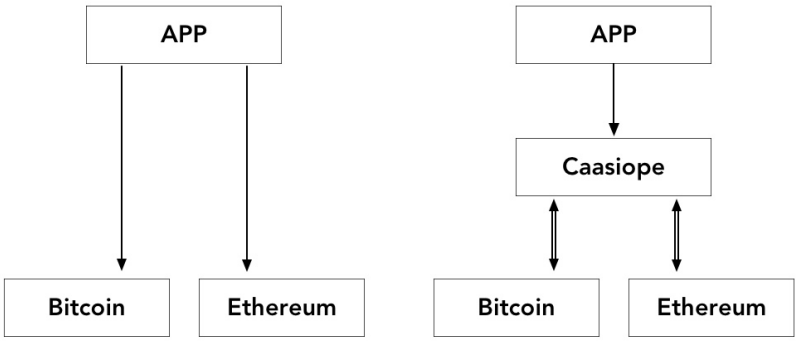
To solve usability and unlock potential opportunities, businesses need a simple single point of integration to manage multiple cryptocurrencies. This will allow users to send, spend, or swap multiple cryptocurrencies seamlessly without the need to use an exchange or to manage multiple wallets.

Complexity vs. Simplicity

Many protocols are focusing on developing cross-blockchain transactions. Decentralized exchanges are also rising in popularity allowing trade between assets without a central custodian. However most of these solutions focus on on-chain cryptographic methods to transact between chains.

As blockchain based systems are slower than centralized transactions, fully decentralized solutions between multiple chains compound scalability issues, result in slower transaction time, and add technical complexity, resulting in poor user experience. We believe that fully decentralized solutions to transact between blockchains only solve a certain subset of problems, but do not cover all the use cases necessary for blockchain to reach global adoption.

We argue there is a third way to solve problems of inter-blockchain transactions which improves user experience and makes cross chain interaction simple. We borrow mechanisms from both traditional FIs and blockchains combining on-chain and off-chain elements. Our solution alleviates the technical complexity of managing multiple assets, provides greater speed than fully decentralized solutions, and most importantly provides a simple, secure, single point of integration for business seeking to implement assets into their business and gives users a better experience when exchanging assets.



The following whitepaper explains what the Cassiope blockchain is and how it solves user experience, integration, security, and speed issues when transacting between assets. We will introduce and explore Cryptocurrency-as-a-Service and Business as Stake, and finally provide some concrete examples of Caasiope in practice.

2. The Caasiope Network

Cryptocurrency-as-a-Service

The Caasiope network (network) is a layer 2 blockchain protocol which serves as a simple, single integration for businesses which want to support multiple crypto assets. The primary purpose of the network is to propose Cryptocurrency-as-a-Service (CaaS as in Caasiope) which lowers technical barriers for businesses to support multiple assets without dealing with the complexity, implementation and maintenance costs, and security risks of hosting a separate wallet for each asset.
Cryptocurrency-as-a-Service gives business access to economic opportunity which were not technically feasible before Caasiope. The network employes a unique governance mechanism called Business-as-Stake which balances the trustless digital nature of a blockchain with the speed of centralized models.

Business as Stake

Business as Stake (BaS) refers to the governance mechanism that powers the Caasiope network. Business-as-Stake uses a trusted set of businesses that have shared economic interest to use the network and have legal and economic consequences external to the network which deter malicious actions to validate transactions, self govern, and secure the funds of the network.

We realized that to achieve the goals of simplicity, security, and speed we needed a model that requires some level of trust, therefore we sought to minimize the trust required for adequate simplicity and transaction speed and created a mechanism to distribute risk. For Caasiope to support assets from other blockchains we were forced to create an asset custody model described later which required us to choose some guardian to secure the assets in custody. BaS uses both on and off-chain mechanisms to achieve a balance between trusted and trustless transactions, centralization and decentralization, and speed and network performance. Inter-network (network) transactions trade security for high speed and low cost. Cross chain transactions (between network and external blockchains) trade security for ease of use.

BaS functions by using businesses that are willing to facilitate, secure, and govern a network because they derive more economic value from being part of the network than leaving or attempting to corrupt it. Economic actors are aligned with one another by sharing three types of stake connected to the network: 1. the business earns some income from operating on the network 2) the business could face hard or soft consequences external to the network, and 3) the business holds claim to some tokens in the network. The multiple forms of stake are economic incentives for the businesses to behave honestly and are deterrents against acting maliciously.

The Caasiope Consortium

To balance between centralized and decentralized we chose a federated model, with a restricted set of actors forming the Caasiope Consortium (consortium) responsible for validation of transactions, self governance, and custody of assets. The consortium is composed of businesses which are legal entities with shareholders, legal jurisdiction, business lines, brand, and reputation. These off-chain elements are similar to how FIs prove trustworthiness and credibility. Potential hard consequences such as legal action and fines, loss of profit, regulatory action, and soft consequences like loss of future profit, brand damage, or loss of reputation act as economic deterrents against malicious behavior.

As a requirement to join the consortium we propose that a business must derive economic value from the network. Businesses integrate with the network so they may gain advantage to its ease of use, speed, or cost savings to perform operations. If the business were to leave the network they could lose some business line or revenue stream associated with the network.

Finally businesses operating on the network will hold claim to some tokens on the network. Should the network fail or be corrupted it would put their own value at risk. The consortium will be guardians of all funds on the Caasiope network including their own and their customers' funds.

Consortium Governance

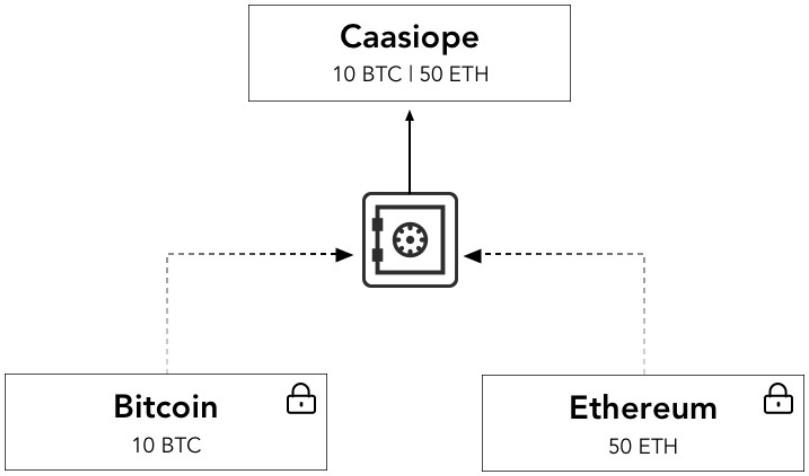
At the beginning the easiest way to bootstrap the consortium is to begin with the core Caasiope team as they will be the initial actors on the network. As new members join, the core team's influence will decline over time.

We propose a mechanism where existing members can choose to incorporate new members. Existing consortium members will take into account both hard and soft value which the new member brings to the network.

Members hold influence over validation, governance, and custody, and some members will hold more influence than others. The weight of influence a consortium member holds in the network could change over time depending on their individual business interest in relation to interests of other consortium members. Member may gain or lose weight in relation to other members due to a change in consortium members, network growth, increase or decrease in economic activity, or a change in external conditions such as a loss in reputation. The consortium should have a governance mechanism to increase or decrease the influence of a consortium member. This allows for dynamic management of influence in relation to internal and external changes and for the consortium to manage risk in a distributed manner.

Custody and Collateralized Assets

The Caasiope network interoperates with multiple blockchains through collateralized assets secured by the consortium in custodian wallets. To understand the consortium security model we must first understand the nature of these assets. Initially Caasiope will support tokenized assets (tokens) which represent assets that exist on blockchains external to the Caasiope network



Creation and Destruction of Tokens

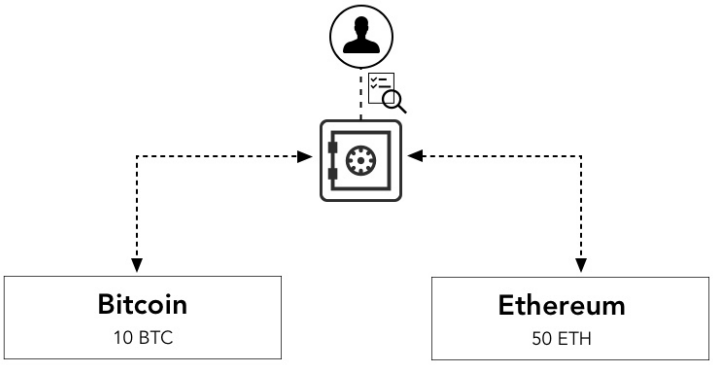
Assets from external blockchains can be deposited to Caasiope. When an asset is deposited it becomes a tokenized asset (token) which must be created by the consortium. Once a token is created it can be transacted on the network between users.

To withdraw an asset from the network, the consortium destroys the network token and performs a corresponding withdrawal transaction on the external blockchain. This process of creation and destruction ensures that tokens on the network are fully collateralized by assets on external chains.

Custodian Wallets

Custodian wallets store assets on the external blockchain of the original asset which are held as collateral for tokens created on the network. The custodian wallets are secured using a multi-signature feature. Consortium members are the custodians of the collateralized assets and each member holds private keys used to secure the assets. Using a multi-signature configuration, any withdrawals from custodian wallets must be signed by a certain threshold of private keys. This process requires multiple consortium members to agree to sign any outbound transaction. The process of signing transactions always carries some inherent security risks, so we also created a model which minimizes the frequency of transactions from custodian wallets.

Collateral of tokens is transparent and auditable. Anyone can monitor public addresses of custodian wallets on external blockchains to know when new assets are received or sent by the custodian wallet.



The collateralize assets held by the Consortium belong to consortium members, customers, and all users of the network. Whereas exchanges and FIs are singular entities, the consortium distributes counterparty risk between all its members.

Consortium and Gateways

The consortium is in charge of creation and destruction of tokens on Caasiope, while deposit and withdrawal functions are performed by gateways. A gateway can be thought of as an agent who interacts with end users of the network to perform a deposit or withdrawal.

A gateway operates with its own funds, and may have a mixture of Caasiope network tokens, and external blockchain assets. When users want to deposit or withdraw they contact a gateway, receive instructions to send the asset to a gateway's external wallet, and the gateway will send the corresponding token to the user's network wallet. To withdraw, a user will receive instructions from the gateway, send the token to the gateway, and once received the gateway will send the corresponding native asset to the user.

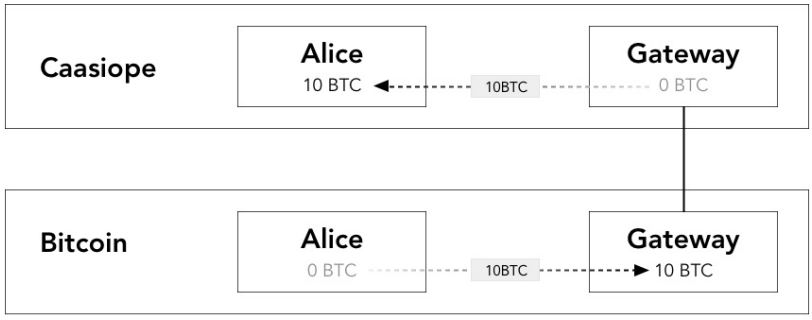
The process of creation and destruction occurs between the consortium and gateways. Consortium members and gateways will have a KYC procedure and are known to each other. While a gateway may process multiple deposit and withdrawal functions with their own funds, they choose how often to interact with the consortium to create and destroy tokens. The frequency of this action will depend on a number of factors such as flow of funds creating an imbalance of user deposit or withdrawal needs and gateway reserves. A gateway may interact with the consortium to create or destroy tokens to top up their reserves. The lowered frequency of transactions from the custodian wallet versus the deposit and withdrawal of tokens by the gateways mitigates risk to custodian wallets.

3. In Practice

In this section we explain practical applications of the Caasiope network. Network users have accounts which can hold multiple types of tokens (termed Currencies on the network) like Bitcoin (BTC) and Ether (ETH) which are backed by the aforementioned collateral mechanism. These tokens can be exchanged inside the network, or can be redeemed (withdrawn) and sent to their external blockchain address. We give examples of how a user may deposit or withdraw, an in-network transaction between different tokens, and how an exchange could use Caasiope to easily begin to operate multiple token markets with a single integration. We also pose other potential uses to be explored in the future.

Deposit and Withdrawal

- **Deposit**



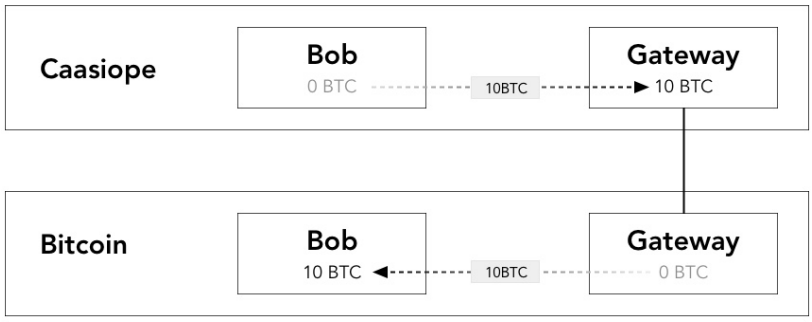
Alice is a Caasiope user and Gary is a gateway. Alice wants to deposit 10 BTC from her external Bitcoin address to her Caasiope network account. She requests a deposit from Gary who gives Alice his BTC blockchain address.

Alice sends 10 BTC to Gary's address on the external Bitcoin network.

Now Gary has 10 BTC on the Bitcoin network. Once confirmed, Gary will transfer 10 BTC from his Caasiope network account to Alice's Caasiope network account.

Now Alice has 10 BTC in her Caasiope network account and Gary has 10 BTC on the Bitcoin network.

- **Withdrawal**



Bob is a Caasiope user and Gary is a gateway. Bob wants to withdraw 10 BTC from his Caasiope account to his Bitcoin network wallet. Bob provides his Bitcoin network address to Gary and requests a withdrawal.

Gary provides Bob with a Caasiope transaction instruction which includes Gary's Caasiope network account and a Caasiope withdrawal identifier. Bob sends a Caasiope transaction for 10 BTC and includes the required information.

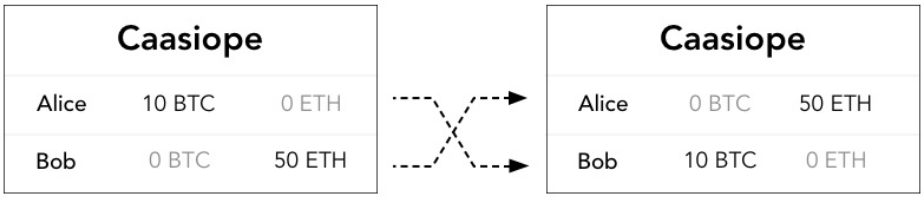
Gary receives 10 BTC to his Caasiope account, and once confirmed he sends 10 BTC to Bob's BTC address on the external Bitcoin network.

Now Bob has 10 BTC on the Bitcoin network and Gary has 10 BTC in his Caasiope network account.

Notice in these transaction examples between the Caasiope blockchain and external blockchains there was no interaction with the consortium. As a gateway Gary is an independent counterparty for Caasiope users. Gary operates using his own funds to facilitate deposits and withdrawals, which segments counterparty risk in a deposit or withdrawal to the individual gateway used for each deposit or withdrawal.

Token Swap

Similar to other cryptocurrencies, transactions in the Caasiope network are transfers of inputs and outputs. One major differences is that Caasiope supports multiple tokens, where input and outputs consist of address, currency (token type), and amount. A single transfer in the Caasiope network could consist of multiple inputs and outputs containing different currencies, making a swap between distinct tokens possible in a single transaction.



Alice and Bob are Caasiope users. Alice has 10 BTC in her Caasiope network wallet and Bob has 50 ETH in his Caasiope network wallet which they would like to exchange.

Alice creates a transaction where she sends 10 BTC to Bob's Caasiope account, and Bob sends 50 ETH to Alice's Caasiope account. Alice signs the transaction and Bob signs the same transaction and broadcasts it to the network.
Once the transaction is confirmed 10 BTC are transferred from Alice's Caasiope account to Bob's account and 50 ETH are transferred from Bob's account to Alice.
Now Alice has 50 ETH in her Caasiope network account and Bob has 10 BTC in his Caasiope network account.

Using an internal transaction Alice and Bob have seamlessly exchanged distinct tokens in the Caasiope network without having to access the Bitcoin or Ethereum blockchains. The tokens they have exchanged are fully collateralized, and have not moved from the custodian wallets. As the Caasiope network is a layer 2 solution it helps both the Bitcoin and Ethereum blockchains scale their respective transaction throughputs as the tokenized asset ownership is swapped without having to transact on the native blockchains.

Cryptocurrency Exchange

An exchange has multiple benefits from integrating with Caasiope. With a single Caasiope wallet integration an exchange could access any assets supported by the network and open trading markets for each asset without having to host multiple native asset wallets. An exchange could also easily facilitate deposits and withdrawals by integrating with gateways.

An exchange could also benefit from the network effect of Caasiope as they could make seamless transactions between any assets with other actors (users, other exchanges, and other types of business) operating on the network.

An exchange could be considered for the consortium, as it matches the criteria for BaS, and assume responsibility for the security of assets represented on the network. An exchange could also act as a gateway as it likely holds significant tokens and assets.

Future Use Cases

A decentralized exchange facilitates users to exchange tokens directly without a central party, removing counterparty custody risk. As Caasiope already supports the ability to transact between distinct tokens, a decentralized exchange would only have to match orders submitted by the users.

A trustless brokerage which helps customers swap one asset for another could be built on top of Caasiope. The broker could use the token swap functionality to exchange assets and would provide their own buy and sell side liquidity.

A merchant could use the Caasiope network to begin accepting multiple assets as payment and use a single Caasiope wallet to manage all assets.

More applications of Caasiope can be imagined and we may dedicate future whitepapers to detail these.

4. Conclusion

The growing popularity of blockchain based assets has unlocked new business opportunities such as exchanging between assets, but has also highlighted issues of technical integration, scalability, and interoperability of blockchains. Exchange trading volumes show there is market demand to trade between assets but they are trusted centralized FIs with custody of user funds presenting consumer risks.

We present a third way to seamlessly transact between blockchain assets with a simple single blockchain integration. Rather than fully centralized or decentralized, Caasiope borrows both on and off-chain mechanisms to create a consortium which validates transactions, governs itself, and holds custody of network funds. The hybrid mechanism adds transactional speed and ease of use, but requires a certain level of trust for on-chain transactions, which is minimized by using off-chain mechanisms to create a good enough trust model tying on and off-chain economic incentives together. A separate deposit and withdrawal mechanism is used to minimize the frequency of external blockchain transactions minimizing security risk to collateral accounts.

While technical integration and usability hurdles had been barriers for businesses to access opportunities, Caasiope's ease of use and seamless user experience can help drive commercial blockchain adoption. Business such as exchanges, merchants, or payment gateways can use the network as a single point of integration to manage all of their blockchain assets and unlock new business models which may have not been able to be explored before.