OTC Contracts: A Decentralized Contingent Payment Platform

November 21, 2017

OTC Contracts is a blockchain-based platform for designing and trading contingent payments contracts. A contingent payment contract can be defined as any contractual agreement that involves a conditional payment triggered by an external event. An insurance policy is one form of contingent payment contract, in which a payment is made by insurer to the insured in the event of a claim. In addition to insurance, contingent payment contracts are ubiquitous elsewhere in the economy, including the financial sector, labor markets, and predictive markets. The OTC Contracts project provides a decentralized platform to design, settle, and trade contingent payment contracts.

1 Introduction

Contingent payments encompass a broad category of transactions between contracting parties, in which the amount and beneficiary of payment is determined by an external event or trigger that is uncertain at the time of agreement. There are many examples of contingent payment contracts including insurance policies, financial derivatives, event contracts, letters of credit, and collateralized agreements. The value of such contractual arrangements can be attributed to managing risk associated with uncertain events. Effective risk management is achieved through engaging in transparent reliable risk transfer between counterparties. However, contingent payment contracts are not accessible to many individuals wishing to manage risk. Entering into contractual arrangements is often prohibitively expensive requiring a legally enforceable agreement to ensure adherence to terms. The secure handling of funds requires a trusted custodian, which further adds to the cost. Moreover, geographic and jurisdictional incompatibilities can be limiting for contracts relying on traditional legal and banking systems.

Smart contracts, as described by V. Buterin [1], are globally operable cryptoeconomic vehicles that can ensure the adherence to contract terms and the secure handling of funds. Smart contracts are transparent and not subject to multiple interpretations. They can mitigate the risk of fraud and execution errors. Moreover, smart contracts are executed on decentralized platforms, like Ethereum, which precludes excessive regulation and nefarious expropriations. In most instances, the cost of using smart contracts is nominal in comparison to traditional contracts. Smart contracts offer a cost effective means of engaging in secure contingent payments.

Although smart contracts offer a promising solution, several obstacles have thwarted their adoption for practical applications. Smart contracts are inaccessible to individuals with limited knowledge of computer programming and the Ethereum Virtual Machine(EVM), the runtime environment for smart contracts in Ethereum. Professional programming and testing are necessary in the creation of smart contracts to ensure that they will perform predictably without security vulnerabilities. This was evident in the high profile hacking of the DAO [2] in 2016 and

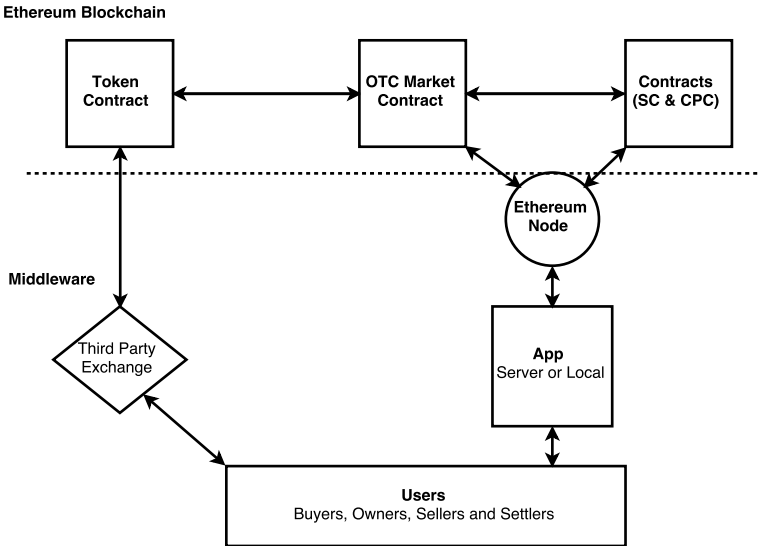

Figure 1: Architecture

the Parity Multisig Wallet [5] in 2017; both could have been prevented with adequate auditing and testing. Implementing contingent payments using smart contracts is coupled with the problem that events in the real world must accurately be translated and reported to the blockchain. P. Sztorc proposed a solution to this problem through the use of oracle corporations [6], which minimize the need for trust in reporting through the use of a reputation token and a multiplicity of reporters. The reputation token is necessary to mitigate the risk of Sybil attacks, in which an individual may post a result through multiple addresses to create the illusion of a prevalent opinion. However, oracle corporations are complex and require many reporters; they would only be suitable for reporting events that are in the public domain and that are popular enough to warrant the expense of incentivizing multiple reporters.

The Over-The-Counter(OTC) Contracts project offers an over-the-counter market of secure standardized smart contracts that can be used for settlement and contingent payments along with an intuitive application that is accessible through a web browser. OTC Contracts focuses on strategic business partners to serve as identifiable and accountable reporters while permitting the appropriate use of oracle corporations. The OTC Contracts project overcomes many of the obstacles thwarting the adoption of smart contracts for contingent payments. OTC Contracts will enable any individual to take advantage of smart contracts to cost effectively manage risk in a secure environment.

2 The Platform

The OTC Contracts Platform exist on two levels of blockchain and middleware. The Ethereum blockchain holds the OTC Market Contract, Token Contract and Contracts for settlement and contingent payments. A Contract will be referred to as a Settlement Contract(SC) or Contingent Payment Contract(CPC) according to its functionality as defined by its state. The conduit to the blockchain is a full stack middleware application. Users interact with the Ethereum contracts through the user interface of the conduit application that connects to the blockchain through an Ethereum node. The user has the option of downloading the conduit application or accessing an online version. In either case, the user can connect with their own private node or use a node provider like Mewify or MetaMask.

The users of the OTC Contracts platform can be categorized as settlers, traders, and owners. Settlers report on the outcome of events through the use of the settlement functions of Con-

tracts. Traders are the buyers and sellers of contingent payments in Contracts. The owners of Contracts and tokens compose the last category of users. Contracts and tokens are the assets of the platform; they are both exchangeable for one and other through functions of the OTC Market Contract.

3 Conduit Application

Users interact with the Ethereum blockchain level of the OTC Contracts platform using the conduit application. The goal of the conduit application is to create a user experience that is intuitive and predictable. The OTC Contract platform is standardized so that the user interface can be made accessible to users with limited knowledge of smart contracts and the EVM. Users will be able to utilize Contracts of interest through an intuitive user interface and bypass the underlying technicalities of smart contracts and blockchain technology.

Settlers can market their own settlement services and access SCs with OTC Contracts' conduit application. An existing business may become a settler by integrating the OTC Contracts' conduit application into their existing systems. For example, a business that reports on the outcome of weather events may publish SC addresses on their website in pending state before posting event outcomes to SCs. Users can access the OTC Contracts' user interface and enter into CPCs that will be settled by these events by querying the OTC Market Contract for the published SC addresses. Businesses can embed the OTC Contracts' functionality into their existing business models to more effectively deliver their services and create new use cases. OTC Contracts offers established event reporters a means to report outcomes to the blockchain and the ability to earn a fee every time their result is called.

Traders can use the OTC Contracts' conduit application to query CPCs from the OTC Market Contract based on the SC addresses. The trader will receive a list of all CPCs in the form of an order book. Traders can lease contracts to post offers in a certain settlement market or buy existing positions from contracted parties wanting to exit their CPC positions.

Owners can redeem tokens for Contracts and recycle Contracts for tokens through the conduit application. This is discussed in more detail later sections.

3.1 Contract Administration

The OTC Contracts platform involves features associated with the ownership and leasing of Contracts. The conduit applications provides an interface for:

1. Redeeming tokens for Contracts and recycling Contracts for tokens
2. Setting rent and collecting the rent for owned Contracts
3. Leasing Contracts
4. Setting the settlement fee, posting results and collecting fees for SCs
5. Requesting settlement in a CPC

3.2 Order Book

The conduit application provides an interface for users to perform the following operations related to managing market positions:

1. Call the Contract ledger from the OTC Market Contract
2. Call variables from the individual Contracts on the ledger

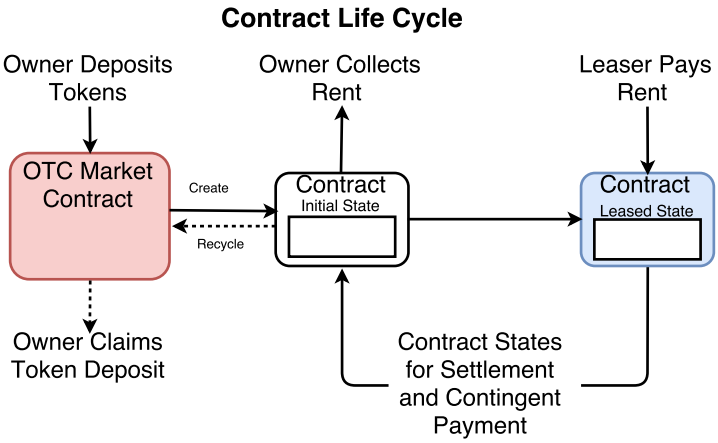

Figure 2: Contract Life Cycle

3. Store a database of Contract information that can be queried
4. Display queried information to users
5. Execute Contract functions

An order book for a specific settlement is created from a query of the Contracts by settlement and state. The Contracts listed can be sorted according to the cost of the position on the event. This way the user can bid on the most valuable contracts in the settlement market. The conduit application database can be in a central location or the user can run the conduit application locally.

The Contract interface enables the user to manage positions in Contracts. The position management occurs in the individual Contracts and not submitted in an exchange for execution. In this way, the market and settlement is operated in a totally peer-to-peer setting. The Contracts are sold and bought over-the-counter without central settlement.

4 Contracts

Contracts compose the basic units of the OTC Contracts ecosystem. Contracts have two functions: settlement and contingent payment. Each Contract has an owner and is created using the OTC Market Contract. Contract creation requires the redemption of tokens at the conversion value along with the gas cost for creation on the Ethereum blockchain. The Contract owner sets the rent for the Contract. Users interested in offering settlement or engaging in contingent payments, lease the Contract for a period of time by paying rent to the Contract. The owner can withdraw the Contract's accumulated rent at the end of the lease or at any time the Contract is in Initial state. Contracts in Initial state only have the owner and rent defined. In Initial state, Contracts can be leased for settlement or contingent payment.

4.1 Settlement Contracts

Settlers require a SC to report events to settle other Contracts. The settler acquires a SC by leasing a Contract in Initial state. Once the Contract is in Leased state, the settler is defined as the leaser. As the leaser, the settler can define the settlement fee moving the SC into SettlementPending state. The settlement fee is the amount that a CPC must pay the SC to receive the result once it is posted. The settler will make the address of the SC public to users

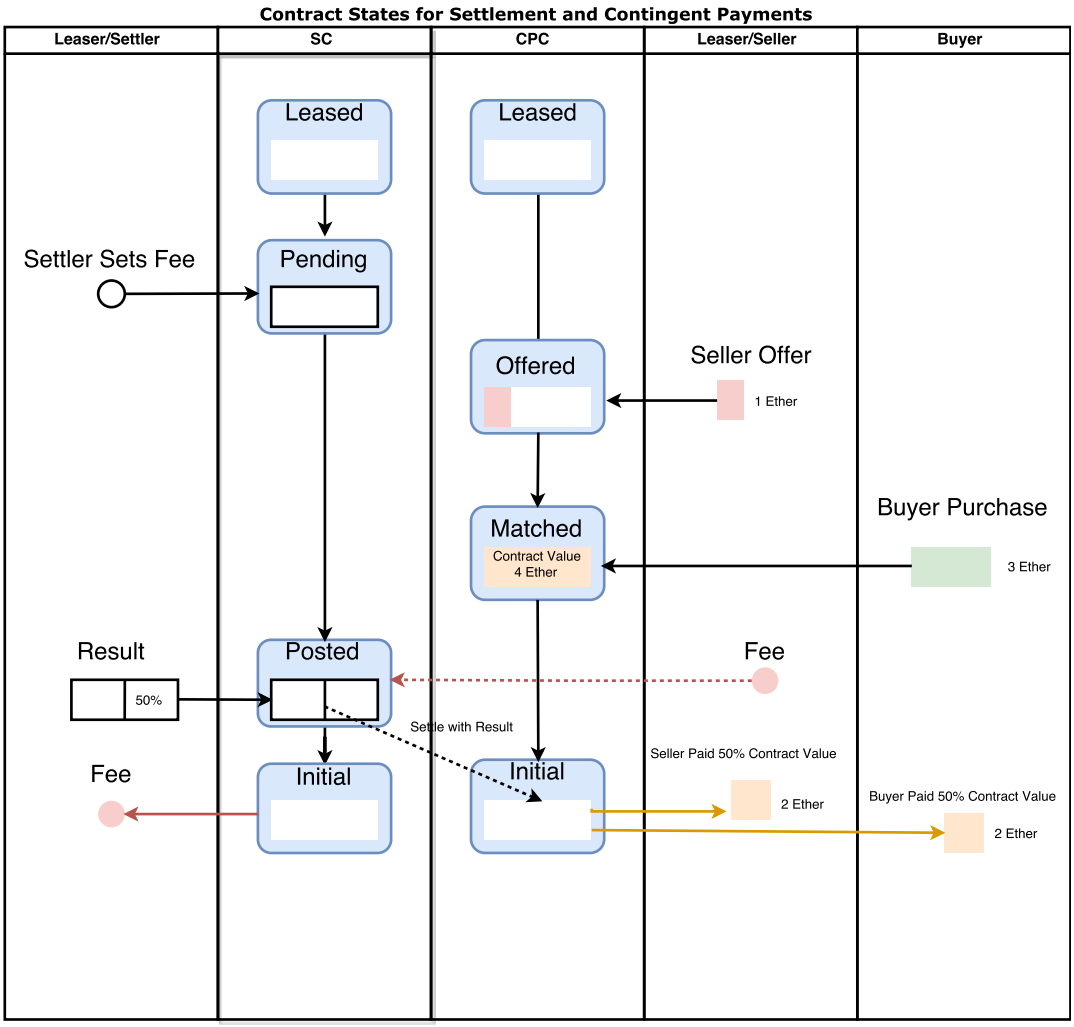

Figure 3: Contract Interaction Example

wishing to write the SC into their CPCs. The settler will publish how the result value will be determined from the event result when it becomes available.

After the result becomes available, the settler will post the result to the SC moving the SC to Posted state. CPCs can be settled by sending the SC the settlement fee while the SC is in Posted state. In this state, the SC accumulates the settlement fees from settlement requests. Once the settlement period is over, the settler can withdraw the accumulated fees moving the state from Posted to Initial. In the Initial state, the settler no longer has control of the Contract.

4.2 Contingent Payment Contracts

A user wishing to enter into a CPC takes the position of the seller. The seller leases the CPC for a specified duration by paying the rent to a Contract in Initial state. As the leaser, the seller defines the SC address, unit value and offers the amount of the contingent payment moving the CPC from Leased state to Offered state. The buyer accepts the offer by paying the CPC the unit value, which moves the CPC into Matched state. The total amount to be settled is the contract value, which is the sum of the offer paid to the CPC by the seller and the unit value paid to CPC by the buyer. The SC address that is assigned in the CPC by the seller defines the event result that will determine how the contract is settled. That is, the SC result will determine how the contract value will be split between the buyer and seller.

There is a secondary market in the conduit application that lists the CPCs in Matched state. The secondary market enables the buyer and seller to sell their respective positions in the CPC to another counterparty for a specified amount in Ether. A position in a CPC is always worth less than its contract value so by default the cost is set to the contract value.

After a result is posted to the SC, the settlement function in the CPC can be called that requests settlement from the SC. The SC in posted state automatically responds with the posted result to the CPC, which settles the contract between the counterparties. The CPC sends the appropriate portions of the contract value to the buyer and seller according to the result value. After the CPC is settled, the contract state reverts to the Initial state.

5 Tokens and Contracts

The interaction between tokens and contracts occurs in the Token Contract and OTC Market Contract portions of the platform. Each token is called a Tera "T" and total number of tokens in circulation is fixed at one million T.

The OTC Market Contract has the function createContract. Conversion value is the cost of a Contract in tokens. Initially this cost is one T per Contract. If a tokenholder wants to redeem their token for a Contract, they call the createContract function. This transfers one T from the tokenholder to the Token Repository Account and the OTC Market Contract writes the tokenholder's address as owner of one Contract storing the Contract address and the deposit value in the OTC Market Contract's contract ledger. The newly created Contract is in Initial state and can be leased at the rental rate determined by the owner.

The OTC Market Contact has a recycleContract function that is analogous to the inverse of the createContract function. When a Contract owner submits their Contract address to recycleContract, the Contract is located in the contract ledger. The owner of the Contract is changed to the Contract Repository Account and former owner is transferred the deposit tokens listed on the contract ledger. Contracts owned by the Contract Repository Account are not available for leasing. These contracts can be used by the createContract function and assigned to new owners instead of creating new Contracts at the higher gas charge. A new and recycled Contract are functionally identical. Hence, a recycled Contract will be issued by default in the OTC Market Contract if there are recycled Contracts available.

The conversion value is subject to change based on the number of Contracts leased. If there are many leased Contracts, the conversion value is adjusted lower so that the Contract owners can recycle Contracts for the deposit on the ledger and purchase a greater number of Contracts with the same deposit. The maximum conversion value is one T per Contract and conversion value is inversely related to the number of Contracts leased.

The gas cost of creating a Contract must be paid by the Contract owner when the Contract is created. It is possible for a tokenholder to increase the number of Contracts leased by creating Contracts and self-leasing them. In this way, the tokenholder could manipulate the conversion value of Contracts to a lower level. However, the gas cost for creating Contracts would make such a manipulation expensive and the manipulator would not gain any advantage over other Contract owners who would be able to create Contracts at the same conversion value.

When a Contract series is upgraded a new OTC Market Contract is deployed using the same Token Contract, which allows the owners of the prior series to recycle their Contracts and use the deposit to purchase the new series.

The correspondence between tokens and Contracts creates the following properties:

1. A fixed number of tokens from genesis
2. An effective means of increasing the Contract supply without diluting the token value
3. An effective means of upgrading the Contract series as needed

4. Using economic incentives to manage the supply and functionality of Contracts

6 Market Contract

The OTC Market Contract creates Contracts upon the redemption of tokens and refunds tokens upon the recycling of Contracts. The OTC Market Contract maintains the list of valid Contracts that are available for leasing, trading, and purchasing. The OTC Market Contract interacts directly with the Token Contract and stores the tokens deposited with each Contract creation in the Token Repository Account.

The OTC Market Contract ledger store the deposits information and Contract addresses. The OTC Market Contract will determine the conversion value, which was defined as the token cost of a Contract. A sample size is calculated to determine the fraction of Contracts leased within a 95 percent confidence interval based on the number of Contracts listed in the ledger. This is accomplished by maintaining a moving average of percentage of Contracts leased, which is updated every time a Contract is created.

The OTC Market Contract maintains the ledger of Contracts. The system of Contracts is closed. A SC can only settle a CPC that is on the OTC Market Contract ledger. This will preclude smart contracts created outside of the OTC Contracts platform from using SCs for settlement. Externally created contracts might not perform consistently with CPCs. Maintaining an closed structure strengthens the network promoting standardization and security.

7 Settlement Integrity

An essential component of contingent payment contracts is reliable settlement. In the OTC Contracts, the settler is an identifiable and established business that has embedded OTC Contracts into their business model. This is an entity that could be held accountable for their reporting services. Individuals using the settlement reporting of such an entity would understand who they are relying on for settlement so that they can make an informed trust assessment. For instance, it would reasonable to trust settlement from a settler if the size of the settler's business and reputation greatly exceed the scale of the settlement they are proposing. For example, if the settler was a popular news service and they advertise that the results reported are based on an algorithm pulling data directly from an exchange API to ensure the integrity. Such an entity could be held liable for false advertising or fraud if there was a misreporting of results due a lack of adherence to advertised protocols. An alternative business to a news service could be an oracle corporation with a transparent system of ascertaining truth and reporting it to SCs. Such an oracle corporation could have a set of SCs embedded in their smart contracts that are automatically reported and the fees collected and redistributed to the reporters.

8 Performance and Scalability

One of the main concerns in blockchain technology is network performance. Exchange products in predictive markets and derivative markets rely on high speed trading platforms with low latency to remain viable. These platforms seek to recreate established markets that currently trade with a high liquidity and low latency in centralized exchanges. The current performance of the EVM will not permit high speed trading algorithms and arbitrage that can support established markets. There is some limited trading available in these markets, but the spreads and slow execution makes them too inefficient for large trading volumes. In established markets, traders require efficiency; they cannot operate in markets without liquidity because they are unable to adjust their positions quickly and reliably. For example, a stop-loss order would be

undesirable in a market with low liquidity because large spreads could result in orders remaining unfilled or filled at prices far below the stop-loss level, defeating the purpose of the stop-loss order.

OTC Contracts does not rely on recreating established markets. Trading on events with established markets in centralized exchanges will occur, but these Contracts are traded over-the-counter in a peer-to-peer environment. Counterparties may negotiate the agreement prior to engaging in a Contract in the same way that over-the-counter financial derivatives are negotiated. OTC Contracts will be used to execute and transfer funds securely. Instead of every trader entering a market by posting an anonymous offer, the users of OTC Contracts will often have established contact in the course of normal business and use OTC Contracts to execute their agreements. This approach creates a system that is valuable in higher latency environments.

OTC Contracts are tradeable. A counterparty can sell their position in a Contract in the secondary market through the Contract without relying on any broker or middleman. Liquidity in secondary markets will be subject to the performance of the EVM. Contracts can be settled according to customized specifications to meet the needs of a specific business transaction. For example, a manufacturer may engage in a Contract with a retail purchaser using a fulfillment company providing settlement. This versatility enables the OTC economy to evolve with the technology and remain effective with uncertain performance.

OTC Contracts offers value with Ethereum's current transaction speeds. However, OTC Contracts also has a long term scaling plan that will be offered as an upgrade when new technologies have been adequately developed. The plan consists of moving the Contracts portion of the platform to a separate OTC proof-of-stake network with all account deposits and withdrawals occurring in the OTC Market Contract that resides on the Ethereum blockchain. The ledger of account balances will be transfered between the Ethereum blockchain and the OTC proof-of-stake network. The OTC proof-of-stake network will operate Contract executions and trading. By only migrating the Contract portion of the platform, the token and Ether balances will not change and users will have the same experience with higher performance. Recent developments with Plasma chains and proof-of-stake are making such a transition possible. However, more progress will need to made before a working prototype can be constructed.

9 Applications

9.1 Event Contract

The Commodity Futures Trade Commission defines an event contract, also known as a prediction or information contract, as a derivative contract whose payoff is based on a specified event, occurrence, or value[3]. Essentially, this is a simple bet made on the outcome of an event.

A settlement service provider reports on the value of Ether. The settlement service provider reports whether or not the value of ETH is above 300 on July 31, 2017 at 12:00 GMT based on the last reported trade on a specific exchange. The settler leases a Contract and moves it to Settlement Pending state. The Contract is a settlement contract (SC) with address 0xSET. The settler also selects a fee for settlement say 0.01 Ether. The address of the settlement contract is then listed in the OTC Market Contract's ledger of valid Contracts. The settler publishes the address 0xSET with the specifications of the event on their own website with a link to the OTC Contract user site.

A hedger is bearish on the performance of ETH until August 2017 and he wants to protect profits on his Ether holdings. The hedger visits the settler's website and accesses the event and the specifications of 0xSET. In the OTC Contract user interface, the hedger leases a Contract. The Contract has the address 0xTRADE. The hedger feels that there is substantially less than a 50 percent chance that ETH closes above 300 on July 31, 2017 at 12:00 GMT. As the Contract leaser, the hedger defines the SC address 0xSET, unit value of 10 Ether and offers 10 Ether as

the amount of the contingent payment moving the Contract from Leased state to Offered state. The hedger is now the seller in the CPC with address 0xTRADE. The contract value is set to be 20 Ether; the trader offers 10 Ether if the event is true and requires 10 Ether if the event is false.

A bullish investor believes that there is a substantially greater than 50 percent chance that ETH closes above 300 on July 31, 2017 at 12:00 GMT. The investor accesses the list of contracts trading on the settlement address 0xSET using the OTC Contracts user interface and selects the 0xTRADE contract. The investor inputs his own address and the required amount of 10 Ether and submits to the Ethereum network. The contract is matched when the submission is confirmed by the network. The contract value is 20 Ether, the sum of the offer and the confirmation amounts.

On July 31, 2017 at 12:00 GMT the settler records the last traded price of ETH at 402 as of 12:00 GMT from the exchange. The settler submits a TRUE value to the settlement contract 0xSET. The 0xSET contract now has the result posted.

On August 1, 2017, the investor wants the contract settled. The investor submits a request for settlement using the 0xTRADE screen on the user interface along with the fee of 0.01 Ether. The settlement contract 0xSET receives the request and responds with a TRUE result forwarded to 0xTRADE. The response triggers the payment of the entire contract value to the investor. That is, 10 Ether that was offered by the hedger and the 10 Ether that the investor sent upon confirmation.

The settler can withdraw all funds from the contract 0xSET after the results are posted, in this case 0.01 Ether. Similarly, the owner of 0xTRADE can withdraw the rent from the contingent payment contract.

9.2 Betting

The following is a technical example of a betting contract. It assumes an understanding of betting terminology used in UK bet exchange markets. Currently, high speed trading and market making is limited by the performance of the EVM.

Suppose the event is Wimbledon and the outcome is Roger Federer winning the singles title. Suppose you are making a market on a traditional bet exchange and you have calculated that Roger Federer has a 23 percent chance of winning. As a market maker, you want to take a spread of 2 percent so you offer Roger Federer at 25 percent, which is equivalent to laying 4.00 in dividend odds. Dividend odds reflect the amount paid to a backer if they pay the layer for the market. If the backer stakes 1 Ether then the backer would win 3 Ether if Federer wins and lose 1 Ether if he does not win. The expected return for the backer assuming a 25 percent chance of Federer winning is

$$0.25(3) - 0.75 = 0.$$

Of course, if the market maker's calculation of 23 percent is accurate, the backer really has a negative expected return, which equates to a positive return for the market maker. In general, market makers will offer odds on both sides of the market to lock in a return for the event and minimize their exposure to loss, as is described in more detail later.

In the OTC Contract framework, the SC would define that the result is TRUE if Roger Federer is the winner and all other outcomes is a FALSE. The market maker would be the seller of a CPC betting that Federer does not win Wimbledon and the buyer is betting that Federer wins the title. The market maker is offering 25 percent for Federer and accomplishes this by offering 75 percent of the contract value; 4 Ether is the contract value in the above example so the seller offers 3 Ether. The buyer will confirm with 25 percent of the contract value; paying 1 Ether in the above example. Suppose Roger Federer wins, the settler posts the result of TRUE to the SC. The buyer then pays the settlement fee to the SC and requests settlement for the CPC.

The SC responds with the TRUE result and the contract value of 4 Ether is paid to the buyer; the buyer is refunded the 1 Ether they paid in and wins the 3 Ether offered by the seller.

The market maker does not want to hold the exposure in the above case. In the bet exchange case, the market maker would hedge the bet by backing Federer at a lower percentage like 23 percent to be able to make the payment in case Federer wins. The spread would enable him to stake 0.92 Ether at 23 percent that locks in a positive return of 0.08 Ether regardless of the outcome. In the OTC Contracts framework, the market maker could sell his position in the CPC for 77 percent of the contract value of 4 Ether and make 2 percent of the contract value, which equals the same result of 0.08 Ether.

In a bet exchange environment, the market maker would be required to open an account and pay a 6.5 percent fee on their earnings in the market. The market maker would also be subject to paying additional amounts to the exchange if they are not paying enough fees for their profits. Suspensions and withdrawal fees are also common when dealing with bet exchanges. There are also restrictions on access and the bet exchange can expropriate the funds if any of their regulations are breached. These risks and costs are eliminated when using OTC Contracts provided the secondary market is sufficiently liquid. We would expect most market makers to own contracts to save on the contract renting charges.

9.3 CPCs on Margin

A CPC on margin has the additional value of Margin Percent and Breakeven Percent. The settlement contract for a margin contract has the margin call function in addition to settle. The CPC will have the seller paid and buyer paid amounts stored as well.

$$SellerPaid/ContractValue > MarginPercent + (CurrentPercent - BreakevenPercent) \quad (1)$$

$$BuyerPaid/ContractValue > MarginPercent - (CurrentPercent - BreakevenPercent) \quad (2)$$

The above conditions must hold or the CPC can be settled early by either counterparty by requesting a margin call from the settlement contract. Margin CPCs are more complex than standard CPCs and require a separate generator contract.

9.4 Futures and Forward Contracts

Futures and forward contracts serve the similar functions. They are contractual agreements to exchange an underlying asset for a specified price and at a specified time in the future. Most contracts are settled on a cash basis for the value of the difference between the market price and the contract price. Futures contracts are exchange products that are marked-to-market through the use of margin calls. Forward contracts are customized over-the-counter versions of futures contracts. Forwards settle upon the settlement date with no margin calls.

A forward contracts can be mirrored in the OTC Contract framework. Suppose the underlying asset is the price of Gold in Ether on July 31, 2017 at 12:00 GMT. The settler defines the value of Gold in Ether as the last trade price of the COMEX Gold August 2017 contract in USD divided by the value of the last trade of Ether on Kraken in USD. The contract will settle the equivalence of one ounce of Gold at 4.6 Ether. The settlement contract defines the contract range as the value of Gold between 2.6 and 6.6 Ether. The seller defines the contract value as 4 Ether and offers 2 Ether. The buyer pays 2 Ether to the contract. In the afternoon of July 31, the settler will submit the percent that the value of Gold is from 2.6 Ether to 6.6 Ether. For example, if the price of Gold is 5.6 Ether, the result would be

$$0.75 = (5.6 - 2.6)/(6.6 - 2.6).$$

Upon receiving the result from the SC, the CPC would pay 75 percent of the contract value (3 Ether) to the buyer and the remaining 25 percent (1 Ether) would go to the seller. The buyer

holds the long position in the contract and makes 1 Ether profit due to the appreciation of the price of Gold in Ether.

In general, forward markets are large in scale. Corporations use forward contracts to hedge exposure to price fluctuations. Counterparty risk is higher due to the lack of a central clearing house and the use of investment banks in creating the contracts makes them costly. Counterparty risk is mitigated when using smart contracts and the SCs eliminate the need for costly investment banks.

Modeling futures contracts is complicated by marked-to-market settlement. CPCs on margin could be used to create contracts that mirror futures contracts and marked-to-market settlement. However, the difference would be that the consequence of not making a margin call would result in the early settlement of the contract. Thus would create less incentive to make margin than in the current futures contracts where assets could be liquidated if margin were not sufficient. However, if the futures contract is used for hedging the counterparty may want to make the margin payment to maintain the hedge as they would likely be gaining in area of their operations.

9.5 Options Contract

The CME Group defines an option as a contract that gives the buyer the right, but not the obligation, to buy or sell an underlying asset at a specified price within a specified time period[4]. A call option gives the buyer the right to purchase the underlying asset at the strike price; the call buyer profits if the underlying increases in value. A put option gives the buyer the right to sell the underlying at the strike price; the put buyer profits if the underlying decreases in value. As with futures, options are normally settled on a cash basis with the underlying asset not being delivered upon settlement.

Call option contracts can be modeled in the OTC Contract framework. Suppose the underlying asset is the price of Gold in Ether on July 31, 2017 at 12:00 GMT. The settler defines the value of Gold in Ether as the last trade price of the COMEX Gold August 2017 contract in USD divided by the value of the last trade of Ether on Kraken in USD. The contract will settle the equivalence of one ounce of Gold at strike price of 4.6 Ether. The settlement contract defines the contract range as the value of Gold between 4.6 and 6.6 Ether. The seller defines the contract value as 2 Ether and offers 1.9 Ether. The buyer pays 0.1 Ether to the contract. In the afternoon of July 31, the settler will submit the percent that the value of Gold is from 4.6 Ether to 6.6 Ether. For example, if the price of Gold is 5.6 Ether, the result would be

$$0.50 = (5.6 - 4.6)/(6.6 - 4.6).$$

Upon receiving the result from the SC, the CPC would pay 50 percent of the contract value (1 Ether) to the buyer and the remaining 50 percent (1 Ether) would go to the seller. The buyer holds the long position in the contract and makes the net profit of 1 Ether payout and 0.1 Ether cost equal to 0.90 Ether due to the appreciation of the price of Gold in Ether.

A put option is same sort of arrangement except in the opposite direction. It can easily be modeled in the OTC Contracts framework with a different contract range and settlement result.

9.6 Letters of Credit

A letter of credit (LOC) is a document from a bank that guarantees payment. There are various forms of LOCs. They can offer security to a buyer or a seller in a transaction.

A LOC from the buyer's bank can offer security to the seller by guaranteeing to make the payment in the case that the order is adequately filled and the buyer fails to pay. The buyer can also be guaranteed by a "standby" LOC if they prepay the seller and the LOC guarantees to

repay the prepaid amount to the buyer in the case that their order is not filled adequately by the seller.

Banks provide a LOC when a business makes an application and has the adequate credit or assets to get approved. LOCs can vary greatly and are often used in overseas transactions making them difficult to understand in many cases.

Consider the case of a manufacturer receiving an order from a new customer overseas. The manufacturer needs assurance that the customer will pay for the goods after they are shipped. The purchase and sales agreement states that the manufacturer will get paid using a LOC as soon as shipment is made. The buyer applies for a LOC at a local bank puts up collateral for the LOC. The seller will only receive funds from the bank once a proof of shipment in provided to the bank. The proof may require a quality inspection in addition to documentation of delivery.

The above transaction can be mirrored with OTC Contracts. The SC can be defined by the by a fulfillment provider settler. The specifications are provided to the settler. The buyer offers the CPC at the purchase price and the seller is the manufacturer who only pays a small amount to the contract as a fee. Once the manufactured goods are received by the settler and match the specification a TRUE result is sent to the settlement contract. The seller then can request settlement of the CPC and get their payment. If the goods are not received in adequate time the settler will post a FALSE result. The buyer can request settlement of the CPC and receive their money back.

Using OTC Contracts, the buyer does not have to risk prepayment or apply for a LOC and pay the associated fees. The seller does not need to trust the foreign bank, but still will have to trust the fulfillment provider. If quality is an issue, the fulfillment company can provide a settlement result that triggers payment of a portion of the contract value from the CPC instead of a simple binary outcome.

Using OTC Contracts removes the bank and the related complications and fees. The fulfillment company will need to be trusted in all cases. The overseas company will not be required to receive payment from a foreign bank and incur many of the complications of overseas transactions.

9.7 Collateralization: Dual Settlement Contracts

Counterparties have the option to specify two SCs to settle a CPC. Each SC settles the payment of one of the counterparty's contributions to the contract value. This feature enables collateralized agreements through the use of Ether to secure off chain transactions that do not involve the exchange of Ether. This is desirable for business transactions in which costs are not incurred in Ether so payment in a fiat currency is preferred. The transaction is described with a Collateralization example.

Investopedia describes collateralization as the act where a borrower pledges an asset as recourse to the lender in the event that the borrower defaults on the initial loan. Collateralization of assets gives lenders a sufficient level of reassurance against default risk, which allows loans to be issued to individuals/companies with less than optimal credit history/debt rating.

When counterparties engage in an agreement, it can interpreted as each counterparty lending to the other. In this context, the loans are repaid through the fulfillment of the contractual obligation. Suppose a clothing manufacturer in the USA is selling 100 shirts for 5,000 dollars to a retailer. They want the transaction completed within a month. We can consider the manufacturer lending 5,000 dollars to the retailer and the retailer lending 100 shirts to the manufacturer once the agreement is established. In this context, we can use a dual settlement contract to collarteralize the agreement. The manufacturer's bank or similar institution will post the result to a SC when the payment of 5,000 dollars is made in USD. The retailer uses a fulfillment company that will post the result to a SC when the 100 shirts are delivered. The retailer and the manufacturer enter into a CPC by paying 20 Ether each into the contract with two SCs. The

20 Ether exceeds the 5,000 dollars in value for the transaction. The first SC is reported by the manufacturer's bank that will post true to the SC when the 5,000 is received within a month and false after a month if the funds are not received. Similarly, the second SC is reported by the fulfillment company that will report true when the 100 shirts are received within a month and false if they are not. After a month, settlement is requested by the manufacturer or the retailer. If the bank has received the 5,000 dollar payment, they will have reported it as true to the SC and the retailer's 20 Ether will be returned. If the bank did not receive the payment, the bank will have reported it as false to the SC and the 20 Ether is transfered to the manufacturer. Likewise, if fulfillment company receives the shirts and reports it as true to the SC, the 20 Ether will be returned to the manufacturer. If the fulfillment company does not receive the shirts within a month, they report it as false to the SC and the 20 Ether is transfered from the CPC to the retailer. In this way, we can see how the counterparties can use Ether to secure a business transaction without actually having to spend any Ether. The collateralized agreement uses Ether as the collateral in securing the fulfillment of the contract obligations. This arrangement is advantageous because it allows businesses to gain the security of using CPCs without having to purchase Ether for every transaction. The Ether a counterparty has in their account would not be spent as long as they meet the terms of the contract.

10 Conclusion

Contingent payments are ubiquitous in today's economy. The increase in demand for cost effective secure contingent payments is exacerbated by the growth in peer-to-peer transactions that are global in scope. The burgeoning technology of blockchains promises to make transactions more secure and cost effective while disrupting the financial landscape. The OTC Contracts project responds to this demand and disruption by serving as a conduit, joining the real economy and the digital blockchain space. The project brings real users and events into the blockchain with settlement and contingent payment contracts offered in an intuitive user experience, while bringing the utility of blockchain based smart contracts into real business models. OTC Contracts functions with the philosophy of keeping it simple by design, offering the maximum utility with the minimum complexity to optimize security and accessibility. Contracts are versatile and can be applied extensively across the economy to meet a variety of demands. OTC Contracts is more than a token, it is a project with a future. OTC Contract is designed with the capacity to upgrade and scale through building onto existing Contracts. OTC will make blockchain real and keep there with its focus and philosophy.

References

[1] V. Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2014.

[2] V. Buterin. CRITICAL UPDATE re: DAO vulnerability. https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/, June 2016.

[3] US Commodity Futures Trading Commission. http://www.cftc.gov/.

[4] CME Group. http://www.cftc.gov/.

[5] S. Palladino. The parity wallet hack explained. https://blog.zeppelin.solutions/on-the-parity-wallet-multisig-hack-405a8c12e8f7, July 2017.

[6] P. Sztorc. Truthcoin: Peer-to-peer oracle system and prediction marketplace. https://github.com/psztorc/Truthcoin, 2015.