DeFi
Education
Fund

## Guiding Principles 2023

Today, DeFi stands before a challenging yet innovative hour, rich with possibilities. Designing, launching, and maintaining DeFi protocols will require both a steady hand and mind to guide us forward.

It presents challenges that incorporate questions across various fields, from governance and economics to the proliferation and protection of open-source code.

The very concept of decentralized finance, where traditional intermediaries are removed and smart contracts rule vast new terrains of peer-to-peer economic activity, is foreign, confusing, and sometimes threatening to most uninitiated observers.

To cultivate a better understanding of DeFi and provide the ecosystem with a foundation for safety and success, we started a months-long collaboration of DeFi participants in 2021 to produce a set of "guiding principles," publishing them on Github in January of 2022 for further discussion.

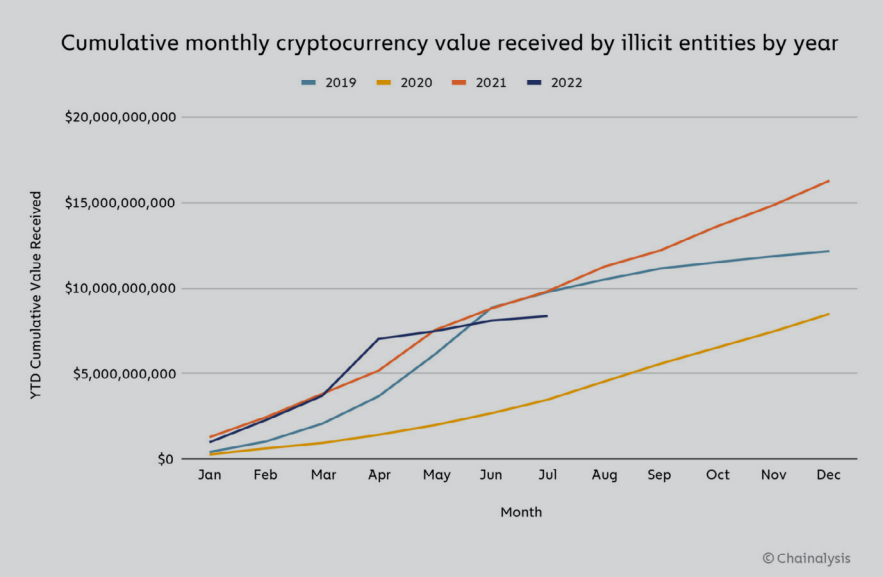
These principles seek to maintain and support the integrity of permissionless DeFi protocols, while providing insight to policymakers as to the workings of well-designed projects and protocols as they seek to further understand DeFi.

Importantly, these principles are meant to spark continued conversation and engagement on these key questions. We encourage insight and discussion as we refine and expand them.

—DeFi Education Fund

**Illicit Activity Prevention**

DeFi developers should commit to leveraging the functionality of distributed ledgers to deter, detect, and disrupt illicit financial activity; concurrently, developers should prioritize, support, and preserve fundamental privacy rights. These goals are not opposed; commitment to sustaining the privacy of individuals does not need to undercut official action against illicit activity.




Chainalysis estimated that only 0.15% of 2021's cryptocurrency transactions were illicit; meanwhile, the International Monetary Fund last estimated in 1990's that 2-5% of traditional financial transactions were illicit and the United Nations last estimated in the 2000's that 2.7% of global GDP was illicit.

**Development and Launch**

The proper development of DeFi protocols is essential to their success and security. As Confucius once said, "Success depends on previous preparation, and without such preparation there is sure to be failure."

Prior to their deployment onto a blockchain network's mainnet, developers should adhere to rigorous standards to test their protocol's code according to the most appropriate practices for the risks involved.

Developers may wish to consider reviewing code both internally and through peer review, performing an independent security review as an additional measure, making recommended changes and repeating the process with each recommended change.

Testing should include both smart contracts and interactions between them, as well as validating the on-chain state of contracts following each phase of deployment.

Thereafter, the protocol should be deployed on a permissionless blockchain network with a decentralized governance structure not modifiable by a single person, entity, or coordinated group of persons or entities, protecting transactional integrity from unilateral control.

Lastly, a DeFi protocol should consider initially launching with the appropriate control in place, such as liquidity caps, to lessen the risk of capital loss to its users. Bugs or potential attack vectors discovered during this "guarded" launch should be appropriately addressed.

**Transparency and Disclosures**
Transparency is fundamental to DeFi's infrastructure where transactions are publicized on a blockchain so that participants can confirm their validity and the order in which they were received, eliminating the need for an intermediary.

Additionally, its open-source code grants transparency into its workings and democratizes authority to developers across the network that vary in knowledge, biases, and incentives. This enables proper checks and balances as well as the ability to build off one another and evolve the technology.

For these reasons, transparency must be embedded in a protocol at a high level to enable verifiability by independent ascertainment. For verifiability to prevail, information and any material changes should be made freely accessible on a public website. Here are suggestions:

Open-Source Code and Transaction Verifiability
Prior to deploying a DeFi protocol's code on a blockchain network, developers should publish a text listing of applicable commands to be compiled or assembled into an executable computer program for participants to access the protocol, amend the code, and confirm transactions, pursuant to an open-source license.

Thereafter, all protocol transactions should be publicly verifiable with a narrative description of the steps necessary to independently access, search, and verify transaction history included.

Tokenomics
The economics of a DeFi protocol's associated token, if any, should be disclosed and independently verifiable. This information should include: the token's launch process, generation process, supply cap, release schedule, initial allocation, total outstanding amount, and how changes can be applied.

Earnings
Disclosures should include a user's potential earnings from mining, staking, liquidity provisions, liquidations, funding rates, or other profitable mechanisms within the protocol, as well as specification of the common circumstances that could result in a user not receiving those earnings.

Fees
Disclosures should include potential user fees from mining, staking, borrowing, liquidity provision, affecting liquidations, being liquidated, or other user-actions, as well as common circumstances that may result in receiving less value than otherwise expected.

Equity Financings, Prior Token Sales, and Related Commitments
Prior token allocations, sales, or commitments—and any limitations or restrictions (e.g. vesting schedules) associated with them—should be disclosed and independently verifiable to the extent possible. Additionally, any restrictions or commitments (e.g. development limitations, prior equity holder approval right before launch, protections tied to protocol activity, etc.) associated with impactful equity financing to protocol development or operation should be disclosed and independently verifiable to the extent possible.

Governance Rights and Process
Governance refers to systems and processes which enable interested individuals, parties, and groups to make effective decisions toward common objectives.

Traditional governance tends to be centralized and fails to encourage robust debate among interested stakeholders; blocks new ideas and strategies; and gets hijacked by loud, partisan forces.

DeFi has an opportunity to shift governance toward a more egalitarian form and promote interdependence and human cooperation by distributing both authority and ownership among its participants.

To shift toward a more egalitarian form of governance and empower participation, DeFi protocols must disclose the following information:

I whether and the extent to which a DeFi protocol is governable;
II what powers governance can exercise over the protocol;
III how the terms and the scope of governance powers can be modified;
IV how any single person, entity, or coordinated group of persons or entities can unilaterally control may modify the protocol, including the effect of those changes on users, any required time delays when making those changes, and the manner in which those changes may be made;
V how governance rights are distributed and exercised;
VI how the governance process works;
VII how a person can participate in governance;
VIII how a person can exit a protocol and governance; and
IX the identity of any person or entity, or group of persons or entities under common control, holding more than 1 percent of the voting power of the governance mechanism, a description of any limitations or restrictions on the transferability of tokens held by such persons to participate in governance, and a description of any rights held by such persons to obtain tokens in the future in a manner that is distinct from how any third party could obtain tokens.

Negative Events
Any event or situation that materially affects the expected functionality of a DeFi protocol should be promptly disclosed and information to independently verify such an event or situation should be made available. Developers of DeFi protocols should develop and test predefined procedures for responding to such an event or situation.

Deployment of New Code
Before any changes to a DeFi protocol's deployed code are implemented, the new code should follow the procedures set forth under Development and Launch.

Third-Party Networks, Protocols, and Oracles
A thorough list of a protocol's required third-party blockchain networks, protocols, or oracles should be disclosed to users and a link, if available, to information regarding said third-parties.

Risks
Developers should inform users of a DeFi protocol's high degree of risk, which may result in a loss of funds, and conduct periodic reviews of risk, including reviews of underlying risk assumptions.

Communications
The information hub should include information about any official communication channels, including for discussion of technical matters related to the protocol.

The formation of the East India Company is a good example of successful governance design supporting future success. A bunch of guys got together and hashed out a new way to pool risk, money, ambition, planning, and the nature of the relationship between the participants of the endeavor. They invented the "joint-stock company" and it was successful, to say the least.

**Market Integrity**
The final component to maintain the integrity of a DeFi protocol is ensuring its market integrity against fraud and manipulation.

Manipulation and Fraud Prevention
DeFi market participants should not:

I engage, or attempt to engage, in any manipulative conduct or scheme to defraud;
II make, or attempt to make, any untrue or misleading statement with respect to material information or omit to state any material information in order to make information made available not untrue or misleading;
III engage, or attempt to engage, in any act, practice, or course of business to, or to attempt to, defraud or deceive any person; or
IV deliver, cause to be delivered, or attempt to deliver or cause to be delivered false, misleading or inaccurate information that affect or tend to affect the price of any asset, knowing or acting in reckless disregard of the fact that such information is false, misleading or inaccurate.

"White Hat" Incentivization
Developers should take additional measures by implementing "white hat" incentives for benign testing and auditing of their code through a "bug bounty" program.