

The Decentralized Derivatives Association

Customized Swaps on Ethereum

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 derivatives. 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. 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

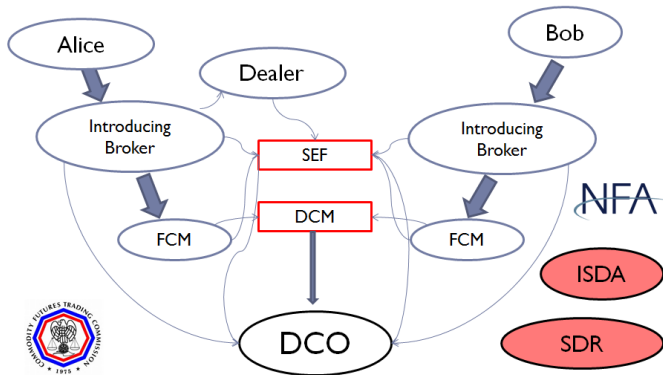
- [Introduction to Blockchains, Decentralized Application Platforms and Existing Concepts](#)
- [The Product](#)
- [Security and Legal Concerns](#)
- [The Future](#)
- [Conclusion](#)
- [Notes and Further Reading](#)

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

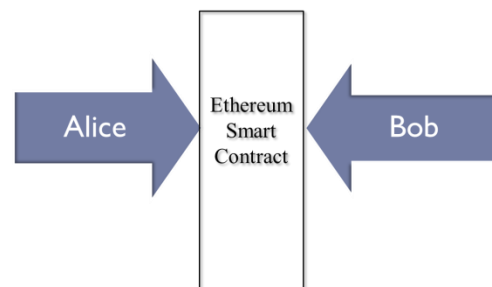
The current model for derivatives is one where participants often need to go to an Introducing Broker who will set them up with a clearing member who will find a swap either by phone with a dealer or in



the case of a future/ option or certain cleared swap they go onto an exchange and then once executed, at the end of day the position will be sent to a clearinghouse and the opposite party will have done roughly 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.

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 clearinghouse, exchange, and custodian all being performed by the smart contract on the Ethereum network. This model is revolutionary.



An Introduction to derivatives

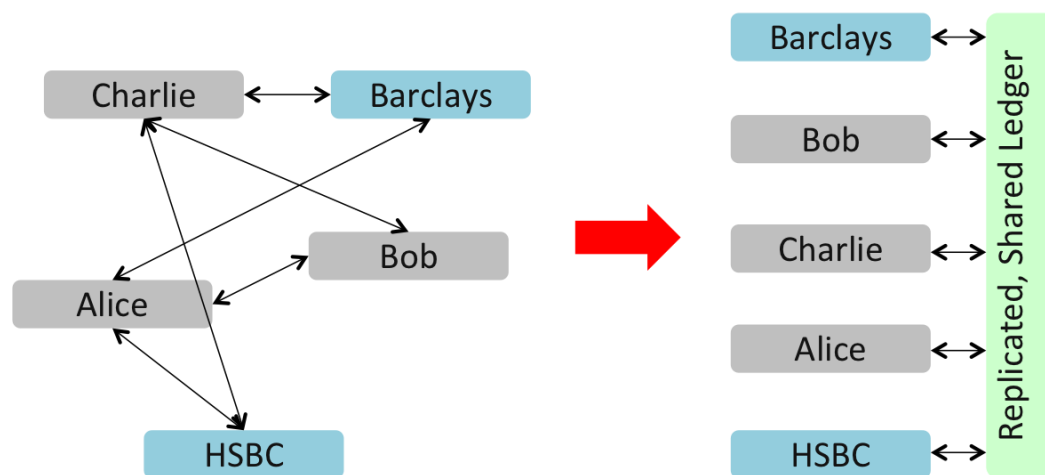
A derivative is any instrument with a price derived from an underlying asset. The most common forms of derivatives include futures, options and swaps. A future is a product to be delivered on certain date ("This contract is good for ten widgets on December 1st 2018"). An option is the right to buy or sell something (i.e. "If you want, you can sell me 10 widgets at 100 dollars a piece for the next 6 month"). 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 technically 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. Ethereum² 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 allow Bob to upload a smart contract onto the network, Alice can verify it and then one piece of code is run by the network and determines the value. This process creates a homogenous computing environment with all of the details laid out in code.



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

¹ <http://bitcoin.org/bitcoin.pdf>

² <https://ethereum.org/>

contract, the two parties have an instrument that tracks the value of the Bitcoin/USD but neither party owns either underlying product.

At the end of the 7 days, the contract would pay the parties the value of the change of the notional * the reference rate and the contract would be closed. Figure 1 shows this contract.

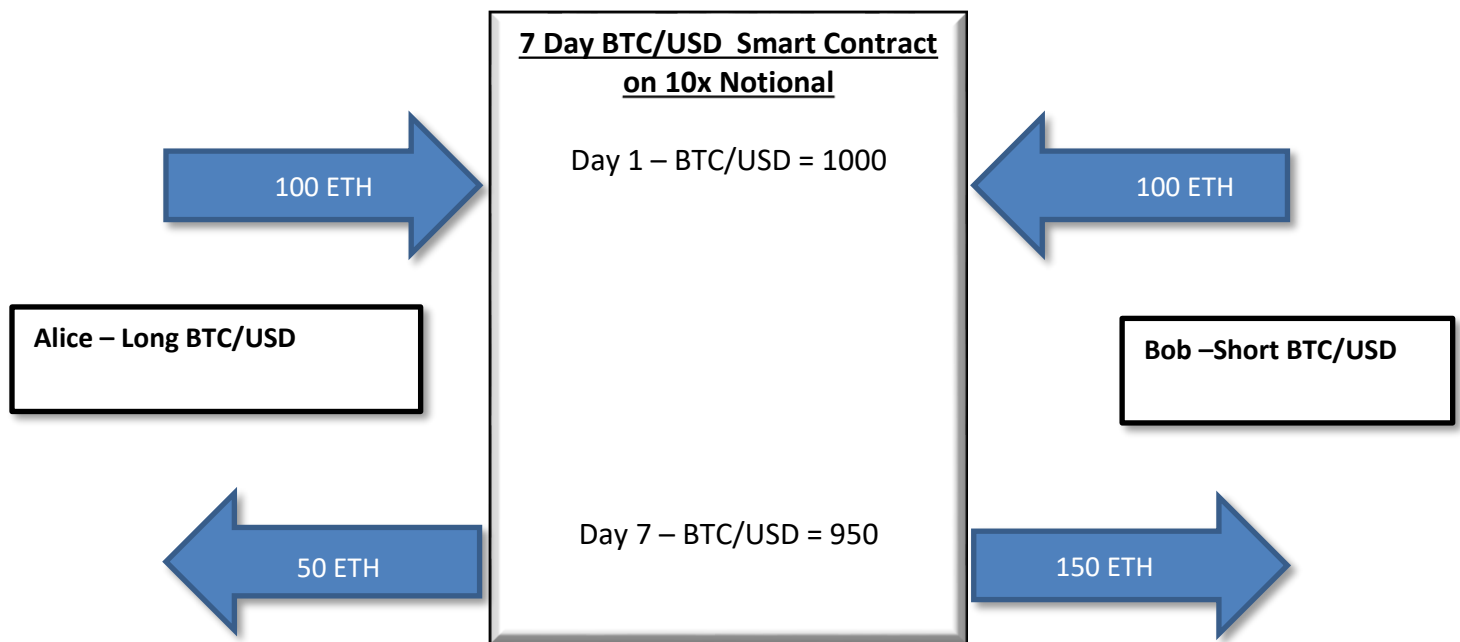


Figure 1: Sample 7 Day BTC/USD 10x Notional Smart

Although the contract in Figure 1 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 or a clearing party. When entered, the cap limit 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) 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 swap³ that is fully collateralized.

³ Capped swap definition

The return is specified by the formula:

$$\begin{aligned} aM &= \text{Party A Cap Limit} \\ bM &= \text{Party B Cap Limit} \\ t &= \text{start date} \\ t + 1 &= \text{end date} \\ \Delta \text{Notional} &= (\text{Notional}_{t+1} - \text{Notional}_t) / \text{Notional}_t \\ \text{if } \Delta \text{Notional} > 0 : \text{ Party A return} &= \min(bM, aM * \Delta \text{Notional}) \\ \text{else: Party A return} &= \min(-aM, aM * \Delta \text{Notional}) \end{aligned}$$

Note that the sample contract in Figure 1 uses a cryptocurrency as the reference rate however any product or rate can be used.

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. 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 2 displays a sample Creator contract.

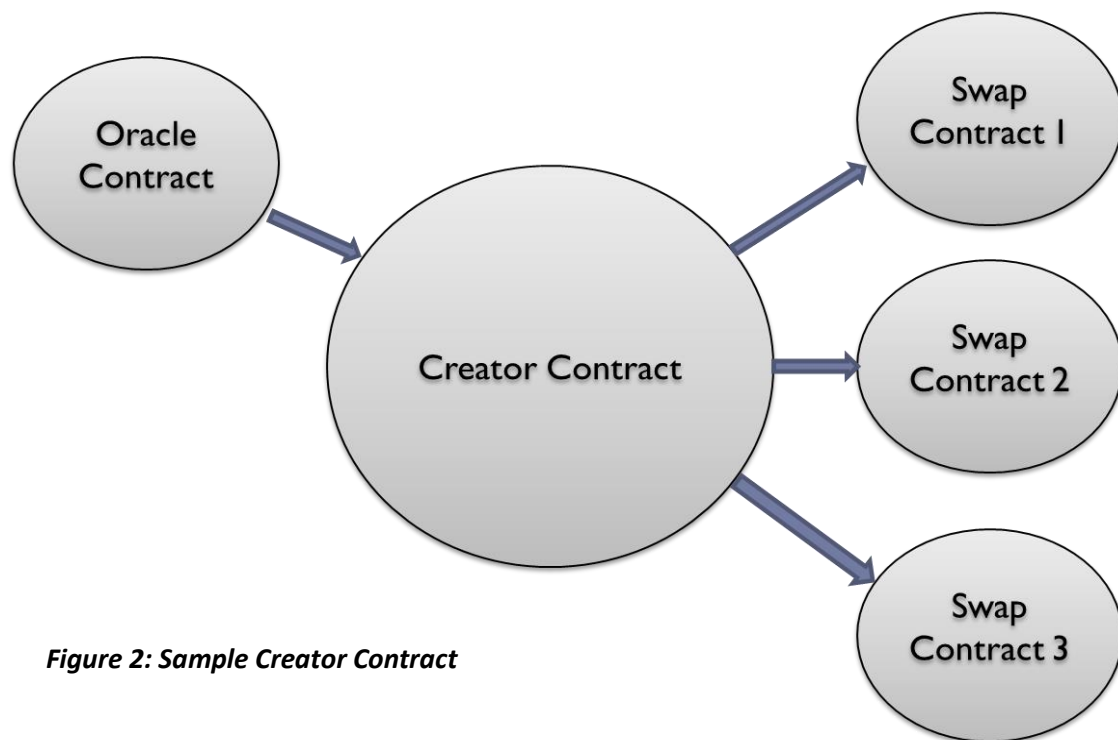


Figure 2: Sample Creator Contract

In order to create a swap contract, the parties will interact with the factory 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 factory 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, parties can then tell the smart contract to calculate their final payouts and 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 applicant⁴.

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 be regulated by the SEC and additional registration and regulatory requirements will apply. Parties will

⁴ <https://coinmarketcap.com/currencies/ethereum/>

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 status⁷. 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 ECP⁹ requirement or the CFTC could decide to pass on jurisdiction, deeming any fully collateralized technology neither a commodity nor financial derivative within their purview. As more liquidity moves to public blockchains, regulators should take the opportunity to monitor systematic risk, promote safe investor behavior and provide the foresight to not limit new technologies and opportunities.

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 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

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

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.^{10 11}

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>

¹⁰ <http://www.cftc.gov/IndustryOversight/Intermediaries/FCMs/fcmib>

¹¹ <https://www.nfa.futures.org/NFA-registration/fcm/index.HTML>