An Anonymous Trust-less Public Peer Consensus Liquidity Pool Staking for Uncollateralised Loans with Underwriting, Disbursement, Repayments and Delinquency Recovery through an ETH-based Network

15 November 2021

Abstract

UCL is a decentralized protocol that allows for uncollateralised crypto borrowing through trust-less public anonymity consensus. Key limitation of existing crypto lending protocols require excessive crypto collateralisations, preventing borrowers from participating due to risk arising from unverifiable and unvalidated credit worthiness. Through trust-less public peer consensus underscore by an automated rig-free credit risk governance mechnism, the UCL protocol allows credit ratings of borrowers to be assessed based on effective redemption of loans rather than actual crypto asset holdings. In addition, the protocol caters for NEAR-COMPLETE recovery of loans in the event of loan default; with recovered credits return to the funded liquidity pool. By removing the need for crypto collaterals and providing additional means for passive yield through extending liquidity to other networks, the protocol dramatically improves credit accessibility, limits risk while improving yields.

1. UCL Introduction

UCL protocol consists of 3 main groups of participants, namely Borrowers, Lenders and Liquidity Providers.

Borrowers are participants who seek funding/financing. Borrower Pools are a collective of borrowers where Lenders will assess their credit worthiness. In addition, Borrower Pools also contains credit information like interest rate, repayment schedules among other T&Cs.

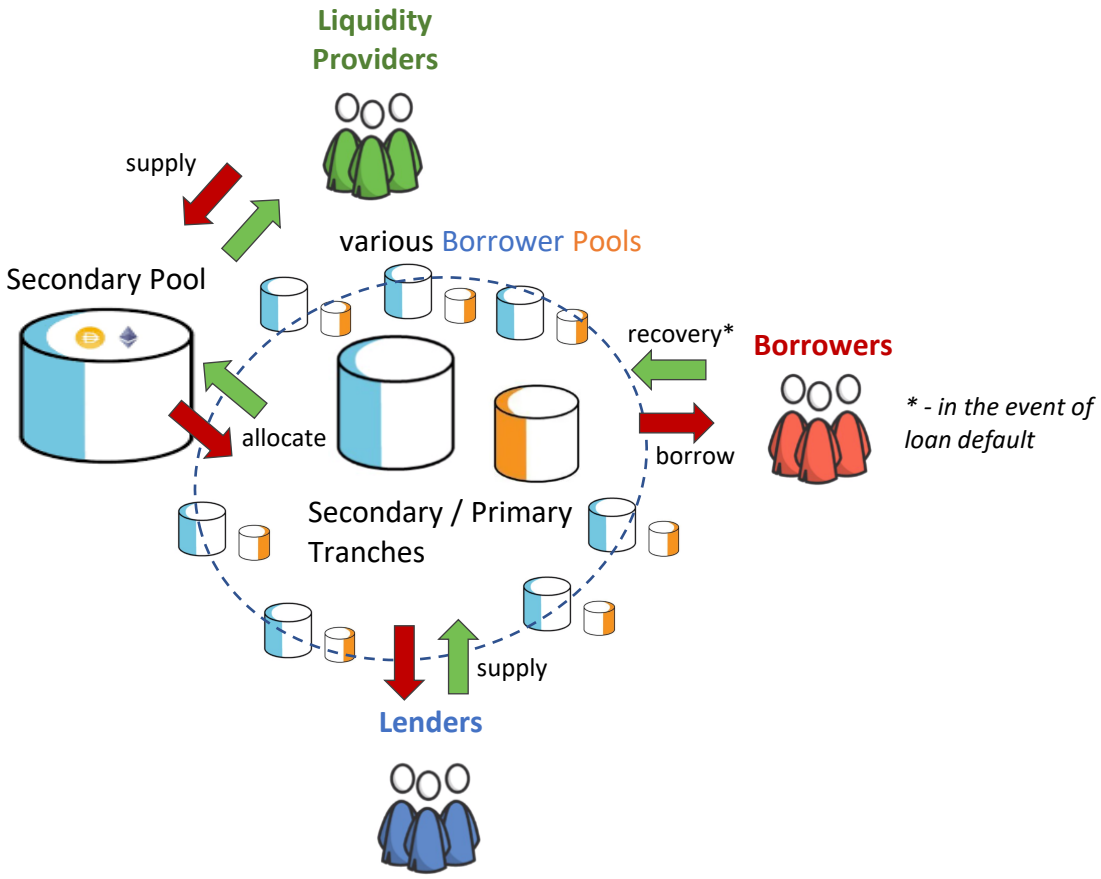
Lenders assess the Borrower Pools and decide if catalytic First Loss capital applies which includes any potential fees such as gas incurred during the *Recovery* of defaulted loans from Borrowers.

Borrowers can then borrow and repay through the Borrower's Pool.

Liquidity Providers capitalise the Secondary Pool in order for investors to profit from passive yield. Leverage Model is used to automatically allocate capital to the Borrower Pools, and calculated based on how many participating Lenders. Upon capital allocation, a portion of its interest is apportioned to the Lenders which increases the Lenders' effective yield, thereby incentivising them to continue to provide

higher-risk catalytic First Loss capital and Borrower Pools assessments.

2. UCL **Protocol**



KEY TERMINOLOGIES

- **Lenders** : Participants supplying Primary Tranche (First Loss) capital (e.g. USDT, BUSD, BNB, USDC, ETH and etc.) to each Borrower Pools.
- **Borrowers** : Participants who raised capital from the protocol via Borrower Pools.
- **Borrower Pool** : Encoded smart contract for a Borrower, including and not limited to interest rate and repayment schedule.
- **UCLtoken** : Token used for Governance votes, staking and liquidity mining, vote rewards, staking on Lenders, Seed Lender rewards and other potential rewards, for all protocol participants.
- **Governance** : Smart contract that is managed by the community DAO and has the ability to update the protocol via decentralized governance votes (to be rollout in phases, starting with off-chain).
- ***Leverage Model** : Mechanism whereby the Secondary Pool determines capital allocation to each Borrower Pool and/or external crypto loans/yield farming network like Aave, Uniswap. Curve, Compound, Pancake swap and etc.
- **Liquidity Providers** : Participants who supply capital (e.g. USDT, BUSD, BNB, USDC, ETH and etc.) to the Secondary Pool.
- **Secondary Pool** : Smart contract that accepts capital from Liquidity Providers and allocates capital to

the Secondary Tranche of Borrower Pools according as per *.

2.1. Borrowers

Borrowers are participants who's seeking for financing through the protocol. They propose financing terms to Lenders in order for them to supply capital to their Borrower Pools.

2.1.2. Borrower Pool

A Borrower Pool is the smart contract through which Borrowers borrow and repay capital with interest. Any Borrower can create a Borrower Pool with proposed terms as below:

i. *Interest Rate* : Fixed interest rate APR, e.g. 20%.
ii. *Limit* : Total capital that can be borrowed, e.g. $3M.
iii. *Payment Period* : Frequency of interest payments, e.g. every 10 days.
iv. *Term* : When the full principal is due, e.g. 90 days.
v. *Late Fee* : Additional interest owed when payments are late, e.g. 8%.
vi. *Recovery* : default in repayment schedules, e.g. late interest/ principal repayment for > 3 days

Creating a Borrower Pool can be understood as a term sheet to Lenders with all the T&Cs. As auto-recovery of loans is an in-herein part of the protocol to protect lenders' funds, Borrowers would not need to convince Lenders to supply Primary Tranche (First Loss) capital. The amount Borrowers can borrow is based on how much Lenders are willing to supply based their credit score, combined with the amount the Secondary Pool is able to allocate as per the Leverage Model.

Borrowers then need to set a limit for their Borrower Pools, an imposed ceiling on borrow quantum as per the DAO governance community collective voting outcome. While Borrowers prefers an infinite supply of credit facility limit, Lenders would want to know that they are staking First Loss capital from the risk perspective. Borrowers therefore are incentivised to set the limit only as high as they can convince Lenders to limit risk exposure. In addition, to create a Borrower Pool, the Borrower must also stake an amount of UCLtoken, which is a fixed rate set by the protocol. This helps guard against potential spam, as it *requires Borrowers to pay for the approval with UCLtoken*. The Borrower can then redeem their remaining staked UCLtoken when they have fully repaid their outstanding balance.

2.1.3. Borrowing and Repayment

Borrowers can borrow capital through the Borrower Pool at any time. The maximum quantum they can borrow is the minimum of :

i. The calculated limit based on the capital that Lenders have supplied and the additional Secondary Pool's leverage amount.
ii. The total capital combined that Lenders have supplied in any Borrower Pool plus the remaining capital in the Secondary Pool.
iii. The Borrower Pool's limit.

Borrowers are required to make repayments to the Borrower Pool according to its interest rate and payment period. In the event if they happened to pay more than the interest owed, the remainder is applied to towards the principal balance.

2.1.4. Primary and Secondary Tranches

Borrower Pools consist of a Primary and

Secondary Tranche. Lenders supply capital to the Primary Tranche, and the Secondary Pool supplies capital to the Secondary Tranche. When a borrower makes repayments, the Borrower Pool applies the amount first toward any interest and principal owed to the Secondary Tranche, before the Primary Tranche.

2.1.5. Seed (founder) Fee

Some participants who work with Borrowers to establish their terms and bring them to the protocol. To compensate them for these efforts, Borrower Pools support a Seed Fee that is paid to the pool's founder. The Seed Fee is defined as a percentage of the interest.

For example, for a $1M Borrower Pool with 15% interest paid monthly and a 10% seed fee, the Borrower would need to pay a monthly interest fee of $12.5K and the founder would then receive a monthly seed fee of $1.25K which is part of the paid interest. To further align and incentivise capital providers, the seed fee is treated as the least prioritised, so every payment goes towards what is owed to the Secondary Pool and Lenders first before paying the founder.

2.1.6. Rationale - Borrower Governance

Limiting risk – Borrowers are likely to continue borrowing from UCL given easy credit availability. To limit risk, once Borrowers defaults any scheduled repayments, the entire disbursed loan will be automatically unwind (*Recovery*) and they'll barred from the network and are unable to borrow further from any of the Borrower Pools. This is achieved through the atomicity of ETH-based network. Concurrently, Lenders would also stop supplying more capital.

Recovery – The smart contract would unwind all the transactional positions between the Borrowers and all transacted third parties less UCL network and admin fees as defined under catalytic first lost capital.

Since Borrowers are required to *publicize* their address as part of KYC and can be validated by service providers impacted by loan defaults from a Borrower (wallet address). when creating pool proposals to Lenders, their on chain history not only becomes public but also to off chain creditors during a recovery.

Loop holes? - While not explicitly supported by the protocol, Lenders may arrange for off chain legal agreements with Borrowers as potential recourse.

2.2. Lenders

Lenders supply catalytic First Loss capital on their Borrower Pools. Lenders can achieve higher returns when the Secondary Pool leverages with additional Secondary Tranche capital.

2.2.1. Supplying to Borrower Pools

Lenders look at Borrower Pools as investment opportunities. They evaluate the information Borrowers provide and decide if they want to supply capital to the Primary tranche Borrower Pool. The Secondary Pool provides additional Secondary Tranche capital to the Borrower Pool according to the Leverage Model.

To account for the lower risk of the Secondary Tranche, 20% of the Secondary Tranche nominal interest is reallocated to the Primary Tranche. In addition, the protocol retains 10% of all interest payments as reserves, which are managed by the decentralized Governance ultimately.

As a result, the Secondary Pool earns an effective interest rate equal to 70% of the

nominal interest rate. Or, in terms of the nominal interest rate, in, protocol reserve allocation, p, and Primary reallocation percent, j:

$$i_{secondary} = i_n * (1 - p - j)$$

Accordingly, based on these same inputs and the leverage ratio, r, Lenders receive an effective interest rate of:

$$i_{primary} = i_n * (1 - p - j)$$

Example :

For instant, consider a Borrower Pool with a 15% interest rate and 4.0X leverage ratio. If the Lenders supply $200K, the Secondary Pool will allocate another $800K. Assuming the Borrower borrows the full $1M for one year, they will pay $1M * 15% = $150K in interest. Of that, the Secondary Pool receives 0.15*(1 - 0.1 - 0.2) = 10.5% interest, or $800K * 0.105 = $84K. The Lenders would receive 0.15*(1 - 0.1 + 4*0.2) = 25.5% interest, or $200K * 0.255= $51K. The balance $15K is the 10% protocol reserve allocation.

2.2.2. Seed Lender Rewards

General phenomena of a Borrower Pool when a lot of other Lenders are already supplying with Secondary Pool as added leverage would give rise to ballooning to specific Borrower Pool associated with lower risk given the support by the participants. It is always riskier to be the first one in a Borrower Pool. To incentivize Seed Lenders supply, the protocol provides additional UCLtoken rewards to all Lenders who made early contribution, decreasing progressively as later Lenders join in the Borrower Pool as it reaches its limit. The protocol assigns the reward when a Lender supplies credit, but the reward is not immediately credited. The reward is proportional to the percentage of the full expected repayment of principal plus interest that the Borrower successfully repays the entire loan. This ensures the Lender only receives the Seed Lender reward after the Borrower Pool is proved to be valuable to the protocol network.

2.2.3. Staking Lenders

In addition to evaluating individual Borrower Pools, Lenders may also evaluate other Lenders in order to gain further leverage. Lenders can do this by staking UCLtoken directly on another Lender.

Based on the amount of UCLtoken staked on a given Lender, the Secondary Pool uses the Leverage Model to calculate a leverage ratio and allocate capital whenever that Lender supplies to Borrower Pools. For example, if a Lender has a leverage ratio of 4.0X based on who has staked UCLtoken on them, then they may supply to a Borrower Pool anytime they want, which the Secondary Pool will also allocate 4.0X of that amount simultaneously.

The Secondary Pool provides this leverage up to a maximum total calculated as the leverage ratio multiplied by the total value of UCLtoken staked on that Lender (if any). For example, if the Lender has $1M worth of UCLtoken staked on them with a 4.0X leverage ratio, the Secondary Pool will allocate up to $4M in total leverage.

When UCLtoken is staked on a Lender, that UCLtoken is collateralised against potential defaults for that Lender's positions in Borrower Pools. When a Borrower defaults, the UCLtoken staked on all the Lenders in that pool are reallocated to the Secondary Tranche until the Secondary Tranche is made up of their expected repayments less first lost capital entirely. This incentivises Lenders to stake on other Lenders who supply to lower risk Borrower Pools with good *credit scores*.

To reward Lenders for staking UCLtoken

on other Lenders, the protocol distributes UCLtoken to them on a regular basis. The network allocates the distributions in proportion to the interest their leveraged UCLtoken earns. This incentivizes Lenders to stake on other Lenders who supply to high yielding Borrower Pools.

Credit Scores – Any Borrower that has unfulfilled/ fulfilled its loan redemption obligations will be assigned and updated with a new weighted credit score from 0 to 5 as follows :

i. 0 : New Borrower
ii. 1 : >15% *DLV*
iii. 2 : 9.2% ≤ *DLV* ≤ 15%
iv. 3 : 4.7% ≤ *DLV* < 9.2%
v. 4 : 1.3% ≤ *DLV* < 4.7%
vi. 5 : 0 = *DLV*

Given that Defaulted Loan Value,

$$DLV = \frac{R - (p + r)}{L}$$

where,

i. Balance loan principal = *p*;
ii. Total accrued interest = *r*;
iii. Loan quantum = *L*;
iv. Recovered quantum = *R*

2.2.4. Rationale - Lender Incentives

Lenders are incentivised to provide First Loss capital to Borrower Pools because they can receive both Seed Lenders' rewards and higher effective yields on the Secondary Pool leverage. They also have an incentive to stake UCLtoken on other Lenders because they can earn additional rewards when that Lender supplies to Borrower Pools.

2.3. Liquidity Providers

Liquidity Providers supply capital to the Secondary Pool in order to earn passive yield. The Secondary Pool automatically allocates their capital to the Secondary Tranches of Borrower Pools.

2.3.1. Supplying to Secondary Pool

Liquidity Providers supply capital to the Secondary Pool in order to earn passive yield. The Secondary Pool then automatically allocates the available capital across Secondary Tranches of Borrower Pools according to the Leverage Model policy. The Secondary Pool thereby provides both diversification across Borrower Pools from Secondary to the First Loss capital of Lenders. Supplying capital to the Secondary Pool is also fully permissionless, a build in trust-less validation and verification mechanism within the network protocol.

To account and compensate Lenders for evaluating Borrowers Pools and providing First Loss capital, 20% of the Secondary Pool's nominal interest is reallocated to Lenders.

2.3.2. Optimised Yield

When Liquidity Providers supply to the Secondary Pool, They receive an equivalent amount of UCLtoken. At any time, Liquidity Providers can withdraw their UCLtoken by redeeming their UCLtoken for another available token (e.g. BUSD) at an exchange rate based on net asset value of the Secondary Pool, minus prevailing fees such as 0.5% withdrawal fee and etc. The exchange rate UCLtoken increases over time as interest repayments were directed back to the Secondary Pool.

It is possible that when a Liquidity Provider withdraws, the Secondary Pool may not have the token for redemption because it has been borrowed by Borrowers. In this

event, the Liquidity Provider may resubmit the withdrawal when new capital enters the Secondary Pool through Borrower repayments or new Liquidity Providers.

2.3.3. Investors' Incentivisation

Investors are incentivised to supply to the Secondary Pool in order to earn passive yield.

2.4. *Leverage Model

The Leverage Model determines how much capital the Secondary Pool allocates towards each Borrower Pool, based on how much it trusts each Borrower Pool.

2.4.1. Trust-less Public Consensus

In order to determine how to allocate capital from the Secondary Pool, the network protocol uses a principle of trust-less public consensus. This means that while the network protocol doesn't trust any individual Lenders, it trusts the majority collective actions within an anonymous structure.

High level concept : when more Lenders supply to a given Borrower Pool, the Secondary Pool will leverage by increasing the ratio.

Since this approach relies on counting individual Lenders, the protocol must ensure they are represented by different unique people, each requiring a UEV (Unique Entity Validation) in order to participate.

2.4.2. Leverage Model Formula

The leverage amount, A, that the Secondary Pool allocates is determined by the formula,

$$A = S * D * L$$

where:

- S is the total capital supplied by Lenders.
- D is the distribution adjustment on a scale of 0 to 1, which accounts for how evenly distributed the Lenders are. D is closer to 0 when the distribution is skewed and closer to 1 when the Lenders are more equally distributed. This ensures no single Lender has a biased influence. The formula for D uses the percent supplied by each Lender, S_n, and is based on the Herfindahl-Hirschman Index :

$$D = 1 - \sum_{i=1}^{n} s_n^2$$

- L is the leverage ratio on a scale of 0 to the maximum potential leverage ratio. Based on the number of Lenders, b, the leverage ratio increases linearly from B_{min}, the minimum number of Lenders necessary for leverage, to B_{max}, the maximum number of Lenders necessary to achieve the maximum potential leverage, L_{max} :

$$L = L_{max} * \frac{max(0, b - B_{min})}{B_{max} - B_{min}}$$

2.4.3. UEV - Unique Entity Validation

Leverage Model relies on trust-less public consensus and hence, it is critical to avoid attacks by ensuring confidence each Borrower/Lender is an unique entity. Therefore, they must each be verified before participation.

Governance approves the protocol's UEV providers. KYC of off chain verification

and validation of wallet addresses to ensure these are unique entities. Once on chain decentralized unique IDs mature, Governance can also vote to migrate the protocol to these new providers.

2.4.4. Governance

Governance is managed by a close DAO community and has the ability to perform maintenance functions and parameter adjustments via decentralized governance votes, rollout in off-chain phases, including but not limited to:

- Upgrading of smart contracts
- Changing/ updating of protocol configurations and parameters
- Selecting UEV providers
- Setting the rewards and distribution of UCLtoken and/or new PAIR type
- Halting protocol activity in the event of an emergency

2.4.5. Anti-Fraud

Because the protocol does not require excess crypto collateralisation, this gives rooms to potential fraud. It is worth exploring in depth how the protocol can combat against it. Fraud scenarios focus on malicious or dishonest activity, not poor performance of valid and legit borrowing.

2.4.6. Fraudulent Borrower & Honest Lenders

A fraudulent Borrower could attempt to fool Lenders into thinking they are legitimate, followed by borrowing capital without repayment. The first line of defence are our Lenders, who are highly incentivised to analyse their investments closely, given that they supply higher risk Primary capital. The second line of defence would be the auto recovery of loan positions. It is likely that Lenders would want to additional validation and verification of Borrowers and potentially communicate with them directly since Lenders are protected should any loan defaults, an attempt to a full recovery will be implemented by the smart contract to unwind all loan positions. Similarly, Lenders may also sign off chain legal contracts with Borrowers for appropriate legal recourse.

2.4.7. Borrower & Lenders Conspiracy

A Borrower could conspire with people they know to act as Lenders and supply to their Borrower Pool. This would artificially inflate the leverage ratio and fool the Secondary Pool into allocating additional capital. The first line of defence against this are the Lenders' assessment via credit scores and off-chain verification if needed as any auto-recovery in the event of loan default would not be 100% (e.g. gas fee). The second line of defence is that it requires many individually verified Lenders to supply significant amounts of upfront capital in order for the Secondary Pool to provide leverage, which makes such conspiracy difficult and highly expensive. Lastly, the UEV adds resistance by making it difficult to programmatically create fake Lenders.

2.4.8. Fraudulent Lenders & Honest Borrowers

An individual or group of Lenders might supply to a particular Borrower Pool even when they do not view it as low risk. This would artificially increase the leverage ratio and fool the Secondary Pool into allocating additional capital, inflating the Lenders' yields. The first line of defence against this is that the UEV requires each Lender to be verified, preventing an attack and requiring the coordination of many people concurrently. The second line of defence against this is that it requires the

Lenders to assume real risk by supplying First Loss capital. The Lenders only achieve higher yields if the Borrower repays what they borrowed, in which case it is beneficial to all participants in the protocol, including the Secondary Pool.

3. CONCLUSION

In this paper we have considered this etherum type (i.e. BEP20, BSC – Binance smart chain) network from two points of view, the Optimist and the Pessimist, and examined the workings of DeFi-based systematically. First, we lay out the primitives for DeFi before categorizing DeFi protocols by the type of operation they provide. We examined if the security challenges protocols are exposed by making a distinction between technical and economic security risks. In so doing, we were able to systematize attacks that have been proposed in theory and/or occurred in practice into categories of attacks that either rely on an agent's ability to generate risk-free profits by exploiting the technical structure of a blockchain or to game the incentive structure of a protocol to obtain a profit/yield at the expense of the protocol. Finally, we drew the attention to open research challenges that require a holistic understanding of both the technical and economic risks. While DeFi may have the full potential to creating a permissionless and non-custodial financial system, the opinion put forward by the DeFi optimist, the open technical and economic security challenges remain strong. The DeFi pessimist is, at least for now, on firm ground: solving these challenges in a robust and scalable way is a central challenge for researchers, developers and DeFi practitioners.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] DeFi Pulse, "The decentralized finance leaderboard at defi pulse," 2020. [Online]. Available: https://defipulse.com/

[3] Uniswap, "Uniswap," 2020. [Online]. Available: https://app.uniswap.org/#/swap

[4] Coinbase, "Coinbase," 2020. [Online]. Available: https://www.coinbase.com/

[5] O. Godbole, "Defi flippening comes to exchanges as uniswap topples coinbase in trading volume," CoinDesk, 2020. [Online]. Available: https://www.coindesk.com/defi-flippening uniswap-topples-coinbase-trading-volume

[6] DeFi Hacks, "Defi hacks," 2021. [Online]. Available: https://defihacks.wiki/

[7] P. Baker, "Defi lender bzx loses $8m in third attack this year," CoinDesk, 2020. [Online]. Available: https://www.coindesk.com/defi-lender-bzx-third-attack

[8] T. Wright, "Akropolis defi protocol 'paused' as hackers get away with $2m in dai," 2020, accessed: 29-12-2020. [Online]. Available: https://cointelegraph.com/news/akropolis- defi protocol- paused- as-hackers-get-away-with-2m-in-dai

[9] K. Reynolds and D. Pan, "Cover protocol attack perpetrated by 'white hat,' funds returned, hacker claims," CoinDesk, 2020. [Online]. Available: https://www.coindesk.com/cover-protocol-attack-perpetrated-by-white-hat-all-funds-returned-hacker-claims

[10] Harvest Finance, "Harvest flashloan economic attack post-mortem," 2020, accessed: 29-12-2020. [Online]. Available: https://medium.com/harvest-finance/harvest- flashloan-economic- attack- post-mortem-3cf900d65217

[11] M. Liu, "Urgent: Ousd was hacked and there has been a loss of funds," 2020, accessed: 29-12-2020. [Online]. Available: https://medium.com/originprotocol/urgent- ousd-has-hacked- and-there-has-been-a-loss-of-funds-7b8c4a7d534c

[12] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W.Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in 2015 IEEE symposium on security and privacy. IEEE, 2015, pp. 104–121.

[13] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meik-lejohn, and G. Danezis, "Sok: Consensus in the age of blockchains," in Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 2019, pp. 183–198.

[14] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "Sok: Off the chain transactions," IACR Cryptol. ePrint Arch., vol. 2019, p. 360, 2019.

[15] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, "Sok: commu-nication across

distributed ledgers." IACR Cryptol. ePrint Arch., 2020.
[16] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1–34, 2019.
[17] G. Wood et al., "Ethereum: A secure decentralised generalised trans-action ledger," Ethereum project yellow paper, vol. 151, no. 2014, pp.1–32, 2014.
[18] V. Buterin, "A next-generation smart contract and decentralized application platform," white paper, vol. 3, no. 37, 2014.
[19] D. Perez and B. Livshits, "Broken metre: Attacking resource metering in EVM," in 27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020. The Internet Society, 2020. [Online]. Available: https://www.ndss-symposium.org/ndss-paper/broken-metre-attacking-resource-metering-in-evm/
[20] S. M. Werner, P. J. Pritz, and D. Perez, "Step on the gas? A better approach for recommending the ethereum gas price," arXiv preprint arXiv:2003.03479, 2020.
[21] DeFi Pulse, "What is defi?" 2019. [Online]. Available: https://defipulse.com/blog/whatis-defi/
[22] S. P. Jones, J.-M. Eber, and J. Seward, "Composing contracts: an adventure in financial engineering," ACM SIG-PLAN Notices, vol. 35, no. 9, pp. 280–292, 2000.
[23] R. Daniel and B. Roth, "weth — erc20 tradable version of eth," 2020. [Online]. Available: https://weth.io/
[24] W. Bitcoin, "Wbtc wrapped bitcoin an erc20 token backed 1:1 with bitcoin," 2020. [Online]. Available: https://wbtc.network/
[25] Synthetix, "Synthetix — decentralised synthetic assets," 2020.[Online]. Available: https://www.synthetix.io
[26] F. Vogelsteller and V. Buterin, "Eip-20: Erc-20 token standard," 2015. [Online]. Available: https://eips.ethereum.org/EIPS/eip-20
[27] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "Eip-721: Erc-721 non-fungible token standard," 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721
[28] M. Fr¨owis, A. Fuchs, and R. B¨ohme, "Detecting token systems on ethereum," in International conference on financial cryptography and data security. Springer, 2019, pp. 93–112.
[29] J. Dafflon, J. Baylina, and T. Shababi, "Eip-777: Erc777 token standard," 2017. [Online]. Available: https://eips.ethereum.org/EIPS/eip-777
[30] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, "Eip-1155: Erc-1155 multi token standard," 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1155
[31] V. Minacori, "Eip-1363: Erc-1363 payable token," 2020. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1363
[32] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.
[33] D. Perez, J. Xu, and B. Livshits, "Revisiting transactional statistics of high-scalability blockchains," ser. IMC '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 535–550. [Online]. Available: https://doi.org/10.1145/3419394.3423628
[34] P. McCorry, A. Hicks, and S. Meiklejohn, "Smart contracts for bribing miners," in International Conference on Financial Cryptography and Data Security. Springer, 2018, pp. 3–18.
[35] F. Winzer, B. Herd, and S. Faust, "Temporary censorship attacks in the presence of rational miners," in 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2019, pp.357–366.
[36] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges," arXiv preprint arXiv:1904.05234, 2019.
[37] R. Leshner and G. Hayes, "Compound: The money market protocol," 2019. [Online]. Available: https://compound.finance/documents/Compound.Whitepaper.pdf
[38] AAVE, "Aave: Protocol whitepaper v1.0," 2020, accessed: 13-08-2020. [Online]. Available: https://github.com/aave/aave-protocol/blob/master/docs/Aave Protocol Whitepaper v1 0.pdf
[39] Maker, "The maker protocol: Makerdao's multi-collateral dai (mcd) system," accessed: 08-06-2020. [Online]. Available: https://makerdao.com/en/whitepaper/