Code Review DAO

Wulf Kaal, Ph.D.[1]

Abstract

The open-source code review process is upgraded and scaled through the use of decentralized community governance. The code review decentralized autonomous organization (CRDAO) distinguishes itself from legacy system code review competitors through industry-leading code review price discovery, increased speed, community audit, competitive pricing, WEB3 transparency, and accountability. The key distinguishing feature of the CRDAO code review process is its unparalleled ability to apply community code review audits.

Key Words: Code Audit, Quality Controls, Code Assurances, Decentralized Autonomous Organization, Token Models, Cryptocurrencies, Feedback Effects, Emerging Technology, Tokens, Blockchain, Distributed Ledger Technology

JEL Categories: K20, K23, K32, L43, L5, O31, O32

---

[1] Professor of Law, University of St. Thomas School of Law. The Author is grateful to many members of the open source community who provided valuable feedback.

Table of Contents

Background

Code review is a process that is intended to ensure software quality. Usually, it consists of developers, other than the author of a given piece of code, manually checking code or changing the code before they are merged into the main code repository.[2] Ideally, the process of code review finds defects or improvement opportunities without the software execution and before the product delivery, thereby reducing the costs of future fixes.[3]

[2] Nicole Davila & Ingrid Nunes, A Systemic Literature Review and Taxonomy of Modern Code Review, 177 J. Sys. & Software 1110951 (2021).

[3] *Id. at 1.*

Modern code review (MCR) can be traced back to software "inspections."[4] Inspections consisted of formal meetings where participants would prepare ahead of time. Unlike inspections, many modern code review processes are asynchronous and often support geographically distributed reviewers.[5] Adopting agile methods and distributed software development has resulted in less formal code reviews where the inefficiencies of inspections are replaced with a flexible, tool-based, and frequent process known as modern code review.[6]

Code reviews are recognized as a vital practice to assure software quality. Many open-source projects such as Android, QT, and Eclipse, include code review as part of their software development process.[7] Moreover, many large technology companies like Microsoft, Oracle, and Samsung, all adopt code reviews for their software development.[8] Code reviews provide many benefits, for example: they attempt to find bugs in the code, help improve the quality of the code on productions, find better ways to implement the change, spread knowledge about the project, and create awareness of the changes in the code base.[9]

---

[4] Jacek Czerwonka, Michaela Greiler & Jack Tilford, *Code Reviews Do Not Find Bugs: How the Current Code Review Best Practice Slows Us Down*, 37th IEEE International Conference on Software Engineering 1, 27-28 (2015).

[5] *Id.* at 1.

[6] *Id.* at 2.

[7] Felipe Ebert, Fernando Castor, Nicole Novielli & Alexander Serebrenik, *An Exploratory Study on Confusion inCode Reviews*, 26 EMPIRICAL SOFTWARE ENG'G 12 (2021).

[8] *Id. at 2.*

[9] *Id. at 2.*

Despite the benefits and widespread adoption within the technology industry, code reviews can incur great cost and slow down the overall code development process.[10] Consequently, modern code review processes are expensive. Developers spend a significant amount of time reviewing the changes of others – an average of 6 hours per week.[11] Not only is this a significant amount of time, but it also requires an opportunity cost on project development as developers are forced to switch away from their current work. Therefore, it is important to pinpoint the issues that make modern code review a timely and expensive process in an effort to understand solutions to these issues.

It is a common conception that code reviews increase the functionality and quality of code. Code reviews also clarify the intended functionality of the code which minimizes the risk that malfunctioning or suboptimal code gets released and causes damages.

Growth Potential of the Smart Contract Industry

The smart contract industry has enormous growth potential. Different measures help asses that growth including the CAGR (compounded annual growth rate) used as well as the current valuation of the smart contract industry. Estimates of the smart

[10] *Id.*

[11] Czerwonka, *supra* note 4.

contract industry's future value by 2032 range from 1 to 2.5 billion dollars.[12]

Smart Contract Vulnerabilities Undermine Industry Growth

The growth of the smart contract industry across industry vectors is affected by the attack vectors pertaining to smart contracts. Smart contract bugs can result in financial loss,

[12] Varying group estimates are listed below from low to high.Group Estimates for the Smart Contract Industry's Value by 2032:

1. **SNS Insider: $1 billion, at a CAGR of 24.2%**
   1.1. *Smart Contracts Market Size*, SNS Insider, https://www.snsinsider.com/reports/smart-contracts-market-1542 (last visited Jan. 4, 2024).
2. **Verified Market Research: $1.2 billion, at a CAGR of 26.4%**
   2.1. *Smart Contracts Market Size and Forecast*, Verified Market Research, https://www.verifiedmarketresearch.com/product/smart-contracts-market/ (last visited Jan. 4, 2024).
3. **Valuates Reports: $1.4 billion, at a CAGR of 24.2%**
   3.1. *Global Smart Contracts Market Research Report*, Valuates Reports, https://reports.valuates.com/market-reports/QYRE-Auto-31L1599/global-smart-contracts (last visited Jan. 4, 2024).
4. **Acumen Research & Consulting: $1.417 billion, at a CAGR of 22.8%**
   4.1.Smart Contracts Market Size: Global Industry, Share, Analysis, Trends and Forecast 2023 – 2032, ACUMEN RESEARCH & CONSULTING, https://www.acumenresearchandconsulting.com/smart-contracts-market (last visited Jan. 4, 2024).
5. **Future Market Insights: $1.5 billion, at a CAGR of 23.5%**
   5.1. *Smart Contracts Market Outlook (2022 to 2032)*, Future Market Insights, https://www.futuremarketinsights.com/reports/smart-contracts-market (last visited Jan. 4, 2024).
6. **Allied Market Research: $2.5 billion, at a CAGR of 29.6%**
   6.1.Smart Contracts Market Research, 2032, ALLIED MARKET RESEARCH, https://www.alliedmarketresearch.com/smart-contracts-market-A144098 (last visited Jan. 4, 2024).

reputational loss, increased smart contract costs, legal issues, and, in extreme cases, destruction of the smart contract.[13]

While no clear data exists to estimate how much smart contract attack vectors will limit the growth of the smart contract industry, the smart contracts industry is still estimated to grow to several billion dollars in the next decade—*despite* the cost of security audits and financial losses from bad actors exploiting smart contracts bugs. Estimates on financial loss attributable to security breaches and attach vectors of smart contracts range from hundreds of millions to billions of dollars. For example, between 2016 and 2018, seven cybersecurity incidents occurred in Ethereum smart contracts resulting in

---

[13] *See* David Balaban, *Navigating The Security Challenges Of Smart Contracts*, FORBES (Feb. 11, 2023, 6:33 AM), https://www.forbes.com/sites/davidbalaban/2023/02/11/navigating-the-security-challenges-of-smart-contracts/?sh=14006afd4992; Majd Soud, Grischa Liebel & Mohammad Hamdaqa, *PrAIoritize: Learning to Prioritize Smart Contract Bugs and Vulnerabilities* (Working Paper), https://arxiv.org/pdf/2308.11082.pdf; Sherman Lee, *Blockchain Smart Contracts: More Trouble Than They Are Worth?* FORBES (Jul 10, 2018,11:38 PM), https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-than-they-are-worth/?sh=74b5654523a6. Haozhe Zhou, Amin Milani Fard & Adetokunbo Makanju, *The State of Ethereum Smart Contracts Security*, 2 J. CYBERSECURITY & PRIV. 358 (2022); Hanting Chu et al., *A Survey on Smart Contract Vulnerabilities: Data Sources, Detection, and Repair*, 196 INFO. & SOFTWARE TECH. 1 (2023), https://www.sciencedirect.com/science/article/pii/S0950584923000757; MacKenzie Sigalos, *Bug Puts $162 Million up for Grabs, Says Founder of DeFi Platform Compound*, CNBC.com (Oct. 3, 2021, 2:41 PM), https://www.cnbc.com/2021/10/03/162-million-up-for-grabs-after-bug-in-defi-protocol-compound-.html; Tamer Abdelaziz & Aquinas Hobor, *Smart Learning to Find Dumb Contracts*, Proceedings of the 32nd USENIX Security Symposium 1775 (2023), https://www.usenix.org/system/files/usenixsecurity23-abdelaziz.pdf, Fabio Gritti et al., *Confusum Contractum: Confused Deputy Vulnerabilities in Ethereum Smart Contracts*, Proceedings of the 32nd USENIX Security Symposium 1793 (2023) https://www.usenix.org/system/files/usenixsecurity23-gritti.pdf. In one study, researchers found that 127 high-impact attacks were responsible for financial losses totaling $2.3 billion. Stefanos Chaliasos et al., *Smart Contract and DeFi Security: Insights from Tool Evaluations and Practitioner Surveys* (Working Paper), https://www.doc.ic.ac.uk/~livshits/papers/pdf/icse24.pdf.

financial losses of over $289 million.[14] In 2021 alone total financial loss from smart contract bugs was estimated at $680 million.[15] Some estimates put the current global financial loss due to smart contract vulnerabilities over 6 billion dollars.[16]

Solutions for Smart Contract Vulnerability

A diverse set of proposed solutions has emerged to address smart contract vulnerabilities issues and reduce the overall number of attacks. One potential solution is the use of a smart contract compiler.[17] For example, one such compiler is HCC, which automatically inserts security hardening checks at the source-code level.[18] HCC develops a code property graph (CPG) to model control-flows and data-flows of a given smart contract. Due to the CPG notation, HCC can be applied to various smart contract platforms and programming languages. HCC developers have demonstrated it efficiently mitigates reentrancy and integer bugs.[19] They also show how to integrate HCC within other blockchain platforms such as Hyperledger Fabric. Their

---

[14] Ayman Alkhalifah et al., *A Mechanism to Detect and Prevent Ethereum Blockchain Smart Contract Reentrancy Attacks*, 3 FRONTIERS IN COMPUT. SCI. 1 (2021), https://www.frontiersin.org/articles/10.3389/fcomp.2021.598780/full.

[15] Thomas Claburn, *Smart Contract Developers Not Really Focused on Security: Who Knew?*, THE REGISTER (Apr. 26, 2022), https://www.theregister.com/2022/04/26/smart_contract_losses/.

[16] Stefanos Chaliasos et al., *Smart Contract and DeFi Security: Insights from Tool Evaluations and Practitioner Surveys* (Working Paper), https://www.doc.ic.ac.uk/~livshits/papers/pdf/icse24.pdf.

[17] Jens-Rene Giesen et al., *Practical Mitigation of Smart Contract Bugs* (Working Paper), https://arxiv.org/pdf/2203.00364.pdf.

[18] *Id.*

[19] *Id.*

evaluation on 10k real-world contracts demonstrates that HCC is highly practical.[20]

Altering the methodology of bug classification and vulnerability analysis provides another promising approach. In one study, researchers propose two new vulnerability classes: distributed system protocol (DSP) and distributed system resource management (DRM).[21]

Community Audits

Community audits, or "bug bounties," have emerged as a popular tool to combat smart contract vulnerabilities. The premise is simple: pay hackers to demonstrate how existing code is exploitable. Alas, hackers often sell the bug or exploit them when they discover them.[22] Bug bounty programs also suffer from additional drawbacks: (1) they use a trusted intermediary that charges hefty commission fees and may have a conflict of interest with the software vendor, and (2) they may provide challenges for security researchers by compensating less than

---

[20] *Id.*

[21] Wesley Dingman et al., *Defects and Vulnerabilities in Smart Contracts, a Classification Using the NIST Bugs Framework*, 73 Int'l J. Networked & Distributed Computing 121 (2019), https://www.atlantis-press.com/journals/ijndc/125913574/view?ref=metastate.

[22] Ed Marcavage, Jake Mason & Chen Zhong, *Predicting the Effectiveness of Blockchain Bug Bounty Programs*,36 FLAIRS (2023), https://journals.flvc.org/FLAIRS/article/view/133377/137631.

guaranteed and may provide no means to appeal against it.[23] Web 3 technologies may help eliminate all of these problems.[24]

One potential solution to these problems is the Hydra Framework.[25] Hydra incentivizes bug disclosure through an exploit gap, a program transformation that enables runtime detection, and rewarding, of critical bugs.[26] The framework transforms programs via N-of-N-version programming, a variant of classical N-version programming that runs multiple independent program instances. *Id.* Testing with Hydra contracts demonstrated the power of bounties and established the first framework for rigorous economic evaluation of smart contract security. *Id.*

Another potential solution exists in Bounty Chain, a decentralized application using Ethereum-based Smart Contracts and the Interplanetary File System (IPFS), a distributed file storage system.[27] Blockchain and smart contracts provide a safe, secure and transparent platform for a bug bounty program. Testers can submit bug reports and organizations can accept or reject the defect via the smart contracts. Transactions on the

---

[23] Lital Badash et al., *Blockchain-based Bug Bounty Framework*, Proceedings of the 26th Annual ACM Symposium on Applied Computing 239 (2021), https://dl.acm.org/doi/pdf/10.1145/3412841.3441906.

[24] *Id.*

[25] Lorenz Breidenbach, Philip Daian, Florian Tramer & Ari Juels, *Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts*, Proceedings of the 27th USENIX Security Symposium 1335 (2018), https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-breidenbach.pdf.

[26] *Id.*

[27] Alex Hoffman et al., Bountychain: Toward Decentralizing a Bug Bounty Program with Blockchain and IPFS, 9 INT'L J. NETWORKED & DISTRIBUTED COMPUTING 86 (2021), https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=1255&context=compsci_fac_articles.

blockchain serve as a persistent and transparent record of software bugs. IPFS serves as a long-term storage system for bug details. Thus, Bounty Chain ensures organization accountability and allows testers to gain irrefutable recognition.

A last solution would be integrating bug bounty programs with improved threat modeling techniques through Metric-Based Feedback Methodology. When analyzing and categorizing vulnerability data, Metric-Based Feedback Methodologyfound enables identifying root causes and refines threat models to prioritize security efforts more effectively.[28]

AI-Driven Solutions

The integration of blockchain technology and AI has immense promise.[29] AI technology appears best suited to eliminating bugs through enhanced bug tracking and bug audits. A recent review of over 100 research papers revealed that integrating the two technologies results increases the security, efficiency, and productivity of the applications.[30]

---

[28] Serhan W. Bahar, *Advanced Security Threat Modelling for Blockchain-Based FinTech Applications* (Working Paper), https://arxiv.org/ftp/arxiv/papers/2304/2304.06725.pdf.

[29] Rashi Saxena, E. Gayathri & Lalitha Surya Kumari, *Semantic Analysis of Blockchain Intelligence with Proposed Agenda for Future Issues*, 14 Int'l J. Sys. Assurance Eng'g & Mgmt. 34 (2023), https://link.springer.com/article/10.1007/s13198-023-01862-y.

[30] *Id.*

Most bug tracking is done manually by software engineers, which impairs bug triaging.[31] To address this problem, researchers propose PrAIoritize; an automated approach for predicting smart contract bug priorities that assist software engineers in prioritizing highly urgent bug reports.[32]

Enhanced smart contract auditing can be accomplished through deep learning techniques. In a recent study, researchers trained three deep models for detecting vulnerabilities in smart contract: Optimized-CodeBERT, Optimized-LSTM, and Optimized-CNN.[33] Experimental results show that Optimized-CodeBERT model surpasses other methods, achieving an f1-score of 93.53%.[34] To precisely extract vulnerability features, they acquired segments of vulnerable code functions to retain critical vulnerability features. Using the CodeBERT pre-training model for data preprocessing, the authors could capture the syntax and semantics of the code more accurately. The authors evaluated its performance using the SolidiFI-benchmark dataset, which consists of 9369 vulnerable contracts injected with vulnerabilities from seven different types.

In another study, researchers trained artificial neural networks (ANN), long-short term memory (LSTM), and gated recurrent unit models (GRU) and compared their accuracy, precision, recall, and

---

[31] Majd Soud, Grischa Liebel & Mohammad Hamdaqa, *PrAIoritize: Learning to Prioritize Smart Contract Bugs and Vulnerabilities* (Working Paper), https://arxiv.org/pdf/2308.11082.pdf.

[32] Xueyan Tang, Yuying Du, Alan Lai, Ze Zhang & Lingzhi Shi, *Deep Learning-based Solution for Smart Contract Vulnerabilities Detection*, 13 Sci. Rep. 1 (2023), https://www.nature.com/articles/s41598-023-47219-0.

[33] *Id.*

[34] *Id.*

receiver operating characteristic (ROC) curve values.[35] The network was trained on an open Google BigQuery dataset with 7000 samples. Their results demonstrated that the LSTM model outperforms ANN and GRU.[36] Lastly, AI technology has the potential to generally improve smart contract security.[37]

Market for Code Reviews

The market for code reviews in 2024 is dominated by centralized market participants. The existing code review industry is subject to significant cost, inefficiencies, barriers to entry, and lack of assurances for code review job posters, among other lack of client services for code reviews. In 2024, the code review industry is dominated by several key players who can charge exorbitant and monopoly-like prices. Despite these high prices, the code review process is subject to significant flaws.

First and foremost, the selection process for the reviewer is an ongoing challenge for the existing code review process in legacy code review firms. The more hierarchical the code review process is, the lower is the quality of the reviewed code. It makes intuitive sense that the more developers review a given code set, the higher the code quality may turn out to be. However, in the legacy review process, the first reviewer within

---

[35] Rajesh Gupta et al., Deep Learning-based Malicious Smart Contract Detection Scheme for Internet of Things Environment, 97 COMPUT. & ELEC. ENG'G 1 (2022), https://www.sciencedirect.com/science/article/pii/S004579062100519X.

[36] *Id.*

[37] Moez Krichen, *Strengthening the Security of Smart Contracts through the Power of Artificial Intelligence*, 12 COMP. 107 (2023), https://www.mdpi.com/2073-431X/12/5/107.

the hierarchical structure of the code review process often gets the highest priority and is often merely followed with minor upgrades by follow-on reviewers. The collective of reviewers is also not incentivized to find flaws in the code to optimize code as a work product of the collective. Rather, it is often seen as the work product of the initial reviewer with minor input from follow-up reviewers. Moreover, the more people review the code with comments that ask for clarification, the more likely it becomes that the code becomes simpler and clearer, which in turn typically increases code quality. However, that is not possible in hierarchical review processes. The hierarchical approach to code reviews undermines long-term participation with opinions from the edges of the reviewer spectrum because those reviewers either have no access or are in no position to help review the code. In other words, the more hierarchical the code review process and the more barriers to entry, the lower the quality of the code.

Single Points of Failure

In the existing legacy code review process, the views of the reviewer and the intent of the code author are often at odds with each other without any crowd control. Because the code reviewer may wish to impose their logic on the code author, the code author may be required to rewrite code over and over even though the core functionality of the code is sound and dangerous issues were controlled for. This can be highly time-consuming and inefficient. It also calls the overall role of the code review process into question. Instead, a code review should focus on the functionality of the code and on keeping mistaken, badly constructed, and dangerous code out.

If the single author of a code review has missed something and the follow-on reviewer focused entirely on the first reviewer's concerns, the code review has a higher risk of lack of accuracy. Crowd wisdom is one way to correct possible myopia and single points of failure through standard legacy code review.

Timing

Depending on the setting of the code review, code reviews in legacy systems can last weeks and months. This can be exacerbated by market conditions in the digital asset market. These significant delays can impact development and may require complete rewriting of contracts because the underlying protocol may have upgraded core libraries during the code review.

Current Players in the Field

Even though most code review firms help clients who hope to decentralize different parts of the industry and capitalize on efficiencies created by decentralizing legacy systems, the code review industry is mainly dominated by a few players.

The current market dynamics dominated by the top 5 audit firms also create high barriers to entry for new players to enter into the code review market.

Given these downsides in the existing code review market, it is a bit ironic that one of the strongest forms of exploitation and centralized economies of scale are being created in a market that is, from the outset, supposed to help support the decentralization of disparate industries.

Overpricing

As a result of the centralization of the industry, most code reviews are significantly overpriced. Clients pretty much pay any price to get the stamp of approval from one of the top 5 audit firms.

No Controls

The centralized power also undermines attempts by other industry players to create internal or external controls on the quality of code reviews. As a result, the public has no or very weak control over the quality of code review services it receives. job posters cannot afford to look for better-priced code reviews and are forced into considerable pricing to obtain market acceptance of their products. In turn, the centralization of the market undermines any form of downward price pressure.

Because of the power of the limited players over the overall market and the process of the code review and its outputs, the quality of code review is often suboptimal.

Moreover, there is little or no recourse for clients in cases in which the code proved to be flawed even after functionality and quality review.

Code Review DAO

The CRDAO is tackling many of the issues that afflict the modern code review market.

The CRDAO provides a new code review platform, which facilitates a decentralized community-driven code review process that utilizes a bidding process on code reviews to drive prices down. It provides open access for code reviews from anyone who qualifies – not just members of the few code review firms. At the same time, it provides full incentivization for community code reviews through its decentralized governance framework.

Given its universal access and price discovery methodology (through a public bidding process), the CRDAO creates low barriers to entry in the code review market. Anyone can join the CRDAO by submitting high-quality code reviews through the CRDAO portal.

The CRDAO also uses a community policing and audit methodology for code reviews. This is enabled by the Code Review DAO[38] (CRDAO) governance model. Moreover, the CRDAO governance and policing functions ensure less duplication of code reviews. CRDAO maintains strong incentives for community-driven code review audits.

The CRDAO can function as a first-round code review or multi-round code review with different code review teams. In summary, job posters receive low-priced, high-quality code reviews with community validation of reviews.

Feedback Loops

[38] DAOs are short for Decentralized Autonomous Organizations. https://en.wikipedia.org/wiki/Decentralized_autonomous_organization#:~:text=Decentralized%20autonomous%20organizations%20are%20typified,dissemination%20of%20a%20distributed%20database.

CRDAO provides an early feedback loop on code reviews for the developer community at a much lower price than the traditional code review and audit market.

The CRDAO crowd controls filter out idiosyncratic code reviewer preferences. Code reviews in legacy code review firms are often highly subjective which leads to rather suboptimal outcomes without crowd controls. No single developer may agree on a given set of code and its intended functionality and quality in achieving the coded objectives. This can be attributed to different programming languages with different styles and unique and often idiosyncratic preferences. Instead, the CRDAO mandates that reviews are subject to crowd review and policing votes by the CRDAO collective. Accordingly, code reviewers are less likely to engage in highly idiosyncratic reviews as they would need to fear slashing and loss of standing in the community.

Price Discovery

The existing code review market does not provide publicly transparent pricing of code review services. As such, the existing market arguably harms the public for the benefit of the few market players and its clients. In the existing system, the unilateral pricing is not disclosed because both the client and code reviewer may not benefit from public scrutiny of the prices.

This price discovery mechanism serves a key public service function in that it enables full-price transparency for consumers based on the visibility of the internal and external

bids on job posts. This price transparency is unique and unprecedented in a market.

Price discovery is a key public services function because, without public pricing, consumers cannot realistically select the service provider that provides the highest value to the job poster. The lack of transparency enables insider deals to the detriment of the clients, who are forced into the price a group of firms dictates.

Standards

The CRDAO also fills the void left in legacy reviews without common standards. The CRDAO creates a compendium of reviews and through it a common standard for code reviews that are otherwise lacking in legacy code review environments. Should a collective review code under a common set of standards, the standards help guide both the reviewers and the collective to come to a common form of expectations on the applied functionality and quality outcomes for the code.

Speed

The feedback provided by the CRDAO for the developer community enables risk-taking for dev teams who wish to move quickly through their governance and upgrade process, which in turn enables accelerated growth and scaling of experimentation.

Code Testing

The code reviews provided by the CRDAO provide a first instantiation of flat hierarchy-driven decentralized peer-reviewed code reviews. All testing performed by the CRDAO follows the core standards established for the CRDAO community. All testing and standards are subject to constant review and experimentation and are continually, dynamically, and evolutionarily updated in a constant feedback loop between all constituents, that is between the CRDAO member, the job posters, and public bidders and applicants for CRDAO VA status.

Community Audit

The audit starts with the community discussion of the code review, followed by an informal vote on the code. The community that bids for the posted jobs and then reviews the submitted job and votes on it after the forum discussion is constituted by the evolving community membership of the Code Review Platform. The informal vote shows all CRDAO members the collective wisdom as applied to the work product examined in the code review. Once the entire community knows how each member feels about the code review examined, the CRDAO now votes in a formal vote in which the reputation tokens staked are at risk. This sequence of votes provides job posters with significant assurances that the code examined and the CRDAO report on the code adheres to the highest standards of quality available.

Moreover, the community of code reviewers is governed by a unique set of governance standards. Developers on the CRDAO Network can participate directly in the evolution of the CRDAO Network through participation in the CRDAO. The CRDAO follows a

decentralized framework of governance that was developed by Craig Calcaterra and Wulf Kaal.[39]

CRDAO Code Review Process

The code review process of the CRDAO revolves around CRDAO community engagement which minimizes issues of lack of crowd controls, lowers time requirements for code reviews, lowers prices of code reviews, increases developer participation, and increases overall feedback.

Scaling the Code Review DAO

Scaling the CRDAO operations is a key objective for CRA. The CRDAO uses several key reputation related metrics, as illustrated below, to scale its operations over time.

[39] Craig Calcaterra Wulf Kaal & Vlad Andrei, *Blockchain Infrastructure for Measuring Domain Specific Reputation in Autonomous Decentralized and Anonymous Systems* (U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-11, 2018), https://ssrn.com/abstract=3125822.

To enable the public to participate in and contribute to the Code Review Platform, the CRDAO is using a gamified reputation system. Any user can access and contribute to the CRDAO and earn reputation tokens and NFTs on the platform. While the code reviews themselves are relegated to the expert members of the Code Review Platform, the public can support the ultimate code reviews via gamified engagements.

Mechanical Turk (as defined below) functionality is a core application of the CRDAO Protocol and the CRDAO ecosystem. Other use cases and applications will evolve on the CRDAO over time. The CRDAO architecture will evolve in any setting that supports the ethical advancement of the crypto evolution.

Freelance Micro Task Market Growth

In the current freelancer market, leading centralized platforms Fiverr, Taskrabbit, Upwork, Crowdflower and Mechanical Turk have their workforces distributed throughout the world. Micro Tasks freelance work is becoming increasingly important in the freelance market.

Micro tasks are defined as small tasks that require human judgment, can be completed by humans independently over the internet, and are part of a larger unified project. Because of the necessity of human judgment that cannot currently be replaced by machines/computers, micro tasks enable organizations to build products or create outcomes that cannot be synthesized by machines/computers alone. For example, the Chinese government uses 2 million micro task workers to aid in censoring the internet. Internet companies, such as Google, Facebook, Twitter,

Ebay, and Linkedin optimize their production ready solutions and enhance their AI model training with micro task workers. Large scale distributions of machine learning researchers, among others, gather structured labeled data for artificial intelligence (AI) training purposes through the use of micro task workers.

Billions of micro tasks are completed each year and the demand for micro task workers is increasing consistently. In an attempt to capitalize on the growing demand for micro task work, Amazon created Amazon Mechanical Turk (MTurk) in 2005. MTurk is an online marketplace that allows requesters to pay workers for performing micro tasks online, thus crowdsourcing data collection. The World Bank concluded in a 2015 report, that the largest crowdsourced data collection platforms Amazon Mechanical Turk and CrowdFlower, a venture backed company that raised over $58 million and is focused on enriching data used for AI, would quadruple their revenue from 2013 to 2016.

The increasing demand for micro task workers that came initially from data scientists and other academics is further increased by the growth of artificial intelligence (AI) and the increasing scope and scale of AI applications in a broad range of industries. Fortune 500 tech companies including Amazon, Apple, Google Alphabet, Twitter, and Facebook use AI and machine learning to improve their services and cut costs, thus increasing profitability exponentially. According to some estimates, Fortune 500 tech companies spent between $20 and $30 billion on the development and enhancement of their AI systems in 2016. More recent data for 2017 suggests that this trend is continuing and increasing. AI is already playing a significant role in consumer expectations and tech companies have the best

possible set of incentives to keep investing in AI to fulfill such expectations and develop new products at marginal cost.

Shortcomings in Legacy Micro Task Market

The evolution, improvements, and growth of AI is correlated with the evolution, improvements, and growth in micro task work. AI uses supervised and unsupervised as well as reinforcement machine learning. Because unsupervised and reinforcement learning are much more complex than supervised learning, supervised learning is to date more common and more relied upon for AI development. While this may change as unsupervised and reinforcement learning evolve, currently, supervised learning depends on labeled data that is produced via micro task work. The mapping function of the supervised AI learning process necessitates the analysis of labeled input variables x and corresponding output variables y. In the supervised learning training phase, the AI neural network examines the training dataset of labeled x input data to learn to classify the input data idealistically. The higher the quality and quantity of such labeled datasets the better the AI neural network's learning algorithm during the supervised training process. Accordingly, the evolution, improvements, and growth of AI is correlated with the evolution, improvements, and growth in micro tasks work. But alas, microtasks platform systems are subject to significant limitations that inhibit the evolution of AI.

Lack of Scaling Solutions in Centralized Micro Task Market

Overpricing

The existing centralized marketplaces for micro task work cannot adequately fulfill the increasing demand for high quality micro task work for AI labeled training datasets. First and foremost, the cost structure for micro task work in centralized systems that necessitate intermediation results in significant overpricing without benefiting the micro task workers directly. The cost structure suboptimality can be traced back to several factors. All too human shortcomings of micro task works, such as limited attention span, irrationality, and inaccuracies result in verification requirements for micro task work. However, manual verification of micro task work is subject to the same human limitations.

Duplication of Work

In an attempt to ensure quality of results and minimize the impact of the human limitations of their workers, requesters in centralized micro task structures set up teams of up to 15 workers to perform the same task in an effort to form a consensus. The multiplication of work inherent in this process significantly increases the cost of micro task work. Requiring requesters to pay proportionally (e.g. up to 15 times) for work per project results in waste. The necessity of multiplication of work also subjects micro task workers to lower rates and lack of payment increases. Moreover, because unmanaged centralized micro task platforms do not supply consumer interfaces needed to accomplish specific tasks, requesters of micro task work are forced to either build their own tools or pay large fees to

startups that hope to capture the enterprise market. Both options are necessary in current centralized systems but also result in underutilization of resources.

No Access for Workers

Most importantly, the circa 38% of the labor pool that is unbanked but skilled does not currently have access to the centralized micro task marketplaces. Without a bank account, workers cannot contribute and profit from the existing centralized micro task marketplace. Furthermore, even for those in the labor pool who do have bank accounts, micro-task work is often associated with practical problems such as high fees of intermediary financial institutions, lost or otherwise affected payments, lost checks, among other issues. Finally, micro workers in centralized systems are faced with invasive, privacy challenging, time consuming, and unclear signup and approval processes that create market entry barriers for micro task workers.

CRDAO Micro Task Work

The CRDAO is tapping into this rising micro task market by providing users with gamified access to code reviews. Key examples that set precedent for the gamification include Axie Infinity and other scaling Ethereum games that attained worldwide audiences.

Through the gamification, the CRDAO is bringing 1000s of additional users to the platform. While the CRDAO has been in operation for over 3 years with over 300 jobs performed by an

expert code reviewer member group of the Code Review Platform, the platform through the proprietary CRDAO token token raise, is opening up the engagement to the public.

Public users can purchase proprietary CRDAO token tokens and use their proprietary CRDAO token to perform micro tasks on the Code Review Platform. Through the non-custodial staking of their proprietary CRDAO token , the public users become part of a larger community and gain reputation tokens. The more they engage with the Code Review Platform, the more their reputation will grow and the more proprietary CRDAO token tokens they can earn.

For example, micro tasks that are required for code reviews can include the creation of learning datasets that can be used by AI optimization tools in the Code Review Platform. With that definition of micro tasks, the public may earn reputation tokens simply by clicking on pictures provided by the Code Review Platform.

The public users who become part of the public proprietary CRDAO token community that earns reputation tokens will receive a proprietary CRDAO token allocation that is associated with the end product of the code review the public community participated in through their micro tasks. Through this mechanism, the public earns proprietary CRDAO token proportional to their engagement with the proprietary CRDAO token token and the Code Review Platform. The higher each public community members' reputation score, the higher their pro rata participation in the code review fees that are paid to the Code Review Platform.

The participation of the public proprietary CRDAO token community goes further with their ability to earn proprietary CRDAO token NFT badges. The CRDAO offers stages of public engagement measured for each user in their respective reputation tokens. Once the public user reaches a threshold of reputation score X, the respective user qualifies for the automatic acquisition of proprietary CRDAO token community NFTs. Such NFTs are for sale on OpenSea and are subject to market force pricing.

Benefits of Reputation in Micro Tasks

Using reputation systems, the CRDAO optimizes the existing Micro Task Market by: 1. Removing the cost of duplication of micro task work and thus scaling micro task work, 2. Minimizing transaction costs, 2. Optimizing payment systems in micro task work, and 3. Facilitating anonymity for enhanced worker participation and equity.

Removing Cost of Duplication

Centralized micro task work requires duplication to ensure quality. All too human shortcomings of micro task works, such as limited attention span, irrationality, and inaccuracies result in verification requirements for micro task work. However, manual verification of micro task work is subject to the same human limitations. In an attempt to ensure quality of results and minimize the impact of the human limitations of their workers, requesters in centralized micro task structures set up

teams of up to 15 workers to perform the same task in an effort to form a consensus.[40] The multiplication of work inherent in this process significantly increases the cost of micro task work. Requiring requesters to pay proportionally (e.g. up to 15 times) for work per project results in waste. The necessity of multiplication of work also subjects micro task workers to lower rates and lack of payment increases.

By contrast, in the CRDAO platform, the community organization software enables a readily available indicator of how reliable a worker or requester is on the CRDAO network. The micro task worker's reputation score is a measure of the worker's history of completing micro tasks on the CRDAO network qualitatively accurate, efficient, and consistent. The requester's reputation score is a measure of the requester's history of interacting with micro task workers on the CRDAO network. The CRDAO reputation score is formed and linked to the respective network participant's wallet address.

Market factors balance the equilibrium of supply and demand of micro work on the CRDAO Network based on the workers and requesters reputation scores. If requesters have a lower reputation score, workers become less likely to accept requesters' offers. In turn, low reputation scores for micro task workers result in a lower likelihood of retention for micro task work on the CRDAO Network. Requesters can select workers based on their reputation score, giving workers an incentive to keep the reputation scores high by performing micro tasks with

---

[40] Neeraj Kumar, *Effective Use of Amazon Mechanical Turk (MTurk); Tips and techniques for better usage of Amazon Mechanical Turk for researchers*, Neeraj Kumar (May 2013, updated May 8, 2014), http://neerajkumar.org/writings/mturk/; Rory O'Reilly, *How the Gems Protocol Reduces Consensus by Redundancy*, GEMS (Nov. 27, 2017), https://blog.gems.org/how-the-gems-protocol-reduces-consensus-by-redundancy- b151de80ecb8.

high accuracy and efficiency. The reputation score mechanism and the building of reputation on the CRDAO Platform allows workers to graduate to the privilege of being a verifier. The reputation score mechanism helps discern malicious actors and simple mistakes. It also protects workers and verifiers from fraudulent requesters and suboptimally designed requests.

In summary, the market factors and market dynamics related to CRDAO reputation scores enable a lowering of the cost of duplication as compared to centralized micro task work. If a reliable and high reputation score worker completes the tasks, the duplication may be brought from 15 to 5 or less in the decentralized CRDAO setup. This enables unprecedented scaling of micro task work.

Transaction Cost Minimization of Micro Task Work

The CRDAO removes transaction costs associated with micro task work. Unlike centralized mechanical turk platforms that require an existing banking relationship to receive account transfers for otherwise unbanked micro task workers, the CRDAO operates entirely through crypto transactions utilizing its reputation tokens and other cryptocurrencies. This enables unbanked workers to avoid opening a bank account to receive payments on centralized mechanical turk platforms, such as Crowdflower or MTurk. This, in turn, brings down transaction costs for mech turk workers on the CRDAO substantially, especially in comparison with micro task work in legacy and web2 markets. In addition, this creates loyalty to the Code Review Platform.

Optimizing Payment Systems in Micro Task Work

The CRDAO also improves the payment system for micro task workers in centralized mechanical turk platforms by orders of magnitude. Centralized mechanical turk platforms are subject to significant payment issues and payment timing for their workers. Workers are further burdened by high fees for intermediaries that facilitate the payment process such as Paypal. The fees in centralized mechanical turk platforms are only economically viable for higher volume workers who can at some point avoid the Paypal fees but create barriers to entry for new micro task workers.

The CRDAO not only allows workers to get paid in CRDAO proprietary CRDAO token tokens but also to capitalize on their growing reputation stakes within the platform. The CRDAO removes all non-CRDAO transaction fees for workers as only requesters post ETH or other cryptocurrencies to request micro-task completion. Holding and storing CRDAO proprietary tokens does not necessitate a banking relationship. All that is needed for a micro task worker to earn a living on the CRDAO is access to the Internet.

Anonymity Facilitates Equity

Workers in the centralized micro task economy are required to pass an approval process before they can start work. According to a study by the World Bank, centralized approval processes and identity requirements for mechanical turk worker registration creates significant limitations for the registration of new workers for micro task platforms. However, centralized micro

task platforms need to verify identity to prevent malicious actors from abusing the network and ensure work quality.

By contrast, on the Code Review Platform, users do not need to verify their identity to complete micro tasks. The CRDAO architecture, and specifically its reputation token staking mechanism, make the CRDAO attack resistant. This mechanism enables the CRDAO to circumvent all the issues that are associated with centralized identity verification processes. Accordingly, workers in the Platform are not required to expense money to qualify for centralized approval processes, don't experience delays, and are not required to surrender their private information. Given those benefits, the CRDAO enhances the labor pool of workers willing to provide micro tasks services.

The CRDAO is built to facilitate such worker disclosures via posts on the Forum. Alternatively, existing decentralized onboarding processes, via Bloom and Ocular, among others, allow the verification of worker identity information. The CRDAO integrates such verified identification information through posts on the Forum in the user interface.

Conclusion

The CRDAO provides key solutions for the existing problems of modern code reviews in a fully decentralized community-driven environment. As the CRDAO iterates on its design and moves

into subsequent phases, the larger web3 community will continue to benefit from the key innovations.