SmartMoney/Enigma Research Note

October 6, 2021

Compound ($COMP)

- TYPE: Borrowing and lending
- CHAIN(S): ETH, Compound Gateway
- CIRCULATING SUPPLY: 6M
- MAX SUPPLY: 10M
- TVL: $10B
- MARKET CAP: $1.92B
- CONTRACT ADDRESS: 0xc00e94cb662c3520282e6f5717214004a7f26888

Product Overview/Summary

The Compound protocol is one of DeFi's oldest borrowing and lending platforms. The protocol's code eliminates the need for intermediaries to regulate over a dozen lending markets. Instead, users deposit assets directly to Compound pools in exchange for interest-bearing cTokens. Compound's governance process approves assets for use as collateral, so lenders can borrow a proportion of their cToken position.

Today, Compound is especially exemplary of DeFi's chief risk from smart contracts. While the code obscures the need for intermediaries, an omitted "=" in a key smart contract allowed millions of COMP tokens to be distributed to the wrong user wallets. Within hours, the Compound community, aided by developers across DeFi, isolated the issue and traced its origin. Participants and observers can view the open governance process in action as users debate on the proposals to patch the code and recover the lost value.

A deliberative governance process is Compound's greatest strength and limitation. Competitor lending markets offer many more assets for lending than users can access on Compound. While more value can accrue to the competition, a strong user community, and innovative value accrual mechanisms help maintain Compound's position among the top DeFi protocols by Total Value Locked.

Why it's interesting

Product and Technology

A suite of smart contracts enables Compound's open money markets. All approved assets are pooled by type. Lenders deposit assets to each pool. Borrowers can withdraw assets at up to 80% of their deposited value that are approved as collateral. Lending positions are represented by cTokens, sent to each lender's Ethereum-based wallet.

Compound's cToken smart contract helped innovate the digital bearer asset model that is foundational to DeFi. As a representation of the lender's stake in a lending pool, the cToken provides programmable proof of the value locked in Compound. Users, including other protocols, could directly and verifiably reference cToken code to structure new financial products. For example, after receiving cTokens in proportion to DAI supplied to Compound's DAI lending pool, the lender could stake their cTokens in a Curve liquidity pool to make a market for the interest-bearing tokens. By lending and supplying liquidity, the depositor accrued compounding yield on their long asset position.

The Comptroller smart contract uses cToken balances to regulate each lending market. Each asset and cToken have corresponding exchange and interest accrual rates, while the code designates several assets as collateral. When a user withdraws an asset, the Comptroller verifies the cToken's collateral status and enables borrowing at the approved loan-to-value, or LTV. As a borrower accrues interest, their borrowed position offsets the interest accrued by their collateral deposit.

Comptroller Smart Contract Bug

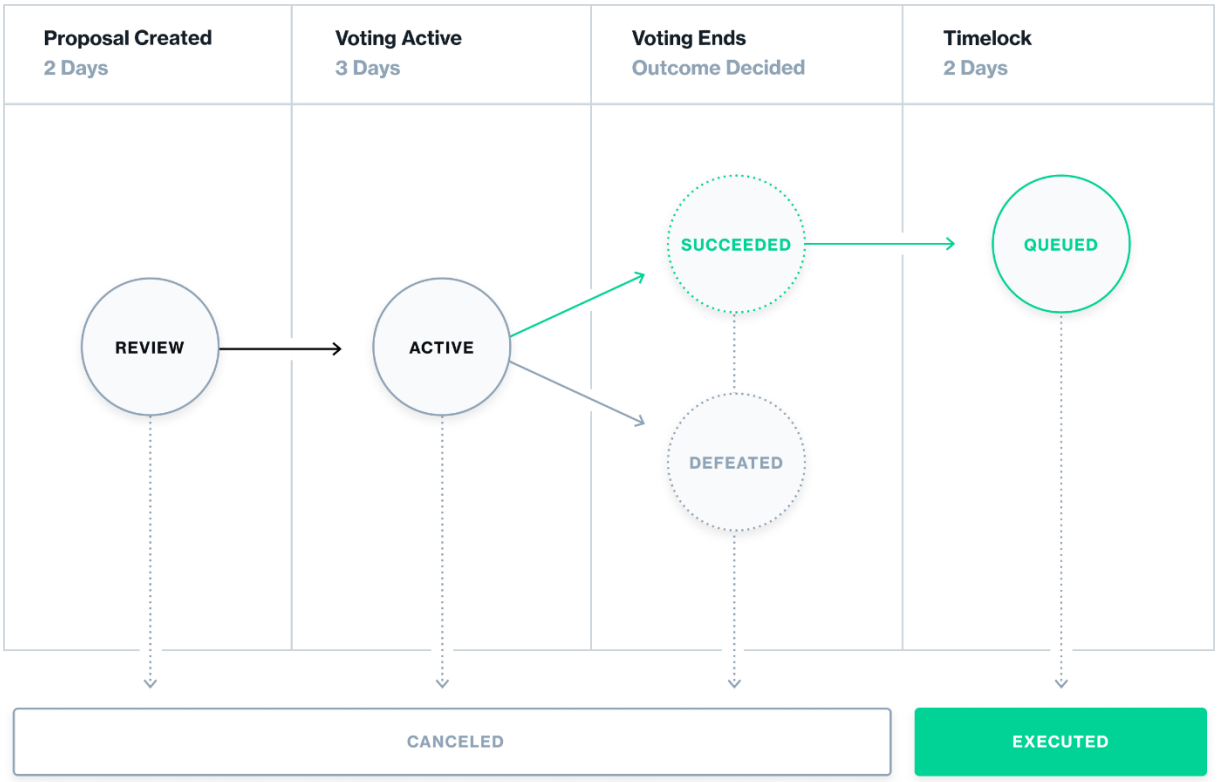
On September 29, 2021, a simple omission issued millions of dollars in COMP tokens to the wrong addresses. Compound Proposal 62 introduced new code that separated COMP issuance rates to borrowers and lenders per asset. Specific COMP issuance rates would be more effective as a borrowing incentive, rather than a flat rate across functions. During implementation, a community developer omitted a "=" where the amount of COMP issued to certain borrowers should have been limited to ">=". One character released caused an estimated 240k COMP tokens to be released to the wrong addresses.

By October 1st, Compound governance participants discovered the bug and began the process to stop all issuance. After several days, and two additional governance proposals, the development community has nearly patched the bug. Instead of confiscating or burning the mistaken COMP, the community decided to allow mistaken recipients to return the COMP. After enough COMP may be returned, the protocol will update its accounting to incorporate the additional issuance.

Governance

Compound set an early standard as one of the first DeFi protocols to fully decentralize. On February 26, 2020, Compound Labs founder, Robert Leshner, announced plans to transition the protocol's governance and operations. By April 2020, on-chain governance launched to match the protocol's open-source operating code separate user interface. This made Compound unique among comparable DeFi protocols. Many projects are open source at the operating level, where community participants maintain the code on public repositories. However, a centralized team may maintain the user interface, which tends to funnel all users to one centralized point of access. Instead, Compound's user interface and operating code repositories are both maintained by the community.

The COMP token powers decision-making among Compound community members. Token holders must post or delegate their COMP to another user to propose, vote, and implement code in any part of the protocol. With 100 COMP, any address can propose an update in the Compound governance smart contract. An autonomous proposal becomes eligible for voting as a governance proposal once users delegate 65,000 COMP in its favor.



After 2 days' review, and at least 400,000 COMP staked, the proposal may be implemented 2 days later. With a total of one week, Compound's governance process was designed to build consensus for deliberate and updates.

TOKENOMICS

Token Distribution and Valuation

Compound issues the COMP token to incentivize community participation among users instead of passive investors. To maintain community governance, Compound only issues tokens to borrowers and lenders of approved assets. Governance participants approve assets to receive COMP to incentivize both borrowing and lending in the asset. Some assets, like ETH, do not receive COMP rewards for borrowing because demand is insufficient. Instead, COMP tokens are awarded to the most users by the pools in highest demand.

Users that supply their COMP rewards receive additional COMP issuance for compound returns. Most COMP issued is staked in the protocol's lending pool or governance contract. To date, over

half of the entire COMP supply has been issued to borrowing and lending pools. Though no dividend or protocol earnings accrue to COMP holders, Compound's issuance drives demand for the token.

Though COMP value can increase due to demand for staking, users can depress price when they sell their COMP to monetize their Compound yield. Additionally, no dividends or revenue to token holders means that COMP holders receive no cash flows without staking.

cTokens and Lender Returns

Lenders earn rewards by supplying assets to the protocol to be borrowed from each asset's pool. For their deposited, or lent, assets, users receive a representative amount of cTokens. Over time, the exchange rate at which cTokens can redeem the lent assets grows, so cTokens can redeem more of the lent asset. Instead of simple interest, lenders redeem more assets than they deposited. The gain in over time represents the revenue to lenders for supplying liquidity to Compound markets.

cToken Yield by Exchange Rate

Lent asset	ETH
cToken	cETH
Exchange rate at lend	0.0200
Exchange rate at redemption	0.0216
Total gain	7.96%

Source: cTokens, Compound Docs: https://compound.finance/docs/ctokens#exchange-rate

Value Accrual

Of the $15B deposited, borrowed assets total $5B. The top 3 deposited assets, ETH, USDC, and DAI, indicate the most used collateral on Compound. The 3 most borrowed assets are also USDC and DAI, accompanied by USDT. The asset composition and interest rates reveal potential opportunities for yield-seeking investors.

Annual Yield and COMP Issuance per Asset Lend and Borrow Positions

Date	10/4/21
COMP Price	$327
Lend Value	$1,000

Asset	Lend Rate	COMP Issuance to Lenders	1 Year Total Yield	COMP Issued	Borrow Rate	COMP Issuance to Borrowers	1 Year Net Yield	COMP Issued
AAVE	0.55%	0.00%	0.55%	0.0000	5.32%	0.00%	-5.32%	0.0000
BAT	**0.18%**	**1.35%**	**1.53%**	**0.0413**	**3.91%**	**23.66%**	**19.75%**	**0.7231**
COMP	**0.79%**	**2.36%**	**3.15%**	**0.0721**	**6.15%**	**14.11%**	**7.96%**	**0.4313**
DAI	2.68%	2.00%	4.68%	0.0611	4.03%	2.54%	-1.49%	0.0776
LINK	**0.41%**	**0.60%**	**1.01%**	**0.0183**	**4.77%**	**5.19%**	**0.42%**	**0.1586**
REP	0.00%	0.00%	0.00%	0.0000	35.57%	0.00%	-35.57%	0.0000
SUSHI	0.06%	0.00%	0.06%	0.0000	2.68%	0.00%	-2.68%	0.0000
TUSD	2.53%	0.00%	2.53%	0.0000	3.74%	0.00%	-3.74%	0.0000
UNI	**0.10%**	**0.55%**	**0.65%**	**0.0168**	**3.48%**	**14.53%**	**11.05%**	**0.4441**
USDC	4.16%	1.81%	5.97%	0.0553	5.57%	2.23%	-3.34%	0.0682
USDT	6.13%	1.01%	7.14%	0.0309	8.02%	1.21%	-6.81%	0.0370
WBTC	**0.18%**	**0.40%**	**0.58%**	**0.0122**	**3.49%**	**6.52%**	**3.03%**	**0.1993**
WETH	**0.09%**	**0.14%**	**0.23%**	**0.0043**	**2.47%**	**3.22%**	**0.75%**	**0.0984**
YFI	3.48%	0.00%	3.48%	0.0000	11.84%	0.00%	-11.84%	0.0000
ZRX	0.76%	0.90%	1.66%	0.0275	6.77%	5.97%	-0.80%	0.1825

Source: User Distribution, Governance, Compound. https://compound.finance/governance/comp

Due to available supply and differences in demand, USDT is nearly 50% more expensive to borrow than USDC. Likewise, USDT offers a higher APR than USDC. An investor could borrow USDC, trade for USDT, and deposit it for a net 3% yield. Because USDT is volatile relative to USDC, USDT is not approved on Compound, so the trade could not occur in reverse.

Competitive Landscape

Compound is among the three most dominant lending protocols on Ethereum and DeFi, generally. Over $10B of net digital asset value is locked in Compound. Only MakerDao and Aave protocols surpassed Compound, with $13B and $14B of TVL, respectively. Unlike commercial and money center banks, DeFi lending protocols rarely compete on cost.

Instead, interest rate variability and over-collateralization require users to compare protocols on yield offered. At the protocol level, Aave, MakerDao, and Compound attract deposits through integrations and composability. Development partnerships and smart contract code allow other protocols to use Compound money markets for lending within their own protocols. More development in each lending protocol's ecosystem grows net TVL.

A limited market offering limits Compound's TVL growth in exchange for reduced volatility and smart contract risk. The Compound community maintains strict approval standards for borrow and lend assets, with more strict approval of collateral assets. Aave offers 31 asset markets compared to Compound's 13.

TVL among Top 5 B&L Protocols

	COMP					Comparables		
	High	Low	Med	Avg	10/4/21	AAVE	MKR	ANC
TVL/MC	0.23x	0.16x	0.19x	0.19x	0.20x	0.28x	0.17x	0.10x

Source: DeFi Llama, accessed 10/4/21: https://defillama.com/home

Recommendations

Though last among the top three lending protocols, Compound is a model for consistent decentralized protocol control. The protocol's governance and development community demonstrated resiliency in the face of the most recent smart contract bug. As the first DeFi protocol to launch non-stable digital asset money markets, the community's experience was an asset to resolving the error and will continue to be in the future.

Despite the protocol's fortitude, COMP is not most productive alone. Instead, supplying COMP to Compound's lending pools will earn yield and grow an investor's holdings. As other investors monetize their COMP yield, long-term suppliers may experience volatility. Long-term COMP stakers are likely withstand price movement while they compound their yield.

DISCLAIMER

This document has been prepared by Enigma Securities Ltd. in cooperation with members of the Makor Group ("Makor" or the "Makor Group") including Makor Securities London Limited, Oscar Gruss & Son, Inc., and Smart Money Financial Services, Inc.. This document is intended for institutional investors and is not subject to all the independence and disclosure standards applicable to research reports prepared for retail investors. This information represents neither an offer to buy or sell any security or cryptocurrency nor, because it does not take into account the differing needs of individual clients, investment advice. Trading cryptocurrency and related instruments carries a high level of risk and may not be suitable for all investors. Those seeking investment advice specific to their financial profiles and goals should contact their Makor Group representative. Makor believes this information to be reliable, but no representation is made as to accuracy or completeness. This information does not analyze every material fact concerning a company, industry, security, or cryptocurrency. Makor assumes that this information will be read in conjunction with other publicly available data. Matters discussed here are subject to change without notice. There can be no assurance that reliance on the information contained here will produce profitable results.

A security or other instrument denominated in a foreign currency is subject to fluctuations in currency exchange rates, which may have an adverse effect on the value of the security or instrument upon the conversion into local currency of dividends, interest, or sales proceeds. Makor trades, and will continue to trade, the securities covered in this document on a discretionary basis on behalf of certain clients. Such trading interests may be contrary to or entered into in advance of this document.