Why Crypto Financial Structures Should Be Built Differently

Cryptocurrencies and crypto assets have emerged as a new asset class and are rapidly becoming more mainstream every day. But investors cannot leverage the full potential of this groundbreaking innovation yet because there is one crucial enabler for this financial ecosystem is still to be built. The total market capitalisation of cryptocurrencies was USD 12.4 Billion in June 2016 but had grown to over USD 106.6 Billion by June 2011[1]. At the time of writing this whitepaper, the total market cap for cryptocurrencies was touching USD 350 Billion. However, this growth was unaccompanied by a supporting financial infrastructure that will facilitate financial activities that are backed by derivatives, market instruments and unified markets.

Let us consider the example of a simple financial activity of applying for a loan in a traditional market. Traditionally, the lenders will estimate the borrower's capacity, acquire collateral, cross-check for over-borrowing and cross-collateralization before proceeding with the loan. Once it is issued, then this loan can be refinanced on the market. However, we don't have an efficient way to collateralise Bitcoin or other crypto assets for a crypto loan. This means that we cannot yet send the crypto assets to a multi-sig wallet which has a trusted signatory who serves as the prospective lender.

This missing crypto asset infrastructure will not only enable simple financial activities but also enable the more sophisticated ones sought after by investors such as hedgers, speculators, margin traders etc. And there is a massive demand for it. The capital markets are valued at 118 Trillion USD[2] while the derivatives market that leverages assets, including the ones from capital markets, are estimated around USD 1.2 Quadrillion[3].

Once this challenge is resolved, it will enable the crypto future markets that are needed for planning investments, controlling risk exposure and price discovery functions. However, there is no native crypto derivatives market now, leaving this market opportunity untapped.

Multiple attempts have been made to address these issues. However, due to the significant differences between crypto and traditional assets, crypto derivatives and financial market instruments can't be built the conventional way. Bitfinex was one of the earliest operators to offer Bitcoin futures. Bitfinex offered a new token class called Chain Spit Token (CST) that will allow market participants to speculate on the outcome of potential cryptocurrency protocol change. However, the platform was compromised in 2016.

The approach towards creating a crypto financial infrastructure should be fundamentally different to the traditional financial infrastructures because crypto assets and traditional assets are fundamentally different. We will first elaborate what are the key differences between crypto and traditional asset, then elaborate why the desirable financial structures for crypto assets can't be built by replicating the traditional financial structures. Then, this paper develops the vision of how these financial structures should be built with a technical overview and examples.

The key difference between cryptocurrency and traditional currency is that the former must have 1) transaction rules, 2) a network and 3) an asset all in one while a traditional currency is simply a representation of value. This is fundamentally different from traditional assets like the US Dollar. The US dollar's transaction rules, for example, how to finalize and settle a transfer, is not an inherent property of USD but rather defined by how the transaction is executed. Similarly, its settlement network is also defined outside of the currency by intermediaries like VISA, MasterCard, PayPal etc.

In comparison, a Bitcoin's transaction is carried by the Bitcoin network; it's finalized by the record on the Bitcoin blockchain. These defining attributes of Bitcoin cannot be separated from it, similar to the way the settlement network and the transaction rules are separated for USD. Similarly, Ethereum cannot be viewed just as an asset. It is a faster alternative to Bitcoin network. However, its principal value is derived from its capacity to enable a wide range of smart-contract assets, from ICO to car ownership[4], loan[5] and university payment tokens[6].

These defining differences lead to unique requirements for the supporting crypto financial infrastructure. These structures cannot be built by replicating their traditional counterparts because the crypto infrastructure will have to 1) support functionalities of the underlying crypto assets, 2) reconcile the differences in asset value in the different networks and in other markets, as well as 3) redefine the accountability for the transactions undertaken. Let us take each of those requirements in detail.

First, financial structures based on cryptocurrencies are expected to serve the needs of the crypto assets enabled by the cryptocurrencies. This is because crypto assets and cryptocurrencies are enabled by the same network with the same underlying technology. As an example, a user who can buy a cup of coffee with Ether should also be able to buy a coffee with an ICO token, if he has an appropriate smart contract.

Whereas, traditional market instruments are bound by their asset classes. The Money Market is different from the Commodity Market. It is impossible to transfer commodity titles via the VISA network. With new crypto assets, this is no longer the case. If Ether can serve as a collateral of a loan, then ICO tokens purchased with Ether should also be able to serve as the collateral for the loan. If Ether owners can use the Futures Market to hedge against the price volatility of Ether, they should be able to do so with the ICO tokens they purchased, too.

Second, the fact that a crypto settlement is carried out on the same network like the one in which it is defined, leads to a situation where traditional assets have multiple representations. There is a USD representation on Ethereum, on specialised blockchains like USDT as well as on Bitcoin blockchain. Financial market instruments which handle such assets will not only have to deal with different networks but also the differences in value on different networks. USDT, for example, trades at a price close to but not equal to USD.

Third, the current financial order is built on accountability and responsibility. Today, the executives of a traditional financial institution can be penalised for transactions such as terrorism financing, which they did not conduct. However, they are compensated for the risk and the administration of the processes.

However, cryptocurrencies can be transacted without anyone being responsible for the execution. The execution happens in smart-contracts where no one has direct control over. Vitalik, the founder of Ethereum foundation, cannot be punished by misconducts carried by the use of Ether, nor is he compensated for that risk. Therefore, the crypto financial structure can't be built on the current accountability model. Many financial services are built around the availability of accountable entities. For the US dollar, the Federal Reserve is accountable for its supply and value. This "find accountable person" model can't be re-used for crypto.

The current accountability model for financial structures leads to highly accountable entities for highly valued financial activities. Banks are so enormous and influential that we almost forgot that they are created by the limitation of the underlying financial technology which requires accountability. Internet, not needing such central entities, grew in a very different path than the financial industry. Hence, we can envision the financial structures around crypto to be different from the centralised approach taken by the banks. It is meaningless to set up a Cryptocurrency International Settlement Bank to settle cryptocurrency transactions across the border.

Realising this, Olympus Labs focused itself on the technologies that can enable the financial products, services and applications, instead of becoming the accountable party of new financial products and providers of new services. What we need is a technical framework that addresses these financial needs in a way suitable for crypto. Such a framework would consist of crypto protocols, standards, oracles, trustless market providers, reference software implementations and libraries. We will address these in the following chapters with some example asset types and the technologies needed to put them to work.

Major financial products, services and applications

There are dozens of financial products available in the traditional market today. They are essentially securities and investments created for investors to make short or long-term gains. These financial products play a major role in the economy by providing liquidity and serve as the key tools for risk management. Many of the financial products are inform of contracts that are negotiated for a price in a financial market. The contracts stipulate cash movement, at present or in future, depending on the contract conditions. Traditionally the financial products are issued by banks, financial institutions, stock brokers, government etc. and they range from shares, bonds, mutual funds to credit default swaps and collateralised debt obligations.

There are many other financial products that are created to cater to the needs of individuals and institutions. Debt and insurance comprise a major share of all the financial products. These products are often meshed with the other investment products based on the way debt is financed by the lending institution and how the lender choses to manage the risk. Some of the products are called as derivatives, because their value is derived by the value of the underlying assets. Its value is determined by the underlying assets. Futures, Options, Forward contracts and swaps are all different forms of derivative products.

Futures market is a bit different in that the participants auction on commodities and contracts underwritten by a variety of assets, for delivery on a specified future date. Future contracts were created to manage the volatility by producers and suppliers of commodities. They negotiate the contract with an investor who is ready to take on both the risk and reward of a volatile market. Future market also serve as an important roles as a price discovery function of the value of assets in future.

In addition to these products, there are financial services that are based on them or facilitate them. Credit rating is a major example of such a service. Custodian services, settlement etc. are types of these services. These services are focused on enabling the transaction and completing it. These services have become so crucial to our economy that the institutions that provide them have morphed into giants in the financial industry in their own right.

The investor gains access to liquidity for his investments through a market. The most well-known among such market place is the stock exchange. Ever since Dutch East India company issued the world’s first shares in 1601, equity markets played a crucial role in facilitating transactions by matching demand with supply of the shares in circulation. There are other exchanges classified mainly by the type of assets they transact. Some of the other key markets are commodities market, currency market, money markets, futures and derivatives market etc. Today all these markets are facilitated by different exchanges, some of which specialise on only one type of assets or products.

As you consider this complicated ecosystem of products, services and markets that facilitates transactions in a traditional environment, it is evident that the crypto infrastructure should be created in an entirely new way because the conditions to facilitate crypto transactions are completely different. In a crypto world, most of the financial services should ideally be decentralised and integrated into the network protocols. One of the key infrastructure would be to create a decentralised exchange.

Decentralised exchange

One of the most infamous episodes in Bitcoin history happened when one of the earliest crypto exchanges was compromised. MtGox was the biggest bitcoin exchange at the time, handling about 70% of the world’s Bitcoin transactions. However, the exchange was centralised in the sense that the buyers were matched with sellers through traditional mechanisms. Also the private key management of the users who transacted also fell short of the Bitcoin standard. This ultimately lead to the hack of the exchange in early 2014, when 850,000 Bitcoin that belonged to the company’s customers were found missing. Bitcoinica was another Bitcoin exchange that was build on the traditional methods but was compromised in 2012, leading to the loss of 43,000 Bitcoins. These events serve as a stark reminder of the fact that traditional and crypto methods does not gel well together. Cryptocurrencies and crypto assets have the capacity to exchange without introducing a 3rd party escrow, hence eliminating the counterparty risk in using an exchange. This is enabled by their smart-contract feature. More specifically, a type of smart-contract called hashed timelock contracts.

As long as fiat currencies are concerned, a certain level of centralisation is necessary because there is no other way of ensuring the transactions are atomic other than escrowing it through on intermediary. Hashed time-lock contracts can overcome this shortcoming of traditional currencies and enable a completely decentralised exchange.

This, however, is not going to be the case for crypto assets. The tethered crypto currency USDT played an important role in facilitating crypto-only exchanges like bittrex and binance. Interestingly, a Chinese counterpart of bittrex was established after PBOC's ban on crypto trade. Further down in the future, national authorities, like Singapore Monetary Authority, are planning to issue fiat currency in crypto, and it is reasonable to expect that it will support smart contract or hash-based contract.

In the next chapter, we will introduce hashed timeclock contracts and how to use them to facilitate decentralised exchange.

The multiple methods of decentralised exchange There are generally three methods for constructing decentralised crypto exchanges. Before we enumerate these types, let us put forward the expectations of an decentralized exchange, and evaluate the fitness of the methods accordingly.

By decentralized exchanges, we refer to decentralized crypto exchanges - exchanging from one cryptocurrency or cryptoasset to another. Any transaction related to fiat currency has to be carried out with a crypto fiat token like USDT.

Exchanges provide liquidity by matching and executing orders. Decentralised exchanges can match and execute orders without third-party escrow. Executing orders, arguably, is the most important function, since a self-interesting user-agent can find the best order to match. There are three expectations of order execution method, and there are three distinct ways to execute orders without using a third-party escrow.

1. BASED ON ETHEREUM:

Ethereum's capacity to represent crypto token within Ethereum. The most prominent being 0x (https://0xproject.com/) although various endeavours on this type of exchange happened long before. This method can only handle exchanges between Ether and crypto assets defined by Ethereum (ERC20) contracts, or two ERC30 assets. Consider Bitcoin is the biggest cryptocurrency by market cap, any solution not compatible with Bitcoin are not addressing the entire need.

1. USING SPECIAL BLOCKCHAIN

The second relies on miners seeking SPV proof on a specialised blockchain. Cosmos is a blockchain solution based on this thinking. The solution faces a few dilemmas on implementation and game theory which deteriorates its serviceability. This design's implications are complicated and deserve its own chapter for explanation.

1. USING HASHED TIMELOCK CONTRACTS

The idea of using smart-contracts to exchange assets cross chain was an old one. Smart-contract are too expensive to carry out the entire function of an exchange, but it can do the core function: order execution. Other functions can be built on top of the core functionality with relative ease.

The type of smart contract which can execute orders across different blockchain is a special type called Hashed Timelock Contracts, thanks to its use of cryptographic hash. Since smart contracts can't access information outside of their blockchain, the trading parties have to provide the information. And because the trading parties do not trust each other, the cryptographic open-commit two-phase protocol was used, which requires hashed timelock.

We will discuss the first proposed protocol 2013, The Tier Nolan protocol for Atomic Cross-Chain Exchange; then we will discuss the features we need from cross chain asset exchanges, and shortcoming of Tier Nolan protocol. Finally, we provide a method to amend Tier Nolan protocol to be used as the core functionality of decentralised exchange.

Using Hashed Timelock Contract, Tier Nolan protocol

Tier Nolan's model consists of 3 phases, prepare, commit and open.

1. In the setup phase, either party can walk away without losing asset or opportunity;
2. In the commit phase, either party can walk away without losing asset;
3. In the open phase, if the first party opens, both parties finalise the exchange; otherwise both take back their asset, losing the opportunity.

The following demonstration is based on an asset exchange between Bitcoin and Bitcoin Cash, since Bitcoin is the most widely used crypto and Bitcoin Cash is symmetric to it. The Ethereum version of it can be created in a similar fashion.

Setup Phase:

Cryptographic commitment requires a random number generator and a hash function. Since we are focusing on order execution, we assume negotiation was accomplished before the protocol starts. We also assume that there are two trading parties: Alice who has Bitcoin and Bob who has Bitcoin cash. Multi-party protocols can be extended later.

The protocol is not symmetric. It requires one party to start, which we assume to be Alice.

In the prepare phase, Alice generates a random number x, uses a hash function $H(x)$ to obtain a hash h:

$h := H(x)$

She needs 2 transactions in this phrase. She creates an unsigned transaction **TX1**, with two redeem conditions:

- either redeemable by providing an x which satisfies $H(x) == h$, and signed by Bob, or;
- redeemable by providing the digital signatures from both Alice and Bob;

She then proceeds on to produce a timeout transaction for **TX1**, spending its input back to Alice with a timeout (`nLocktime`). A timeout transaction does not provide x; it uses the other redeem rule which requires Alice and Bob's signature.

Alice signs the timeout transaction and sends it to Bob with **TX1**, who signs it and returns it to Alice.

Bob learns h from Alice and does the same, creating a transaction **TX1'** and its timeout transaction from his Bitcoin Cash with similar redeem conditions:

- either redeemable by providing an x which satisfies $H(x) == h$, and signed by Alice, or;
- redeemable by providing the digital signatures from both Alice and Bob;

The timeout transaction, likewise, spends from **TX1'** and outputs it back to Bob with a timeout.

The timeout value should be long enough to allow 4 transactions to be added to the blockchain.

Commit phase

TX1 and **TX1'** are committed transactions: Alice and Bob commit their asset which can be redeemed only by revealing x, before the timeout. Alice then must sign her **TX1** and publish it on the Bitcoin blockchain. This process takes an hour or more.

Bob, seeing the transaction on Bitcoin blockchain, sign his **TX1'** and publish it on the Bitcoin Cash blockchain. This process again takes an hour or more.

At this stage, both parties have committed for the trade. They lose the opportunity to do other trades with the same fund until this trade is successfully carried out or times out.

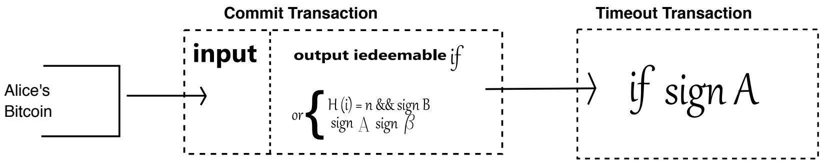
Open phase

Alice, confident that both parties have committed, creates a transaction **TX2'** on Bitcoin Cash blockchain, spending **TX1'** to her address on Bitcoin Cash blockchain. She is able to do so because she possesses x.

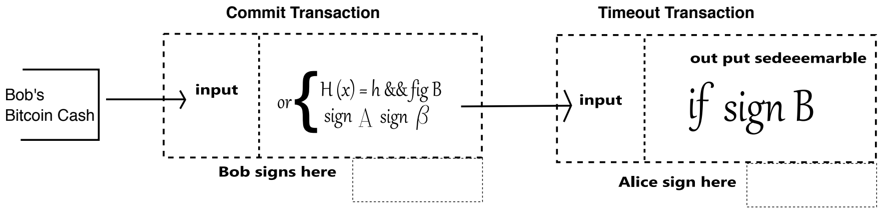
Bob observes that his transaction **TX1'** is redeemed by Alice using x. He then proceeds on to redeem Alice's transaction **TX1** with the same x. Protocol finalised.

If Alice does not enter the open phase correctly, both parties redeem back their asset and no trade happens.

0. Alice generates a random number x, calculates its hash h
1. Alice sends 2 transactions to bob



2. Bob signs the timeout transaction, send it back to Alice, learning h
3. Bob sends 2 transactions to Alice



4. Alice signs the timeout transaction, send it back to Bob
5. Alice and Bob both sign and put their commit transaction on the blockchain

The requirements of a decentralised exchange

Tier Nolan protocol was first published in 2013, but so far no decentralised exchanges used this method because it does not satisfy all the requirements of an order execution process. We can enumerate these requirements by observing traditional exchange order execution: the execution has to be committed, atomic and binding.

Commited

: Both party enters the trade with funds. As soon as both party enter the trade, the funds can't be used for other purposes.

Atomic

: The protocol is either terminates by a successful trade or terminates by returning funds to the original owners. Furthermore, it terminates.

Binding : Once both parties are committed to the trade, it only terminates by a successful trade, not terminate by returning funds to the original owner.

The three requirements can be explained in trader's words:

Committed ~ you can't make an order if you don't deposit money.

Atomic ~ if your order is accepted, you either get what you ordered or get a refund.

Binding ~ if your order is accepted, you get what you ordered.

The atomic property can be elaborated by saying that the scenarios cannot happen: 1) Alice transferred Bitcoin to Bob, but Bob did not transfer Bitcoin Cash to Alice; 2) Bob transferred Bitcoin Cash to Alice, but Alice did not transfer Bitcoin to Bob. In other words, an asset exchange is either successful for both parties, or for none. Before crypto, when asset and currency were distinct concepts, this was commonly called Delivery-versus-payment, meaning the delivery of asset happens as the payment with currency. We have had this problem for the entirety of human trade activities, but it wasn't until blockchain was invented that this can be solved without inviting a 3rd party escrow.

Observe the Tier Nolan protocol, it is committed, atomic but not binding. At any of the three stages, the starting party in the protocol, Alice, can terminate the protocol by doing nothing at all. Consider that the entire order could take several hours to execute, Alice would be incentivized to walk away from a trade if the change in price is disadvantages to Alice. Bob, however, doesn't have this advantage. This creates a dilemma where both parties want to play the starting role.

The improved Tier Nolan protocol

Tier Nolan protocol can be improved by adding a binding phase at the very beginning.

Binding phase

By requiring Alice to not only provide a deposit (be committed), we can further require Alice to provide an ante (be bound).

Alice creates and broadcasts an ante - a signed transaction with the following redeem conditions:

- either redeemable by providing an x which satisfies *H(x) == h*, and signed by Alice, or;
- redeemable by providing the digital signatures from both Alice and Bob;

She then creates a timeout transaction for the ante, which is redeemable by Bob with a `nLocktime`. She pre-signs that transaction, passes it to Bob. The value of this `nLocktime` has to be smaller than the timeout of the commit transactions.

Having received the timeout transaction, Bob will either receive Alice's committed asset in exchange for his or, if Alice refuses to reveal *x*, Bob will receive Alice's ante through the ante's timeout transaction. Either way, Bob can acquire Alice's asset.

Secured Loan

We demonstrated that cross chain exchange - a financial service traditionally hosted by trusted third parties - can be done with trustless blockchain technology. We then proceed on to the realm of financial product. Secured loan is a basic financial product. It has a time element in it - loans are not returned immediately. The decentralised technologies used for secured loan are the basis more complicated products like futures and swaps.

Protocol

Let us assume Alice wants to use her Bitcoins as collateral to secure some loan in other crypto than Bitcoin. Instead of continuing Bitcoin Cash as the example, this time we demonstrate an Ether loan. We can show that smart-contract, as defined by EVM, can interact with Bitcoin and other more traditional blockchains. There is also a technical consideration, that if we are to use Bitcoin Cash loan, we will rely on `SIGHASH_ANYONECANPAY` - a Bitcoin construct unfamiliar to most readers - since blockchains based on UXTO doesn't have the concept of Account, making the source of the loan payment unpredictable.

In the example, Alice has Bitcoins to use as collateral to secure a loan in Ether. Bob is a lender who has Ethers. Since lenders are usually market makers, we assume Bob commit first.

This time we provide the protocol first and then examine the phases.

1. Bob generates a random number *x* and its hash *h*.
2. Bob deposit his Ether into a smart-contract, let us call it Loan Contract. Bob commits *h* in the same transaction. He can take the money out by revealing *x*.
3. Alice transfers her collateral Bitcoins to a transaction with the following redeem condition: It can be redeemed by providing *x* which satisfies $H(x) == h$ and signed by Alice.
4. Bob, confirming that the collateral is recorded on the Bitcoin blockchain, release the loan by signing a release to the smart-contract, who in turn releases the loan to Alice's Ethereum address.
5. After a while, Alice repays the payment to the Ethereum contract with interest.
6. Bob sends a transaction to the smart-contract, revealing *x* and acquires the loan principal and interest.
7. Alice, learning the value of *x*, uses that to create a redeem transaction, redeeming the collateral to herself.

The entire transaction consists of the following phases.

Commit phase

In step 2, Bob commits his Ether into a contract. At this point, Alice may or may not continue the protocol. If Alice bails out, Bob can redeem his money by revealing *x*, the equivalent of cancelling a loan offer.

If Alice continues, committing her collateral, she may be concerned if Bob would reveal *x* and quit. Should that happen, Alice can do nothing but redeeming her collateral by providing the *x*.

In the commit phase, each party can walk out without penalty.

Release phase

Once Bob sees that the collateral was correctly recorded on the Bitcoin blockchain, he releases the Ether fund to Alice. At this point, the smart-contract won't continue unless the fund was returned, and the collateral is held locked. Neither Alice nor Bob can operate on it.

End phase

When Alice paid the loan back in full - principal and interest, as per Loan contract dictate, Bob has to reveal *x* to retrieve the fund, which leads to Alice acquiring the collateral.

The protocol is demonstrated in the following diagram:

Ethereum Smart Contract | Bitcoin

1. Bob deposits, committing h

```
contract Loan {

 function deposite(byte32 h)
 ...
 function release(address lender)
 ...
 function repay()
 ...
 function withdraw(byte32 x)
 ...
}
```

2. Alice sends Bitcoin to collateral transaction

```
Input:
Alice's bitcoin

Output:
Redeemable if
 - provide x such that H(x) == h
&&
 - signed by Alice
```

3. Bob releases the loan

```
Loan.release(alice_address)
```

4. Alice pays back the loan

```
Loan.repay()
```

5. Bob withdraws, revealing x

```
Loan.withdraw(x)
```

6. Alice redeems the collateral with x

It's worth noting that the smart-contract has to be written in the way that Bob can only withdraw the loan payment if Alice paid the entire principal and interest. If Bob can withdraw partial payment, then there are different undesirable outcomes depending on whether or not the smart-contract requires Bob to reveal *x* in a partial withdrawal. If Bob is required to reveal *x* in a partial withdrawal, then Alice will be able to regain the collateralized Bitcoin before the loan is entirely paid back. This, of course, will incentivize Bob to withdraw as late as possible, and incentivize Alice to not to pay the last bit of the loan, knowing that Bob will find getting most of the payment is better than waiting for a last 1% which may never come. If Bob is not required to reveal *x* in a partial withdrawal, then Bob can simply not withdraw the final 1%, effectively recovering the loan payment without letting go the collateral. There is no advantage to be gained by Bob of such nasty behaviour, but if Bob knows Alice, he can use this to blackmail her.

Terminatable protocol

This simple loan protocol does not involve timeout, therefore, it does not default. If Alice failed to make the loan repayment, Bob will be waiting forever for the payment, while Alice effectively lose control over the collateral. Alice may not have the capacity to repay the loan with compound interest, yet Bob not able to liquidate the collateral. Therefore, a point in time as termination is needed for default to happen. There is a second disadvantage of a protocol without timeout. Bob may delay releasing the loan or quit the deal altogether, after Alice committed the collateral. There are practical cases delaying release of loan provides Bob some advantage, yet, quitting the deal can happen too, causing both the loan and collateral being locked up. Therefore, two timeouts are needed. A long one for the loan payment and a short one for the loan release. Adding these timeout, however, is non-trivial. We will cover this topic in the upcoming technical detail documentations.

Tokenomics

All transactions carried out on the Olympus Ecosystem, including product creating, payment settlements, product purchases, and transactions on the exchange, are subject to fees in order to prevent network abuse and encourage a healthy ecosystem. The fees required for the transactions are specified in units of gas. Gas is used to pay the fees for all transactions that deploy on the Olympus blockchain or the Olympus smart contract. The specific amount of gas required for each transaction depends on the type of the transaction and the amount of system resources required to execute it. Gas only exists in the context of executing transactions in the Olympus Ecosystem. MOT (Mount Olympus Tokens) are used to purchase the gas used to conduct the transactions, so the gas price is quoted in the number of MOTs. The gas price will fluctuate based on the amount of transactions on the network and the amount of resources that are available to reach an equilibrium price.

Disclaimer

THIS DOCUMENT AND ANY OTHER DOCUMENTS PUBLISHED IN ASSOCIATION WITH THIS WHITE PAPER RELATE TO A POTENTIAL TOKEN OFFERING TO PERSONS (CONTRIBUTORS) IN RESPECT OF THE INTENDED DEVELOPMENT AND USE OF THE NETWORK BY VARIOUS PARTICIPANTS. THIS DOCUMENT DOES NOT CONSTITUTE AN OFFER OF SECURITIES OR A PROMOTION, INVITATION OR SOLICITATION FOR INVESTMENT PURPOSES. THE TERMS OF THE CONTRIBUTION ARE NOT INTENDED TO BE A FINANCIAL SERVICES OFFERING DOCUMENT OR A PROSPECTUS. THE TOKEN OFFERING INVOLVES AND RELATES TO THE DEVELOPMENT AND USE OF EXPERIMENTAL SOFTWARE AND TECHNOLOGIES THAT MAY NOT COME TO FRUITION OR ACHIEVE THE OBJECTIVES SPECIFIED IN THIS WHITE PAPER. THE PURCHASE OF TOKENS REPRESENTS A HIGH RISK TO ANY CONTRIBUTORS. TOKENS DO NOT REPRESENT EQUITY, SHARES, UNITS, ROYALTIES OR RIGHTS TO CAPITAL, PROFIT OR INCOME IN THE NETWORK OR SOFTWARE OR IN THE ENTITY THAT ISSUES TOKENS OR ANY OTHER COMPANY OR INTELLECTUAL PROPERTY ASSOCIATED WITH THE NETWORK OR ANY OTHER PUBLIC OR PRIVATE ENTERPRISE, CORPORATION, FOUNDATION OR OTHER ENTITY IN ANY JURISDICTION. THE TOKEN IS NOT THEREFORE INTENDED TO REPRESENT A SECURITY INTEREST.

---

1. http://fortune.com/2017/06/26/bitcoin-blockchain-cryptocurrency-market/ ↩
2. https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Global%20Capital%20Markets/118%20trillion%20and%20counting/MGI*118*trillion*and*counting*Taking*stock*of*capital*m*
3. https://www.investopedia.com/ask/answers/052715/how-big-derivatives-market.asp ↩

4. https://www.coindesk.com/blockchain-move-self-driving-cars-fast-lane/ ↩

5. https://cointelegraph.com/press-releases/ethlend-introduces-secured-loans-on-ethereum-blockchain ↩

6. https://cointelegraph.com/news/australian-university-allows-students-to-earn-ethereum-from-campus-purchases ↩