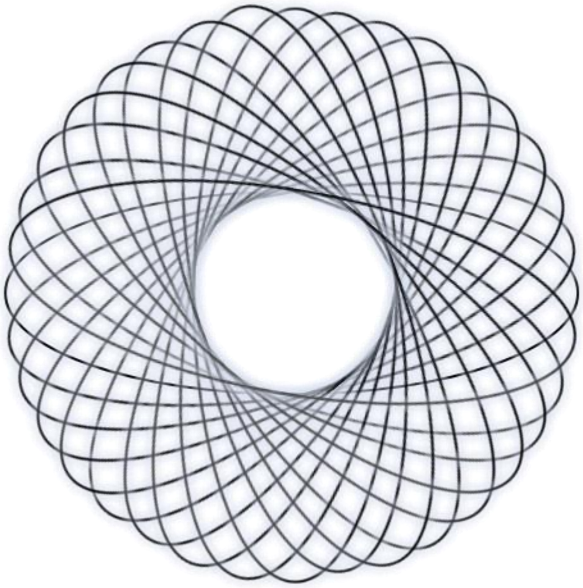
## The Decentralized Derivatives Association

*Custom Financial Products on Ethereum*



The Decentralized Derivatives Association provides custom financial products on public decentralized computing networks and a legally compliant framework for which to execute them.

Many cryptocurrencies and smart contracts are beginning to take the form of financial derivatives. Although the technologies behind cryptocurrencies and distributed virtual machines are state-of-the-art, the underlying financial transactions fall under the category of traditional financial products. Despite being an initial ambition of many blockchain platforms, there are currently no options for decentralized financial contracts. In addition, US customers have very limited options for any leveraged or bidirectional exposure to cryptocurrencies. The solution is in decentralized smart contract derivatives taking the form of fully collateralized, uncleared, capped swaps executed in a peer-to-peer manner through the Ethereum infrastructure. By leveraging decentralized exchange technology and the ability to tokenize the payouts of the swaps, a robust and liquid market can exist on Ethereum in a way it could not through a centralized exchange. Growing volumes and efficiency on decentralized networks have created the appropriate environment to introduce standard contract formats and peer-peer execution of customized derivative contracts.

***Table of Contents***

## Introduction

Decentralized computing and blockchain technology has commenced the age of the digital asset, and with it new methods of creating traditional financial assets. The ability to transfer, store and trade computationally validated contracts anonymously and over completely distributed systems will fundamentally transform the way market participants manage risk. Similar to how the internet enabled businesses to sell to anyone in the world, distributed virtual machines such as the Ethereum Virtual Machine (EVM) allow anyone to create and trade cryptocurrencies and derivative contracts without a central clearinghouse or exchange. This solution will refer specifically to executing smart contracts on the EVM; however the concept can be applied to any decentralized computing application (e.g. Rootstock, Eris, Tezos, etc.). Despite the seemingly complex nature of the underlying technology, most smart contracts and/or financial derivatives created on the EVM can be reduced to their basic nature of a financial swap. Unlike traditional swaps however, a decentralized contract has no central counterparty and can be purposefully structured to eliminate counterparty risk.

### *Current Model for Derivatives*

The current model for derivatives is one where participants go to an Introducing Broker who will set them up with a Futures Commission Merchant (FCM) that is a clearing member. The FCM will then find a counterparty either by phone, with another intermediary acting as a dealer, or in other cases on an exchange (SEF/ DCM). After execution, the position will be sent to a clearinghouse. The counterparty the participant traded with will have also done the same thing. Every step of the way you have intermediaries taking their cut, introducing risk, and getting in the way of two parties simply wanting to transfer risk or take a position. Enter blockchains, decentralized networks and Ethereum and now we can get rid of all of this.

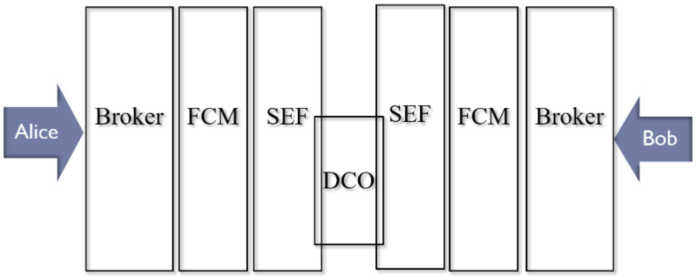


***Figure 1: Old Model***

### *New Model for Derivatives*

This is the new model. Alice can go directly to Bob. The matching of parties can be done in a peer-to-peer manner, with the functionality of the broker, dealer, clearinghouse, exchange and custodian all being performed by the smart contract on the Ethereum network. This model is revolutionary.

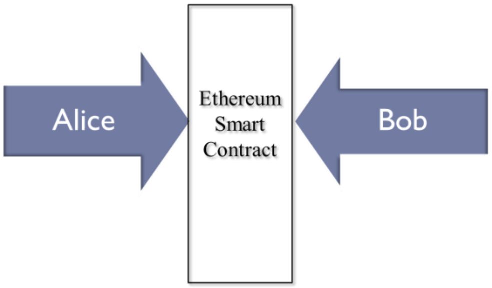


***Figure 2: New Model***

*An Introduction to derivatives*

A derivative is any instrument with a price derived from an underlying asset. The most common forms of derivatives include forwards, futures, options and swaps. A forward is a customized contract between two parties to buy or sell an asset at a specified price on a future date ('I agree to sell you 10 widgets in 6 months") A future is a standardized and centrally cleared product to be delivered on certain date ("This contract is good for ten widgets on December 1st 2018"). An option is the right to buy or sell something ("If you want, you can sell me 10 widgets at 100 dollars apiece for the next 6 months"). And a swap is an exchange of cash flows based on the price of something ("I'll pay you 100 dollars in 6 months if you pay me the price of a widget").

The model for contracts on Ethereum will use Ether as collateral, and currently plans to have any asset or rate as the underlying. Since there is no physical delivery (or cash settled version), the contract created by the DDA is a financial swap.

*Ethereum*

Cryptocurrencies and blockchains originated from a paper in 2008 titled *Bitcoin: A Peer-to-Peer Electronic Cash System*.[1] This paper outlined the usage of a peer-to-peer network for generating the trust necessary for anonymous electronic transactions. In January 2009, the bitcoin network came into existence. Ethereum[2] began as an idea in 2013 by Vitalik Buterin. The decentralized platform was specifically built to run smart contracts; applications that run as programmed on a blockchain based infrastructure. If a traditional blockchain can be thought of as a shared Excel document, Ethereum can be thought of as a shared computer, with users running the same validated programs.

To drastically simplify, imagine Alice agrees to pay Bob the price of a widget on Sunday. They both write code to calculate the price, however when Sunday rolls around they come up with slightly different prices. The problem is that they ran slightly different code. Decentralized computing networks now allows Bob to upload a smart contract, Alice to verify it and the network to run this one piece of code that determines the value. This process creates a homogenous computing environment with all of the details laid out in the smart contract code.

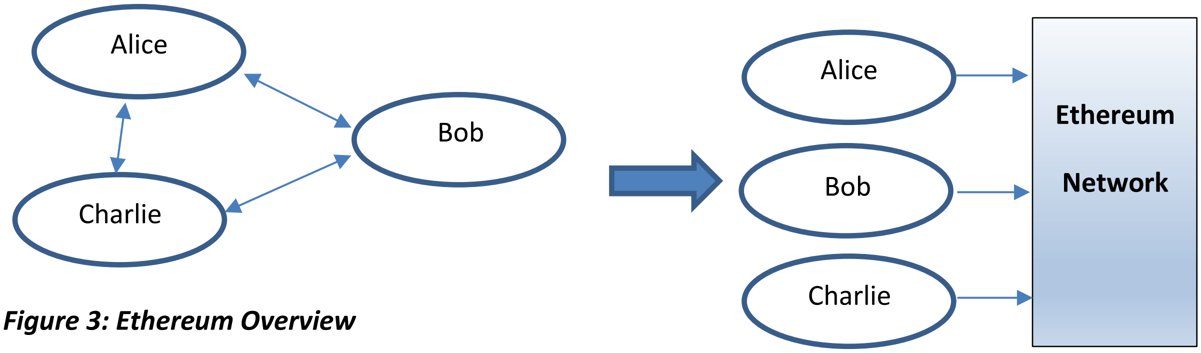


***Figure 3: Ethereum Overview***

[1] http://bitcoin.org/bitcoin.pdf
[2] https://ethereum.org/

**The Product**

Below is an example of an over-the-counter (OTC) contract on the Ethereum network. The base financial derivative described is a fully collateralized, uncleared, capped swap.

For the swap, two parties would state a notional amount in Ether (e.g. 1,000 ETH), an end date for the swap (e.g. 7 days) and a cap limit in Ether (e.g. 100 Ether) that would be deposited into the contract. A reference instrument and methodology would also be associated with the swap (e.g. BTC/USD). In this contract, the two parties have an instrument that tracks the value of the Bitcoin/USD. Note that neither party needs to own the underlying products to enter into this swap but may own them and be entering into this swap for a hedge.

At the end of the 7 days, the contract would pay the parties the value of the change of the notional multiplied by the reference rate, and the contract would be closed. Figure 4 shows this contract.

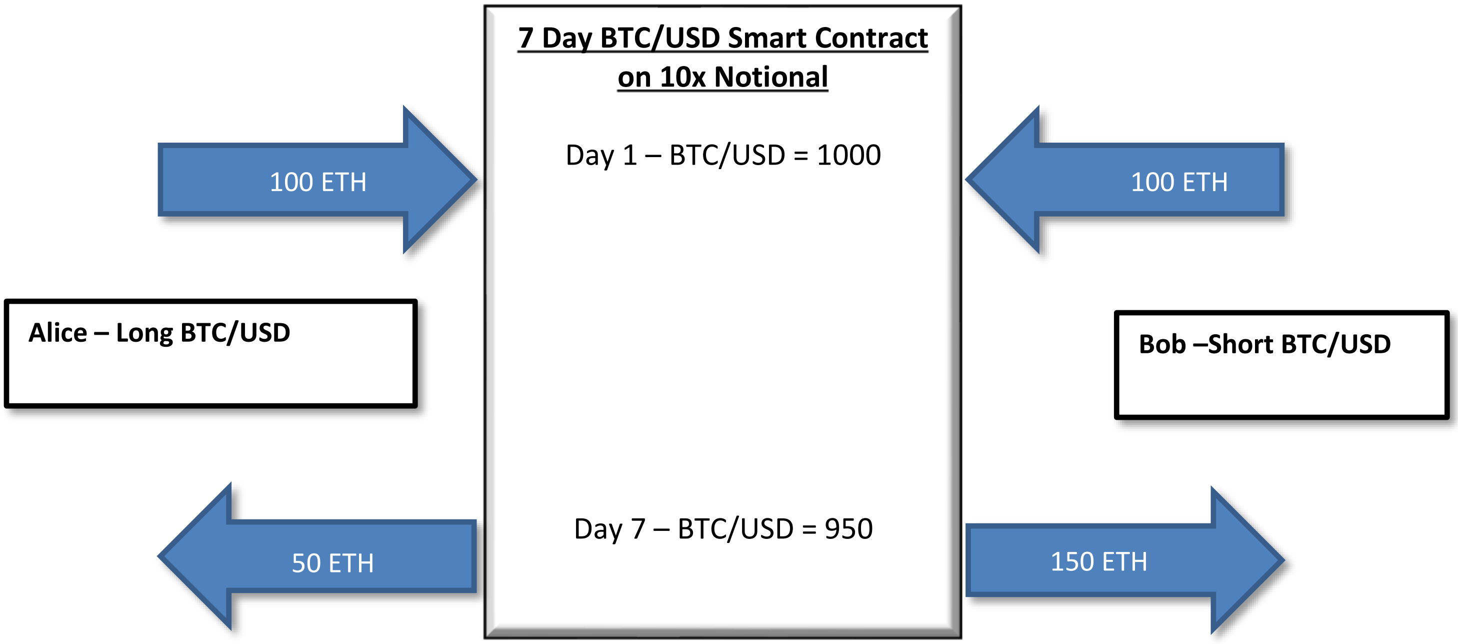


*Figure 4: Sample 7 Day BTC/USD 10x Notional Smart*

Although the contract in Figure 4 in many ways looks like a traditional rate swap, the difference lies in the creation of a swap that requires zero trust on behalf of your counterparty, a clearing party or any intermediary relaying and/or processing information. When entered, the cap limit (100 Ether in the Figure) acts as margin and is locked on the EVM in the contract. The reference rate (BTC/USD in this case) is provided via an oracle (another contract or outside source) and the counterparty (Bob) is anonymous. Since Bob is anonymous, this means that the idea of margin collection is a non-starter. All losses and gains are capped at that of the initial deposit placed in the contract. In this sense, the financial contract is a capped swap[3] that is fully collateralized.

Where Party A is long, the return is specified by the formula:

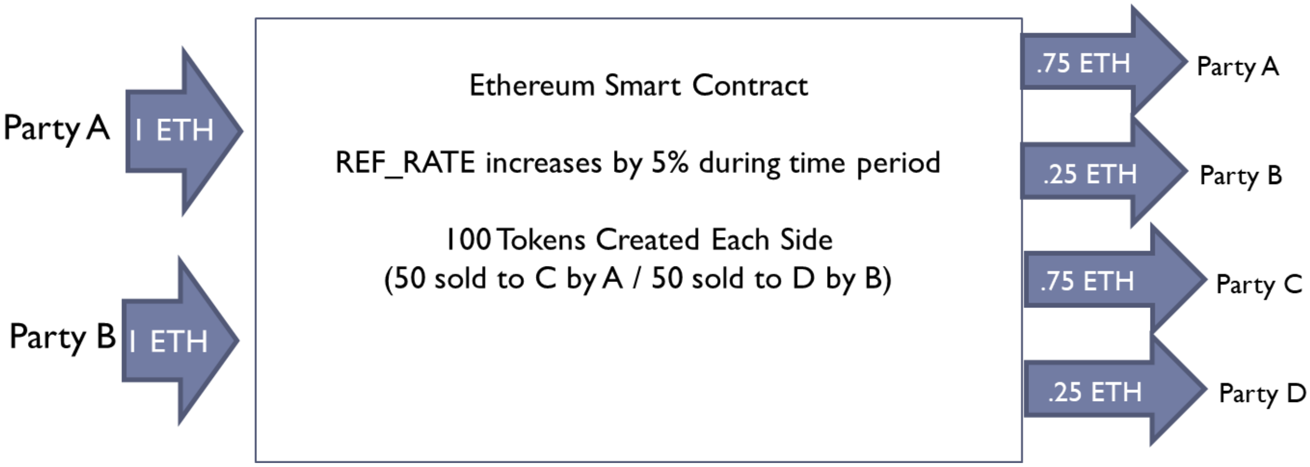
$$aM = Party\ A\ Cap\ Limit$$
$$bM = Party\ B\ Cap\ Limit$$
$$t = start\ date$$
$$t + 1 = end\ date$$
$$\Delta Notional = \ (Notional_{t+1} - Notional_t)/Notional_t$$

$$if\ \Delta Notional > 0 :\ \ Party\ A\ return = \min(\mathrm{bM}, (\mathrm{aM} + \mathrm{bM})/2 * \Delta Notional)$$
$$\text{else: } Party\ A\ return = \max(-\mathrm{aM}, (\mathrm{aM} + \mathrm{bM})/2 * \Delta Notional)$$

Note that the sample contract in Figure 4 uses a cryptocurrency as the reference rate however any product or rate can be used.

*Tokenized Swaps*

In addition to simply creating the swap, the Ethereum network also allows for the creation of 'tokens'. These tradeable assets can be structured to represent the payout of our swap. So as our Figure 5 shows, the payout of the swap no longer goes to the parties that entered into the swap initially, but rather to the owner of a token that represents a leveraged directional asset of the underlying reference rate. Through these tokens, it becomes possible to exit and/or increase swap positions in a manner that is not possible through traditional OTC swap contracts.



Party A
1 ETH
Party B
1 ETH
Ethereum Smart Contract
REF_RATE increases by 5% during time period
100 Tokens Created Each Side
(50 sold to C by A / 50 sold to D by B)
.75 ETH
Party A
.25 ETH
Party B
.75 ETH
Party C
.25 ETH
Party D

***Figure 5: Sample Tokenized Contract***

[3] A capped swap is a derivative product where the payments between counterparties are limited to a predetermined amount.

Unlike most ERC20 tokens, these tokens have an expiration date and are actually collateralized by the swap payout.  DDA has created several structures for delivery of payouts, accepting tokens rather than Ether into the Swap and the ability to eliminate currency risk from the swap.

### *Blockchain enabled OTC transparency*

In the current OTC framework for most uncleared swaps, parties are matched by dealers who either take one side of the trade themselves or solicit other dealers / swap participants through a request-for-quote (RFQ) in which they shop around for the best price for their client.  This current black box of a model leaves customers reliant upon the tenacity and goodwill of their dealer to provide a desirable price.  This new model removes this reliance and places the responsibility of finding a counterparty on the participants themselves.

The blockchain of the Ethereum network allows for any transaction (or in this case open contract) to be broadcast to all other nodes.  This RFQ-to-all model allows customers to set the price and details of the swap, broadcast the available transaction to the network and allow dealers or other customers to decide if they accept.  Many projects are taking advantage of this visible message data and creating entire decentralized exchange protocols.  These protocols allow for any tokenized product (for instance one side of a DDA swap) to be traded on their platform in a trustless manner.  Whether parties will choose to use a decentralized exchange, a dealer based model or find counterparties in a different manner has yet to be seen, but by standardizing contract formats and creating best practices for customers, a robust and truly transparent OTC market can be created on the Ethereum network.

### *Details*

Parties may create swaps by calling a Creator contract, which writes a swap contract for the party using a secure and standardized contract format.  Once the swap is written, ownership and execution of the swap are the responsibility of the party calling the Creator contract.  Regulators and counterparties, anonymous or otherwise, will know that any swap written by the Creator contract is secure and the details transparent.  Figure 6 displays a sample Creator contract.

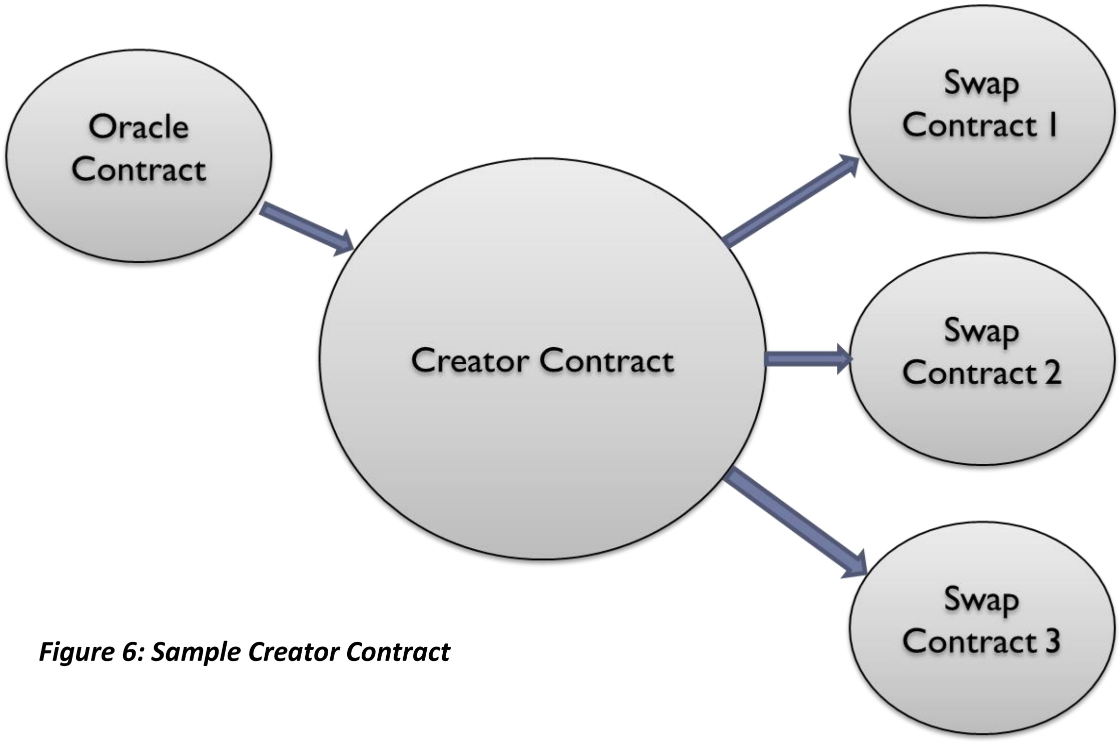


***Figure 6: Sample Creator Contract***

In order to create a swap contract, the parties will interact with the creator contract at the address based on which oracle it will reference (given by the Decentralized Derivatives Association). Then parties will pay the fee to the creator contract to create a swap contract. The address of the newly created swap contract will be returned.

The creating party can now call into the swap to enter the details. The difference between Alice's margin (the capped amount Alice would be able to lose/ Bob would be able to gain) and Bob's margin (the capped amount Alice would be able to gain/ Bob would be able to lose) is how a spread is accounted for. If Alice desires more immediacy for her swap or does not have a counterparty lined up, she can entice other parties by reducing Bob's margin relative to Alice's. This would make the swap more one sided in its risk profile with a tighter cap on the side with the smaller margin. Note also that the difference between the margin and the notional is the "leverage" of the contract. All differences in the contract are calculated based on the notional and the margins simply cap the amount gained or lost.

Once started, it is the responsibility of the first party to find a counterparty for the swap. There is no implicit matching engine or centralized orderbook for the swaps. The Ethereum blockchain holds records of all transactions however and can be used to see open swaps. The other party (regardless of how they are found) can enter into the other side by calling the contract, verifying that they are an eligible counterparty based on their jurisdiction.

Once the end date of the contract has arrived, each party can then withdraw their share of the contract balance based on the movement of the underlying reference rate. After the swap is completed, all reporting requirements are the responsibility of the counterparty based upon the jurisdiction they reside.

## Security and Legal Concerns

One of the greatest struggles faced by companies interacting with or utilizing cryptocurrencies and decentralized technology is regulatory uncertainty. The following section attempts to layout the U.S. regulatory framework for cryptocurrency derivatives and should give regulators ease to know that the existing law is being heeded and these products require no regulatory sandbox or relief.

### *The Clearing Mechanism*

Although financial swaps proposed on the Ethereum network are uncleared, the full collateralization renders the distinction moot. Regulations on derivatives focus on three areas: who is holding customer funds, with whom does the ultimate risk lie in the case of a default, and who is matching counterparties. The product proposed does not have an intermediary that holds customer funds, have any risk in the case of a counterparty default, and does not match counterparties. All three aspects of the derivative are handled by the EVM and/or the participant(s). Although the decentralized network (e.g. the EVM) as a whole could be considered and required to register as a DCM or DCO, forcing the Ethereum foundation to register would be an exercise in futility. Any regulatory effort requiring a technology to register as a financial firm would be a detrimental grandstand in a thinly veiled effort to protect incumbents. Reporting requirements and customer safety can be enforced, however traditional classifications of registrants may not apply directly to decentralized networks. There is no counterparty risk in a decentralized exchange as the entire system was built around not trusting one's counterparty. Contracts are built around the idea of unenforceability beyond the contract and incentives created by the contract. Any clearing or registration mandate for certain products will only convolute the transaction, increase costs and force innovation underground. Excepting the risk inherent in specific programs or applications, the only risk for the aforementioned swaps is that which resides in the system itself (hacking and network issues). Central clearing parties (CCP's) are not immune from this risk and although the potential dangers of Ethereum are unfamiliar, the value and security of the Ethereum network towers over that of any DCO applicant[4].

### *The current regulatory landscape*

There are high registration and regulatory compliance costs for traditional derivatives exchanges, intermediaries and participants, which point to the need for a decentralized, peer-to-peer framework for derivatives execution.

Current restrictions for OTC derivatives on Ethereum are numerous in the U.S. To start, many swaps will be off limits for participants on Ethereum. If the swap is Made-Available-to-Trade (MAT), there are Swap-Execution-Facility (SEF) and clearing requirements. Any swap referring to equity performance will

[4] https://coinmarketcap.com/currencies/ethereum/

be regulated by the SEC and additional registration and regulatory requirements will apply. Parties will also be required to report to Swap Data Repositories (SDRs). Should no SDR accept these transactions, the reports can be filed manually to the CFTC.[5] Parties must also obtain a valid Legal Entity Identifier (LEI) for reporting purposes.[6] In addition to these requirements, currently only eligible contract participants (ECP's) are able to enter into swaps on their own behalf. These requirements include high net worth values and/or third parties with a registered status[7]. Other additional requirements and restrictions may also apply and parties should seek counsel for complete guidelines. For the decentralized swaps proposed herein, all reporting and eligibility requirements are the responsibilities of the individual parties involved in the swap.

As the space develops and more traditional players enter the market, swaps with more recognizable formats will begin to appear. Swaps on cryptocurrencies and other digital assets are a natural starting point for financial derivatives on Ethereum; however the standard format and conventional terms of the contract could turn decentralized networks into automated clearinghouses, reducing costs for already familiar companies and products.

Currently the CFTC and SEC have not exerted jurisdiction over the use of decentralized derivatives with any actions. The nascent technology and lack of large players have made Ethereum more of an enigma than an outright violator of policy. Promising speeches have been made by the current CFTC commissioner and by the Trump administration promoting innovation. Although the rejection of several Bitcoin ETF's indicate that the space is still seen as too obscure for main street investors, the rise of digital assets and the decentralization of costly intermediaries will continue.[8] No action relief or a formal rule could exempt U.S. retail participants from the ECP[9] requirement or the CFTC could decide to pass on jurisdiction, deeming any fully collateralized technology neither a commodity nor financial derivative within their purview.

## The Future

*API Oracle Swap* – Recognizing that complete decentralization requires full independence from DDA and all intermediaries, a currently developed version of our swap will have underlying reference rate as a data field in the creation of the swap. Based upon a decentralized API oracle service (such as Oraclize), the swap will be completely free of all intermediaries. [10] DDA can also provide custom oracles for non-API available references (e.g. future tokens, multiple levels of computation performed on various API's,

[5] https://www.law.cornell.edu/uscode/text/7/6r

[6] https://www.gleif.org/en/about-lei/how-to-get-an-lei-find-lei-issuing-organizations

[7] https://www.law.cornell.edu/uscode/text/7/1a

[8] https://www.sec.gov/rules/sro/batsbzx/2017/34-80206.pdf

[9] CEA Section 1a(18) defines an ECP as being, among other persons and when acting for its own account, a financial institution, a State-regulated insurance company, an investment company regulated as such under th

[10] http://www.oraclize.it/

additional third party validation on top of API). The decentralization of oracles is important, however there are currently no legal restrictions or registration requirements on running oracle services.

*Netting-* Full collateralization of offsetting positions results in a party locking up twice the collateral for zero risk. In order to incentivize market makers, DDA will soon release a netting swap contract creation factory. These swaps will allow parties to fully collateralize their swaps by having one contract control the inflow and outflow of each payout, not allowing the max loss of the portfolio to exceed the collateral. To give an example, if Dave collateralizes a 7-day long BTC/USD swap on 1000 Ether with 100 Ether, he will be able to also enter a 7-day short BTC/USD swap on 2000 Ether. The position will require no extra collateral since the two swaps offset themselves and his max loss is still his 100 Ether.

*Decentralized Interface* – A full decentralized swap would benefit from a decentralized swap exchange. Any centralized swap exchange would need to register as a SEF at the CFTC and be subject to very large capital requirements, registration fees and other regulatory burdens. Luckily for DDA (and its users), the Ethereum blockchain stores message data from all swaps created and/or entered into. Client side software can then scrape the blockchain for swap message data (i.e. open swaps, details of swaps, terminations, etc.) and then each individual can create an orderbook for themselves. This GUI will create a better decentralized user experience than the command prompt or Mist wallet and be tailored for DDA swaps specifically.

## Conclusion

A decentralized framework for OTC peer-to-peer swaps will allow participants to engage in financial derivatives without the need for a centralized website, exchange, middleman or clearing house. Smart contracts structured as capped, uncleared, fully collateralized swaps provide significant cost benefit and risk mitigation abilities to participants. It is likely that these products will be under the regulation of the CFTC and in the U.S. are currently legal only with proper reporting and for eligible contract participants. The decentralization of derivatives in a trustless and central counterparty-less format has arrived. As volumes on the Ethereum network and in cryptocurrencies grow, these contracts will provide a significant pool of capital to access for new and existing swap participants in cryptocurrency-based, custom and illiquid contracts.

The Decentralized Derivatives Association has created customizable swaps for execution on the Ethereum blockchain. For those seeking to hold customer funds or enter into/ execute swaps on behalf of U.S. customers, full registration requirements can be found via the CFTC's website and the National Futures Association's website.[11] [12]

[11] http://www.cftc.gov/IndustryOversight/Intermediaries/FCMs/fcmib

[12] https://www.nfa.futures.org/NFA-registration/fcm/index.HTML

*Disclaimer: This paper in no way intends to give legal advice or imply the thoughts or future actions of any regulatory agency. For the decentralized swaps proposed in this paper, all reporting and eligibility requirements are the responsibilities of the individual parties involved in the swap.*

*The Decentralized Derivatives Association (DDA) has open contract factories ready to create your next financial swap. DDA has also created full demos and sample code for creating decentralized swaps, scanning the blockchain for open swaps, viewing details and entering into these contracts. We also provide many oracles for public use with methodology and detailed user guides. Please visit our Github page for more information at: www.github.com/DecentralizedDerivatives*

*For those interested in updates, customized oracles, need assistance in executing swaps contracts, or have questions about our methodology and/or services, please visit our website at www.decentralizedderivatives.org*

## Notes and Further Reading

Bitcoin Whitepaper- https://bitcoin.org/bitcoin.pdf
Ethereum Whitepaper- https://github.com/ethereum/wiki/wiki/White-Paper
Capped Swap Readings:
https://en.wikipedia.org/wiki/Interest_rate_cap_and_floor
http://www.investopedia.com/terms/c/capped-rate.asp