Smart Contracts / Blockchain Level	Examples https://immunefi.com/severity-updated/	Bounty Reward (up to)
3. Critical	- Empty or freeze the contract's holdings (e.g. economic attacks, flash loans, reentrancy, logic errors, integer over-/under-flow) - Cryptographic flaws - Cronos (blockchain), smart contracts and app with the focus on any vulnerabilities causing unintentional withdrawal/draining of funds/loss of user funds.	Up to USD 1,337,133.7
2. High	- Users spoof each other - Theft of yield - Transient consensus failures	Up to USD 250,000
1. Medium	- Contract consumes unbounded gas - Block stuffing - Griefing denial of service (i.e. attacker spends as much in gas as damage to the contract) - Gas griefing	Up to USD 25,000

Websites and App Level	Bounty Reward (up to)
Note: The web vulnerabilities in scope are those which will directly lead to loss of user funds, or breach of sensitive data, or deletion of site data	
All web vulnerabilities are covered here. 1. Remote Code Execution 2. Significant manipulation of the account balance 3. Leakage of sensitive data 4. XSS/CSRF/Clickjacking affecting sensitive actions 5. Theft of privileged information 6. Partial authentication bypass 7. Other vulnerability with clear potential for financial or data loss 8. Other XSS (excluding Self-XSS) 9. Other CSRF (excluding logout CSRF) Qualifying Vulnerabilities in the Cronos website/application. Once user submitted vulnerabilities report, we will use CVSS calculator to check severity and based on that we will reward bounty. Note: If the Report does not include a valid Proof-of-Concept, the qualification of rewards will be decided according to reproducibility and severity of the vulnerability, and the rewards amount may be reduced significantly. The specific amount of the bounty will vary according to: ● The effect of the bug. ● The cause of the bug. ● Whether or not the person who reports the bug suggests a solution to the bug or helps in its resolution.	Critical - USD 15,000 High - USD 7,500 Medium - USD 1,000