The Rainbow Network: An Off-Chain Decentralized Synthetics Exchange

Dan Robinson[†]

dan@paradigm.xyz

March 2019
WORKING DRAFT, rev. 1

Abstract

This paper presents the Rainbow Network, a design for an off-chain non-custodial exchange and payment network supporting any liquid asset. The Rainbow Network allows a user to trade, lend, borrow, send, and receive any liquid asset, entirely off-chain, while having only one on-chain payment channel collateralized by a single asset. The network is composed of Rainbow channels, a variant of payment channels where settlement balances are computed based on the current prices of other assets. This paper presents three constructions of Rainbow channels, one of which can be implemented on top of any bidirectional payment channel, such as the Bitcoin payment channels used in the Lightning Network.

1 Introduction

This paper introduces a design for a non-custodial off-chain exchange, built on top of a new primitive called **Rainbow channels**. Rainbow channels are an extension of payment channels in which the participants can hold synthetic balances in *any asset*, rather than just the asset that is used as the collateral for the channel. When the channel is closed, the amount sent to each participant is based on the current prices of the synthetic assets in the channel.

A Rainbow channel can support long and short positions in any asset for which the participants can agree on a price oracle, with as much leverage as the participants are willing to accept, entirely collateralized by a single asset on the parent chain. As in any payment channels, payments and trades in Rainbow channels can happen nearly instantaneously and at essentially zero cost.

Users can execute all of their trades in a single bilateral Rainbow channel with one market maker. In order to hedge that trade, that market maker can

[†] The author is a Research Partner at Paradigm.

enter into a offsetting trade in some other Rainbow channel, forming a scalable network of fully-hedged market makers: the **Rainbow Network**.

This paper presents three constructions of Rainbow channels. In the first, the escrow contract uses a mutually-agreed-upon price oracle to compute the settlement prices. In the second, the contract enforces "physical settlement," where the underlying crypto asset needs to be provably delivered as part of channel settlement. In the third, the parties continuously cash-settle their balances to the payment channel. The latter two constructions do not require a trusted price oracle, and the third can be implemented on any bidirectional payment channels, such as the Bitcoin payment channels used in the Lightning Network.

1.1 Prior work

In most decentralized cryptocurrency exchanges, such as Uniswap [1] and 0x [2], trades are executed on a blockchain. This increases latency and requires users to pay transaction fees on every trade. Similarly, most solutions for leverage (such as dYdX [3], Dharma [4], and Compound [5]) and/or synthetics (such as UMA [6] and MakerDAO [7]) require on-chain transactions for every state update.

Arwen [8] is a protocol for non-custodial off-chain atomic exchange. In Arwen, a user can only sell assets that they hold in an on-chain escrow, and can only buy assets that an exchange has put into an on-chain escrow reserved for that user. Similarly, payment channel networks such as Lightning [9] and Interledger [10] can support multi-asset trades, but only if users already have channels with sufficient sending capacity in the asset they want to sell, and sufficient receiving capacity in the asset they want to buy. Plasma Cash [11] and related plasma constructions can help mitigate the difficulties of finding receiving capacity, but still require that senders have sufficient balances in the assets that they wish to send or sell. Additionally, all of these constructions only support assets that are already held on a blockchain, and none of them natively support leveraged trading or short-selling.

Abra [12] is a platform that offers off-chain synthetic positions in various currencies and cryptocurrencies, backed by collateral held in a single cryptocurrency. This is similar to the kinds of synthetic positions used in Rainbow channels. However, in the system described by Abra, this collateral is held in a 2-of-2 multisignature address between the platform and the user [13]. This means that each party is subject to counterparty risk with respect to their entire balance—either the user or the platform can prevent the other from withdrawing any collateral. This would make it difficult to use this model in a decentralized network, where participants would prefer to minimize the credit risk that they take on.

Amoveo [14] is a blockchain that only supports a single token on-chain, but supports payment channels in which parties can enter into synthetic positions that are settled with reference to on-chain prediction markets, as well as multi-hop trades across those channels. This is very similar to the price-oracle-based construction of Rainbow channels described below.

2 Background

2.1 State channels

A state channel is a construction in which two (or more) parties lock up some state and/or assets in an escrow contract on some parent blockchain. The participants can make off-chain updates to the channel by signing messages committing to new states. Parties can cooperatively exit from a particular state instantly; otherwise, a party can unilaterally initiate an exit, which completes after a delay. If a party attempts to exit an outdated state, their counterparty can challenge by showing a more recent state.[1]

2.2 Simple payment channels

A payment channel is a state channel where the state being managed is a ledger representing the participants' ownership in some collateral that is locked up on the parent chain.

Let's suppose Alice and Bob have a payment channel with each other. This payment channel is secured by a pot of 20 ETH on the parent chain, which means that the total value that can be safely allocated between the parties is 20 ETH.

Suppose Alice currently has a balance of 5 ETH and Bob has a balance of 15 ETH. This means that Alice and Bob each have a signature from the other on a message that represents the following state:

Example A, State 1	
Recipient	**Balance**
Alice	5 ETH
Bob	15 ETH

The signed state includes the current balances of the parties, along with a nonce (which is 1 in the above example) representing the recency of the state.

If Alice wants to pay Bob 1 ETH, she and Bob can sign a state that includes updated balances, along with a higher nonce:

Example A, State 2	
Recipient	**Balance**
Alice	4 ETH
Bob	16 ETH

[1] This paper mostly abstracts away the details of the underlying state channels. For a more detailed explanation of how state channels work, see the Counterfactual paper [15].

While Alice can use this channel to make payments to Bob in ETH, in traditional payment channel constructions, she would not be able to purchase ETH using other assets, such as USDC (a dollar-backed stablecoin [16]).

On Ethereum and other sufficiently programmable blockchains, it is possible to have payment channels that are collateralized by multiple assets. Suppose Alice had a payment channel that was collateralized by 300 USDC and 20 ETH. In this channel, as long as her current USDC balance was higher than 150 and Bob's ETH balance was higher than 1, she would be able to purchase 1 ETH for 150 USDC from Bob by updating their channel balances like so:

Example B, State 1	
Recipient	**Balance**
Alice	5 ETH 200 USDC
Bob	15 ETH 100 USDC

Example B, State 2	
Recipient	**Balance**
Alice	6 ETH 50 USDC
Bob	14 ETH 250 USDC

2.3 Payment channel networks

Payment channel networks like Lightning [9] and Interledger [10] loosen these requirements a little, by allowing the assets to be held in different payment channels, and even in channels with different counterparties.

But for Alice to purchase ETH for USDC through one of these payment channel networks, she would need to have a channel in which she has sending capacity in ETH, and one in which she has receiving capacity in USDC. Additionally, her counterparties in those channels would need to be connected by some route. And, of course, she would only be able to trade assets that were already issued on a blockchain.

3 Rainbow channels

What if Alice could temporarily "transmute" some of the ETH in her payment channel with Bob into USD, and use that to purchase ETH from Bob?

Rainbow channels are an extension of payment channels that allow parties to enter into *synthetic positions*.

Rainbow channels can be implemented on any blockchain with Turing-equivalent smart contracts. It is even possible to implement a limited version of Rainbow channels on Bitcoin, as described below in section 3.5.3.

3.1 Turning gold into lead

Suppose Alice has an ETH payment channel with Bob, in which she has a balance of 5 ETH and Bob has a balance of 15 ETH.

Example C, State 1	
Recipient	**Balance**
Alice	5 ETH
Bob	15 ETH

Alice wants to buy 5 ETH from Bob for 750 USD (with an implied price of 150 USD/ETH). They can update the balances of their channel as follows.

Example C, State 2	
Recipient	**Balance**
Alice	10 ETH -750 USD
Bob	10 ETH 750 USD

This update happens entirely off-chain, between the parties. The underlying collateral on the parent chain is still 20 ETH. So how can this channel be settled? The key is that the escrow contract computes how much ETH each participant should get *based on the price of the assets at the time the exit is completed.*

If the channel is exited while the price is still 150 USD/ETH, then Alice will receive 5 ETH and Bob will receive 15 ETH:

Example C, State 2, Settling at 150 USD/ETH			
Recipient	**Balance**	**Value**	**Exit**
Alice	10 ETH -750 USD	10 ETH -5 ETH	5 ETH
Bob	10 ETH 750 USD	10 ETH 5 ETH	15 ETH

Alternatively, if the channel is exited when the price is 300 USD/ETH, Alice will receive 7.5 ETH and Bob will receive 12.5 ETH:

Example C, State 2, Settling at 300 USD/ETH			
Recipient	**Balance**	**Value**	**Exit**
Alice	10 ETH -750 USD	10 ETH -2.5 ETH	7.5 ETH
Bob	10 ETH 750 USD	10 ETH 2.5 ETH	12.5 ETH

Finally, if the channel is exited when the price is only 75 USD/ETH, Alice will receive 0 ETH and Bob will receive 20 ETH:

Example C, State 2, Settling at 75 USD/ETH			
Recipient	**Balance**	**Value**	**Exit**
Alice	10 ETH -750 USD	10 ETH -10 ETH	0 ETH
Bob	10 ETH 750 USD	10 ETH 10 ETH	20 ETH

3.2 Theory

In typical payment channel designs, a particular channel state represents a ledger—a mapping of owners to balances. Computing how this state will settle on-chain is trivial—each user receives the exact amount of ETH specified in the channel's state.

In Rainbow channels, each state represents a *contract for difference* that can be settled at any time. Settling one of these states involves computing the total current ETH value of each of the positions (positive and negative) that each party is entitled to under the swap, which involves looking up the current price. A purchase or sale inside of a channel effectively involves cancelling that contract and replacing it with another one that with the same current economic value.

In Example C, the swap entered into between Alice and Bob is similar to a contract for difference, with USD as the underlying reference asset and ETH as the settlement currency.[2]

3.3 Other assets

Example C involves a trade between USD—a synthetic asset, in this context—and ETH. However, there is no reason that Alice and Bob would be limited to trades that involve ETH. For example, if Alice wanted to buy 1 Bitcoin (BTC) for 4000 USD, she and Bob could execute the following trade:

[2] This resembles an off-chain bilateral version of the total return swap used as part of UMA's protocol for on-chain synthetic assets [6].

Example D, State 1	
Recipient	**Balance**
Alice	10 ETH
Bob	10 ETH

Example D, State 2	
Recipient	**Balance**
Alice	10 ETH -4000 USD 1 BTC
Bob	10 ETH 4000 USD -1 BTC

Note that at prices of 150 USD/ETH and 4000 USD/BTC, 4000 USD and 1 BTC are each more valuable than the total amount of ETH locked up as collateral! Despite this, the channel is still safely overcollateralized for both parties, because at current prices, Alice's balance of 1 BTC is exactly nullified by her balance of -4000 USD, and vice versa for Bob. This is an example of how Rainbow channels can enable leverage, as explored further below in section 3.6.

If the price of BTC falls below $2500, however, Alice's portfolio will become undercollateralized (assuming that the price of ETH has not changed). The risk of undercollateralization is discussed in greater detail in section 3.7.

The assets simulated in a Rainbow channel could include other cryptocurrencies (such as BTC), fiat currencies (such as USD, EUR), commodities (such as gold or oil), or even more exotic assets, such as prediction market shares.[3] As described below in section 3.5, the assets that can be simulated depend on which construction is used.

3.4 Other collateral

The above examples use ETH as the entire collateral for the channel, but any token on the parent chain could potentially be held as part of the collateral for the channel. Parties might sometimes find it convenient to use a stablecoin as collateral.

3.5 Constructions of Rainbow channels

The above description of Rainbow channels glosses over how, exactly, a channel is able to settle based on the prices of the underlying assets.

This paper presents three ways to construct Rainbow channels, each of which make different tradeoffs. In the first, the positions are *cash-settled* upon close,

[3] Prediction market shares are particularly well-suited for Rainbow channels, because their prices have a fixed upper bound, which means it is possible to fully collateralize positions in those shares. In fact, trading prediction market shares in Rainbow channels only requires the same amount of collateralization as is required to trade those shares on-chain.

with the settlement prices dynamically computed by the escrow contract using some mutually-agreed-upon price oracle. In the second, the positions are *physically-settled* upon close: the contract requires that a party with a short position deliver the underlying assets to the escrow contract (or prove that they delivered them to their counterparty). In the third, the positions are *continuously cash-settled* by updating the balance of the payment channel.

3.5.1 Rainbow channels with price oracles

In perhaps the most straightforward construction of Rainbow channels, the parties mutually agree on some price oracle. At the time the channel is closed, the escrow contract consults that price oracle and computes the balance to which each party is entitled. Critically, there is no need for a universally agreed-upon price feed—the parties in each channel can agree upon the price oracle to be used to settle that channel.

The design of difficult-to-manipulate price oracles is an area of ongoing research, which is far too deep to explore in this paper. For ERC20 tokens, a price feed based on a decentralized exchange like Uniswap may be sufficient, if it is sufficiently hardened to prevent manipulation. For assets like USD, the parties could rely on price feeds from exchanges, or piggyback on other USD-pegged assets on the parent chain.

3.5.2 Rainbow channels with physical settlement

There is an alternative construction that does not depend on the existence of a price oracle, although it is not as flexible—it only supports crypto assets (and only a specific subset of those assets).

Suppose the asset being traded was not USD—which is not represented natively on the Ethereum blockchain—but USDC.

Example E, State 1	
Recipient	**Balance**
Alice	5 ETH
Bob	15 ETH

Example E, State 2	
Recipient	**Balance**
Alice	10 ETH -750 USDC
Bob	10 ETH 750 USDC

As in Example C, this channel is collateralized by a deposit of 20 ETH on the parent chain, and the parties enter into this position off-chain.

If the channel was closed now, Alice's USDC balance would be -750. If this were a cash-settled channel, the contract would use a price oracle to convert that value to ETH. However, since USDC is a crypto asset, there is an alternative—the contract can require *physical delivery.* During the delay period for the channel close, while waiting for either party to challenge the recency of the state, the contract also waits for Alice to deliver 750 USDC. If she does not, all of the collateral in the contract goes to Bob. If she does, then when the channel close completes, the 750 USDC, along with 10 ETH, is delivered to Bob, and the remaining 10 ETH is delivered to Alice.

Remarkably, physical settlement is not limited to assets that are on the same parent chain as the channel. There is also a way the contract can enforce physical settlement of *BTC* positions. If Alice has a -1 BTC balance, the contract can require that she send 1 BTC to Bob's address. Alice can prove this to the escrow contract by providing a Simplified Payment Verification ("SPV") proof, showing an inclusion proof of the transaction in a block, covered by at least 6 blocks of proof-of-work.[4] As an optimization, the contract could skip the SPV proof unless Bob challenges Alice to provide it. This would reduce the gas cost in the normal case, but increase the time to exit.

Whether this construction is possible for a given asset depends on the capabilities of the channel's parent chain and the consensus mechanism of the crypto asset's host chain. For example, on the Ethereum chain, it is easiest to evaluate SPV proofs from proof-of-work chains that use supported hash functions (such as Bitcoin and Bitcoin Cash), while it may be more difficult to evaluate such proofs from blockchains that use other proof-of-work algorithms, or proof-of-stake blockchains.[5]

Note, however that this construction only requires *one-way* SPV proofs, from the host chain of the crypto asset to the parent chain of the Rainbow channel; it does not require a two-way peg. This enables something new: trading of synthetic BTC on an Ethereum payment channel, without a price oracle or trusted custodian.

3.5.3 Rainbow channels with continuous cash settlement

Both of the above approaches require some custom computation on the base layer that may not be possible on a more constrained platform like Bitcoin.[6]

However, it is possible for parties to implement some of the functionality of Rainbow channels on top of any bidirectional payment channel, including the Bitcoin-based payment channels that are used in the Lightning Network. The approach has somewhat more off-chain computational and communication overhead, and likely imposes even higher capital requirements, but eliminates the need for sophisticated smart contracting capabilities. Like physical settlement, this solution also does not depend on a trusted price oracle.

Suppose Alice and Bob have a simple Lightning payment channel, and want to enter into a position like the one in Example C. Entering into this contract

[4] These kinds of proofs are used by Summa [17] to verify Bitcoin payments on Ethereum, as part of a Dutch auction protocol.

[5] Various technologies for proof-of-stake SPV messages, such as Cosmos's Inter-Blockchain Communication Protocol [18], could make this easier.

[6] It might be possible to construct oracle-dependent payment channels on Bitcoin using Discreet Log Contracts [19], but any such solution would likely have astronomically high computational and communication overhead.

does not involve updating the state of the channel. Instead, during the pendency of the contract, the parties continually recompute the current channel balance based on the new price, and update the channel state to reflect that new balance.[7] Note that Alice and Bob are not executing new *trades*—they are *settling* their existing contract to the channel.

If Bob stops participating in these updates, Alice should immediately initiate a close of the channel. When Bob does this attack, he can only steal a negligible amount of *value* from Alice, since he can only take advantage of the price movement since their latest update.[8] However, Alice does immediately lose her *exposure* to the position that she entered into in that contract, instead gaining exposure to Bitcoin. This is different from fully-featured Rainbow channels, where, unless the channel becomes undercollateralized, this shift in exposure only happens at the time Alice's channel close completes (which is also the time she regains access to the collateral and can put it into another channel or trade it on-chain).

Assuming Alice wants to maintain her exposure to those assets, she can immediately "novate" that position by entering into the same position in another one of her channels. If she is able to do so efficiently, then Bob's betrayal only costs her some limited amount, based on the price movements during the short period of exposure, as well as the costs of novating the position. However, this solution does require Alice to maintain some Bitcoin in another Rainbow channel, in case she ever needs to novate a position from another channel.

3.6 Leverage, interest, and flows

Note that in Example C, Alice is effectively *levered long* ETH. She only put down 5 ETH in capital, which was worth $750 at the time. When the price of ETH doubled to $300, her position tripled in value, to $2250 (7.5 ETH at $300 each). This is a 1.5x levered long position. In effect, Alice has borrowed $750 from Bob and used it to purchase 5 ETH from him.

These kinds of channels are similar to the collateralized debt positions ("CDPs") used in the Maker system [7]. Alice plays the role of the CDP creator who "borrows" DAI (the USD-pegged stablecoin) and trades it for more ETH. Bob plays the role of the mechanism that lent the DAI to Alice, as well as the party that sold ETH to Alice in exchange for the DAI.

In addition to a fee or spread on the initial trade, Bob might reasonably want to charge Alice interest on the borrowed USD. To support this, we can add an

[7] While this does require Alice and Bob to remain online and to constantly sign new updates to their payment channel, those are similar requirements to those already imposed on routing nodes in Lightning.

[8] In other words, an attacker has the option whether to accept or reject each channel update based on the price movement since the previous update. Since updates could conceivably happen every few seconds, the value of this free option should be relatively small compared to the value of the channel. Indeed, these few seconds of optionality seem likely to be insignificant compared to the "free option" that one party gets in a multi-asset HTLC trade [20]. This does mean, though, that parties should be even more careful when entering into positions in volatile or levered assets.

additional feature to Rainbow channels. In addition to understanding formulas that compute final balances based on price oracles, the settlement logic of the payment channel could also understand *flows*, formulas where the final balance depends in part on the time of the exit.

Suppose Alice agreed to pay 4% interest annually, computed in USD, without compounding (which amounts to $30 per year).

Example F, State 1, Time T

Recipient	**Balance**
Alice	10 ETH -750 USD -30 USD/year
Bob	10 ETH 750 USD 30 USD/year

If the channel is exited six months later, Alice would have to pay $15 in interest (0.1 ETH, if the price of ETH remains at $150).

Example F, State 1, Settling at 150 USD/ETH, Time T + 6 months

Recipient	**Balance**	**Value**	**Exit**
Alice	10 ETH -750 USD -30 USD/year	10 ETH -5 ETH -0.1 ETH	4.9 ETH
Bob	10 ETH 750 USD 30 USD/year	10 ETH 5 ETH 0.1 ETH	15.1 ETH

The formula could be tweaked to allow interest to be computed in different ways, such as having it computed in ETH rather than USD, or with compounding, or even with a floating interest rate.

This feature could be used to support arbitrary flows, not just interest payments. For example, this protocol could support subscriptions, donations, or salaries that are paid continuously until cancelled.[9]

Flows are possible in all three Rainbow channel constructions. Non-cancellable flows, however, may only be possible in certain constructions, as described in section 5.2.

[9] Vitalik Buterin has suggested a similar protocol for continuous payments [21]. In his proposed protocol, however, changing the payment rate would require an on-chain transaction, rather than an off-chain state channel update.

3.7 Risk of undercollateralization

In Example C, if the price of ETH falls by 50%, Alice's balance in the channel is effectively worth nothing. If the price of ETH falls further than that, the channel would become undercollateralized—Bob would no longer be able to withdraw his USD at its current value.

Bob should therefore ensure that the value of Alice's portfolio remains high enough that volatility in her assets will not cause it to dip below $0 too quickly. Alice could increase her collateral by "topping up" the channel with additional ETH when her portfolio falls in value. If her position falls too close to $0 and she fails to top up her channel or participate in a cooperative close, Bob should initiate an exit from the channel.

In the first and second Rainbow channel constructions described above, the parties are exposed to price risk while the channel is closing.[10] Since payment channels take some time to settle (often between one hour and three days, depending on the security parameters of the parties), there is a risk that the portfolio will become undercollateralized before the exit is finalized, since it will be exposed to a long period of volatility.[11]

If Bob wants to preserve his long and short exposure to that basket of assets, then when his counterparty's portfolio goes below zero, he can try to immediately hedge his position by entering into the same positions in some other channel (or on some exchange), exiting that hedge if the position goes back above zero. Hedging is described in greater detail in section 4.1.

4 Rainbow Network

Rainbow channels provide a powerful primitive for trading, borrowing, and lending assets with a channel counterparty. But they would still be of limited use if you could only enter into a trade when you have a channel with someone who wants to make the opposite trade. By networking these channels together, we can construct a system in which market makers can give their customers execution on arbitrary trades without taking on significant additional risk themselves.

4.1 Hedging

In Example C, Alice initiated the trade because she wanted to increase her economic exposure to ETH, relative to USD. Bob essentially acted as a market maker, executing the trade in exchange for (presumably) some fee, spread, or interest rate.

[10] Recall that in the continuously-cash-settled construction described in section 3.5.3, Bob *immediately* loses exposure to the assets as soon as the channel close begins (or as soon as Alice stops cooperating), so he needs to hedge that position immediately if he wants to maintain it.

[11] In the price-oracle-based construction described in section 3.5.1, it is possible to incentivize Alice to top up the channel by imposing a liquidation penalty on her—zeroing out her balance if it is too close to zero.

What if Bob didn't want to change his market exposure? Bob can *hedge* this trade by executing the reverse trade (paying 750 USD to buy 5 ETH) somewhere else. He could do this on a centralized exchange, or on an on-chain exchange such as Uniswap, but a natural place to execute it would be *another Rainbow channel*.

Participants in Rainbow channels could therefore form a "hedging network", where market makers execute trades for users and then hedge and net those trades with each other, entirely off-chain. We can call this network the **Rainbow Network**, on the premise that rainbows are basically just multicolored lightning.

There are many possible topologies for this network. One possibility is a hub-and-spoke model, where medium-size market makers like Bob would hedge their trades with end users by entering into offsetting trades with larger market makers. After netting these trades against each other, these very large market makers could hedge their own exposure by executing trades on a centralized exchange, or on-chain.

The flexibility of Rainbow channels means that currency exchange is significantly simpler in the Rainbow Network than in other payment channel networks. In a multi-asset Lightning Network, to purchase BTC for LTC, Alice would need to find a route starting with her BTC payment channel and ending with her LTC payment channel. In the Rainbow Network, rather than finding a path to a particular *channel*, the parties only need to find a path to someone willing to take a position in a particular *asset*. Additionally, unlike in Lightning, Rainbow Network trades do not require atomic updates of multiple channels—once Bob has agreed to trade with Alice, how he hedges it is not Alice's concern.

4.2 Payments

In addition to being used to buy and sell synthetic assets, Rainbow channels can easily be used like an ordinary payment channel, for making payments in any asset. If Alice wants to make a 100 USD payment to Bob, she can do so as follows:

Example G, State 1

Recipient	**Balance**
Alice	5 ETH
Bob	15 ETH

Example G, State 2

Recipient	**Balance**
Alice	5 ETH -100 USD
Bob	15 ETH 100 USD

Rainbow channels can also support multi-hop payments, using protocols like Lightning[12] or the Interledger Protocol. Unlike with traditional payment

[12] Lightning supports multi-hop payments using a two-phase commit protocol, during which

channels, Bob would not need to have a channel open in a particular currency in order to send or receive funds in that currency.

5 Areas for further research

5.1 Protocol specification

The above discussion informally proposes abstract features that could be supported by Rainbow channels, without attempting to specify the actual protocol.

The state-channel functionality would likely be implementable within a framework for generalized state channels, such as Counterfactual [15].

A full solution would also likely need to specify a domain-specific language for the payment channel states, which need to define a mapping from recipients to balances as a function of price (and sometimes as a function of time). It may be possible to adapt an existing protocol for on-chain margin positions, such as dYdX [3].

5.2 Other derivatives

Each Rainbow channel state corresponds to a specific kind of derivative: a swap contract that is cancellable at any time by either party. While this turns out to be an extremely flexible and powerful derivative, it doesn't come close to capturing the full range of rights that Alice and Bob could define with respect to the channel.

For example, Alice and Bob could enter into an *options contract* inside their payment channel. The option could be cash-settled (based on a price oracle) upon exercise, or it could be physically-settled, with the seller sacrificing their entire collateral if they fail to deliver the underlying asset.

As another example, the rest of this paper assumes that Rainbow channels, like typical state channels, can be closed and settled at any time by either party. This would make the synthetic "loan" in Example C different from typical loans (or CDPs), which usually are not cancellable by the lender. If Bob settled the channel early, Alice would no longer have the leveraged long exposure to ETH that she thought she had signed up for. While she could enter into a new trade, it may have a less favorable interest rate.

To allow Alice and Bob to lock in the terms of a long-term position, Rainbow channel states could allow parties to set conditions on when a channel can be closed. If such a condition were added, Bob would also want to ensure that he could initiate an early settlement (or "margin call") if the value of Alice's portfolio comes too close to undercollateralization.

some of the assets in a channel are allocated to a hashed timelock contract (HTLC). This can be supported in Rainbow channels by allowing states to specify arbitrary smart contracts, rather than public keys, as the "recipients" of particular balances.

On Ethereum, it may be possible to allow parties to define some of these more advanced derivatives using an existing protocol like dYdX. Supporting more complex derivatives in *Bitcoin* payment channels (using the construction described in 3.5.3) is likely more difficult, and is left as a subject for further research.[13]

5.3 Plasma

One disadvantage of the above construction is that these synthetics are tied to the relationship between Alice and Bob. By combining this mechanism with the non-fungible off-chain transfers enabled by Plasma Cash, we could allow both the synthetics and their collateral to be transferred between parties. (This section only presents a sketch, and assumes some familiarity with Plasma Cash research.)

Suppose that rather than being an ordinary channel, this was a Plasma Debit [22] channel, with Bob serving as the operator. Plasma Debit allows users to transfer their interests in payment channels to other users. Using this construction, Alice would be able to transfer her entire portfolio (including its collateral, synthetics, and debt) to another party.

Further extensions could allow any two parties—where neither has to be the plasma chain operator—to enter into a swap position on a plasma chain. We could even allow channels to be split into ranges (as is supported in Plasma Cashflow [11]). If you split off a piece of the portfolio containing synthetic USD, as well as some of the corresponding collateral, then that piece could be transferred independently of the rest. This would allow the synthetic USD in a Rainbow channel to be transferred to other parties, mostly independently of the collateral—similar to a futures contract.

All of these ideas can likely be implemented within generalized plasma [23], a framework that supports custom plasma variants within a single plasma chain.

6 Acknowledgments

I'd like to thank Patrick McCorry, Hayden Adams, James Prestwich, Boyma Fahnbulleh, Karl Floersch, Daniel Winters, Hart Lambur, and Vitalik Buterin for their valuable feedback. I'm also particularly grateful to Paradigm for supporting this kind of research, and to my colleagues—Matt Huang, Fred Ehrsam, and Charlie Noyes—for their review and helpful comments.

References

[1] Hayden Adams. *Uniswap.* URL: `https://docs.uniswap.io/`.

[13] One possibility is that the parties could treat *the option itself* as the underlying asset, and constantly update their payment channel based on the option's current computed value.

[2] Will Warren and Amir Bandeali. *0x: An open protocol for decentralized exchange on the Ethereum blockchain.* Feb. 2017. URL: https://0x.org/pdfs/0x_white_paper.pdf.

[3] Antonio Juliano. *dYdX: A Standard for Decentralized Margin Trading and Derivatives.* URL: https://whitepaper.dydx.exchange/.

[4] Nadav Hollander. *Dharma: A Generic Protocol for Tokenized Debt Issuance.* URL: http://whitepaper.dharma.io/.

[5] Robert Leshner and Geoffrey Hayes. *Compound: The Money Market Protocol.* June 2018. URL: https://compound.finance/documents/Compound.Whitepaper.v04.pdf.

[6] Hart Lambur. *UMA – Universal Market Access.* Dec. 2018. URL: https://medium.com/uma-project/uma-enabling-universal-market-access-266eb9e5fd90.

[7] MakerDAO. *The Dai Stablecoin System.* URL: https://makerdao.com/en/whitepaper/.

[8] Ethan Heilman, Sebastien Lipmann, and Sharon Goldberg. *The Arwen Trading Protocols.* Jan. 2019. URL: https://arwen.io/whitepaper.pdf.

[9] Joseph Poon and Thaddeus Dryja. *The Bitcoin Lightning Network.* Jan. 2016. URL: https://lightning.network/lightning-network-paper.pdf.

[10] Interledger. *Interledger Architecture.* URL: https://interledger.org/rfcs/0001-interledger-architecture/.

[11] Plasma Group. *Plasma Group's Plasma Spec.* Jan. 2019. URL: https://medium.com/plasma-group/plasma-spec-9d98d0f2fccf.

[12] Daniel McGlynn. *Abra's Synthetic Currency.* Oct. 2018. URL: https://www.abra.com/blog/abras-synthetic-currency/.

[13] Daniel McGlynn. *How non-custodial wallets let you be your own bank.* July 2018. URL: https://www.abra.com/blog/noncustodialwallet/.

[14] Zack Hess. *Amoveo White Paper.* URL: https://github.com/zack-bitcoin/amoveo/blob/master/docs/white_paper.md.

[15] Jeff Coleman, Liam Horne, and Xuanji Li. *Counterfactual: Generalized State Channels.* June 2018. URL: https://l4.ventures/papers/statechannels.pdf.

[16] Coinbase. *USD Coin (USDC).* URL: https://www.coinbase.com/usdc.

[17] Summa. *Welcome to Summa Auctions.* URL: https://summa.one/auction.

[18] Cosmos. *Cosmos Inter-Blockchain Communication (IBC) Protocol.* URL: https://cosmos.network/docs/spec/ibc/.

[19] Thaddeus Dryja. *Discreet Log Contracts.* URL: https://adiabat.github.io/dlc.pdf.

[20] ZmnSCPxj. *[Lightning-dev] An Argument For Single-Asset Lightning Network*. Dec. 2018. URL: https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-December/001752.html.

[21] Vitalik Buterin. Feb. 2019. URL: https://twitter.com/vitalikbuterin/status/1093091291066294272.

[22] Dan Robinson. *Plasma Debit: Arbitrary-denomination payments in Plasma Cash*. June 2018. URL: https://ethresear.ch/t/plasma-debit-arbitrary-denomination-payments-in-plasma-cash/2198.

[23] Plasma Group. *Towards A General Purpose Plasma*. Feb. 2019. URL: https://medium.com/plasma-group/towards-a-general-purpose-plasma-f1cc4d49c1f4.

Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Paradigm or its affiliates and does not necessarily reflect the opinions of Paradigm, its affiliates or individuals associated with Paradigm. The opinions reflected herein are subject to change without being updated.