AUDITCHAIN

Decentralized Continuous Audit & Reporting Protocol Ecosystem™

AUDITCHAIN CORE CONTRACTS V1

AUDITCHAIN

Decentralized Continuous Audit & Reporting Protocol Ecosystem™

CONTENTS

Abstract

This whitepaper describes the design of an Ethereum based gamified incentive settlement and on-chain governance layer for actors in a decentralized continuous audit and real-time financial reporting protocol ecosystem for assurance and disclosure. It covers the functionality of Ethereum based core ERC20[1] and ERC721[2] factory smart contracts which enable an increase in assurance quality, auditor independence and objectivity, trustless settlement and the reduction of counterparty and regulatory risk.

Introduction

Traditional assurance methodology and periodic financial disclosure[3] underpin the traditional financial markets. Global disclosure frameworks address current information requirements for publicly traded enterprises whose financial transactions are concealed from public view and occur behind the firewalls of legacy accounting information systems and bank custody environments.

Traditional assurance and disclosure are not sufficient for issuers of digital assets and decentralized finance. Periodic reporting causes more confusion and results in less transparency for open public ledger based decentralized finance. Furthermore, the adoption of crypto assets by large, accelerated filers with the SEC is revealing material conflicts with periodic disclosure and assurance frameworks. Furthermore, the increased speed and volatility of the expansion and contraction of the typical business cycle is rendering periodic reporting and assurance and disclosure not useful or reliable.

Material changes in the financial state of decentralized networks and issuers of digital assets occur in real-time. The evidence of such changes is exposed to the public in real-time but lack the contemporaneous relevant explanation, context and disclosure from a regulatory perspective.

The core contracts[4] covered in this paper describe the functions of a standard ERC20 token contract ("AUDT"), an ERC20 cohort external validation factory contract ("EVC") and an ERC721 factory contract for ownership of curated controls over financial reporting. The core contracts are designed to function as a game theory incentive trustless settlement and governance layer in a decentralized virtual machine for accounting, audit, financial reporting and analysis.

Operating together, the EVC outputs a new contract address which binds an economic entity or a curator of control logic to an external validation agreement with a cohort of independent external validators when a minimum number of validators have accepted the requested engagement. On chain governance features allow the community of holders of AUDT to make proposals to change the minimum number of validators required to be bound in a single cohort for each category of assurance.

For financial state validation, the cohort begins performing validations of each financial state transition of an economic entity. In the case of a cohort engagement with a curator of control logic, the cohort validates that the control meets the specified functional objective pursuant to standards set under ISAE 3402[5] .

When a validation of the financial state of an economic entity is made by the cohort, it triggers a call to mint AUDT to the staked account of each validator in the cohort who attested to the financial state transition. The same process is achieved upon the validation of the functional objective of a control. The

[1] https://eips.ethereum.org/EIPS/eip-20
[2] https://eips.ethereum.org/EIPS/eip-721
[3] https://www.handbook.fca.org.uk/handbook/DTR/4/2.pdf
[4] https://github.com/Auditchain/Core-Smart-Contracts-v1
[5] https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

governing dynamics are designed to promote assurance levels on controls over financial reporting and financial disclosure for reporting entities that theoretically match the integrity of the methodology with which transactions are validated on a public blockchain[6].

Problem

Global regulatory guidance[7] [8] has suggested that certain open ledger based digital assets are securities and therefore subject to securities law compliance. Securities law compliance is significantly comprised of initial and ongoing financial and operational disclosure.

Regulation of digital assets is also occurring through enforcement[9] as opposed to legislation. The hostile approach to regulation is proving a critical need for an alternative yet compliant method of initial and ongoing disclosure for open ledger based digital assets.

A written independent audit opinion on the periodic financial and operational condition of an enterprise is the end result of a backward-looking independent statistical sampling[10] [11] of a fraction of data by a single accounting firm in order to independently determine if the financial and operational condition is fairly presented. In addition, internal control procedures as well as disclosure controls of larger enterprises are subject to cursory examination by the same auditor under a comprehensive independent audit engagement[12].

Auditors rely heavily on the representations of management of the enterprise and are paid directly by wire or by check by the enterprise itself. This is largely impractical for decentralized finance protocols and issuers of open ledger based digital assets. A traditional audit engagement is deficient in scope and methodology as well as cost prohibitive for development teams building and launching a base layer protocol, or a decentralized application.

Furthermore, direct payment by the enterprise to the auditor poses conflicts of interests that largely remain unresolved by regulators and the audit profession. The failure to timely settle audit engagement obligations jeopardizes the independence of the auditor. It is therefore necessary to reduce or eliminate the conflict of misaligned incentives by reallocating and *perfecting* assurance settlement obligations and deploying a plurality of auditors to eliminate as many points of failures as possible across the audit and reporting information supply chain.

Solution

Receiving payment for proof of work has been proven on the Bitcoin blockchain[13]. The core contracts provide a game theoretical layer 2 settlement and governance infrastructure built in Solidity that enables uninterruptable consensus based external validation of curated control logic, financial and operational state transition and disclosure for economic entities, issuers of open ledger based digital assets and decentralized finance protocols. The EVC addresses the problem of questionable auditor independence,

[6] https://bitcoin.org/bitcoin.pdf
[7] https://www.sec.gov/litigation/investreport/34-81207.pdf
[8] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/
[9] https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf
[10] https://ec.europa.eu/regional_policy/sources/docgener/informat/2014/guidance_sampling_method_en.pdf
[11] https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/au-c-00530.pdf
[12] https://www.icaew.com/-/media/corporate/files/members/regulations-standards-and-guidance/ethics/section-290-independence--audit--review-engagements-amendments-jan-2017.ashx?la=en
[13] The author keeps its own copy of Bitcoin: A Peer-to-Peer Electronic Cash System – Alternatively: https://bitcoin.org/bitcoin.pdf

substandard methodology, misaligned incentives, dislocated settlement obligations and data interruption across the audit and financial reporting information supply chain.

The core contracts described in this paper enable developers of assurance technology as well as curators of machine-readable control logic to contribute to the virtual machine and to provide validation of financial and operational state transitions in a decentralized continuous audit and reporting protocol pursuant to existing global standards and standards set by the DCARPE Alliance Association[14], (the "Alliance"). Standards will be adopted by a vote of a majority of Alliance members who currently play a role in the assurance, financial reporting, technology, standard setting and regulatory profession.

Functionality of EVC

The EVC enables economic entities and curators of machine-readable control logic to transmit a request for audit, ("RFA") to validators. Validators may respond to the RFA and accept its role as a validator in the validating cohort. A new contract address is outputted by the factory contract[15] when a minimum number of validators accept the RFA. Upon acceptance of the RFA, each of the validators in the cohort become bound and the new EVC contract address representing the engagement between the members is outputted.

Validators in the cohort begin validating output instances of the financial state transition of the economic entity. Validators also begin validating the effectiveness of a control developed by a curator and if the control meets the specified functional objective.

Each validator must make its own assessment of an output instance or a control and make its own attestation. The cohort of validators must achieve consensus on an attestation for a validation to occur. Each cohort is confined to a single category of assurance. This version allows up to six separate categories of assurance.

The EVC and the AUDT token contract act as the settlement layer for assurance obligations between the validators in each cohort and the enterprise when consensus is reached by the cohort. Consensus attestation represents Proof of Assurance and triggers the settlement and a call to mint AUDT to each of the attesting validators in the cohort. Payment is made to the attesting validators in the cohort following the achievement of consensus of at least 75% of attesting validators subject to on-chain governance.

Functionality of NFT Factory

The NFT Factory is an ERC721 contract that is designed as a digital rights management system for curators of machine-readable control logic that affect financial reporting. The controls play a role in automating accounting, audit, reporting and analysis processes in the virtual machine.

Curators of controls receive a NFT for each control they create. A "call to mint NFT to creator" function is triggered when a validation of a new control is completed. The NFT representing the control and all its metadata becomes available for the curator to claim.

The NFT enables the allocation of royalties between the curator and the validators, each time the control is used. Upon use, AUDT is paid by the user of the control to the curator and the validators.

[14] https://dcarpe.org
[15] https://uniswap.org/docs/v2/smart-contracts/factory

In addition to the digital rights management features, the new control contains proofs of the curation process and the validation process. Included in the NFT metadata is: name and wallet address of creator, name and wallet address of each validator and the cohort address of the cohort of validators who validated the control.

Auditors of financial statements rely on an economic entity's controls over financial reporting to help them gain confidence in the data. Under recent CEAOB guidance[16], machine readable, as well as human readable data and logic is now within the scope of an audit engagement for financial statement audit in Europe. The set of NFTs that represent all the controls over financial reporting for an economic entity can be presented as a knowledge graph with proof of assurance in the metadata to auditors who audit financial statements.

Staking and Settlement Function

Validators

A minimum of 5,000 AUDT and a maximum of 25,000 AUDT must be staked by each validator prior to being admitted to the Protocol and becoming eligible to respond to RFAs and participating in one or more Cohorts in one or more categories. The amount of the stake of a validator determines the proportion of each validation reward received by a validator.

Validators may participate in three initial separate categories of assurance:

1. Financial State
2. System and Organizational Control
3. Control Logic

Each cohort is dedicated to a category. A validator may participate in all three categories. Any one or more categories may be requested through separate RFAs by an enterprise. An attestation is made by each validator in the cohort. Each cohort must achieve consensus of a majority of attesting validators.

Enterprises

The enterprise must stake a balance of AUDT. The staked amount is determined by the community of actors on the Protocol. The staked balance is decremented for each attestation in accordance with the settlement algorithm illustrated below. See "Settlement Algorithm".

Data Subscribers

Data subscribers use AUDT to pay for deeper levels of financial data and audit analytics. The subscription cost by data subscribers is determined by the community of actors on the Protocol. Data subscribers must subscribe for each enterprise and its cohort of validators. The proceeds of all subscriptions are split between the enterprises, validators and Auditchain at a ratio determined by the community of actors on the Protocol. A record of data access by subscribers is retained and can be used as proof of reliance by the data subscriber on the enterprise data and audit attestation and validation data.

[16] https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/191128-ceaob-guidelines-auditors-involvement-financial-statements_en.pdf

Settlement Algorithm

The number of AUDT minted for each validation by a cohort is set through on-chain governance. The figure below illustrates which actor undertakes the liability for settlement of a validation and is based on attestation levels and abstentions. For the purposes of illustration, we assign a value of 1 to a payment.

Attestation Level	Reasonable	Adverse	Abstention
Enterprise	1	1	
Protocol	1	1	
Validator			2

A majority[17] of the validators in the cohort must achieve consensus on an attestation. Validators that attest receive their proportional share of the validation reward in proportion to the staked amount by the validator in the cohort. Validators that fail to attest forfeit their proportional share of the allocation and pay a penalty equal to the amount they would have otherwise received if an attestation was made.

Attestations by individual validators as well as the achievement of consensus are recorded as proof of assurance ("PoA") on the Auditchain Protocol. Final PoA by consensus triggers the validation and a call to mint AUDT to the attesting validators in the cohort and decrements the staked amount of the enterprise.

The proceeds of all payments made to all actors is credited to each of their respective staked accounts. AUDT is redeemable from the staked accounts at any time by enterprises and validators.

On Chain Governance

The core contracts feature on chain governance which allows changes to be made to the protocol[18]. Proposals may be made through the delegation of a minimum of 1% of the number of AUDT in circulation to a delegate. A holder of AUDT may delegate to themselves or to another delegate. The governance infrastructure featured in the core contracts is a fork of the Compound Protocol[19]

Member Contract

The governance functions for the engagements between reporting entities and validators allow the following changes:

- Changes to the amount of rewards paid to validators through inflation
- Changes to the amount of rewards matched by the reporting entity
- Changes to the reallocation of proceeds from data subscriptions between members of a cohort
- Changes to the minimum required deposit for continued compliance (fair warning)

[17] A minimum of three validators must be bound to the cohort. Two out of three must achieve consensus.
[18] https://github.com/Auditchain/Core-Smart-Contracts-v1/tree/main/contracts/Governance
[19] https://compound.finance/docs/governance#introduction

Cohort Factory

Governance allows changes to the minimum number of validators in a cohort for each category of assurance.

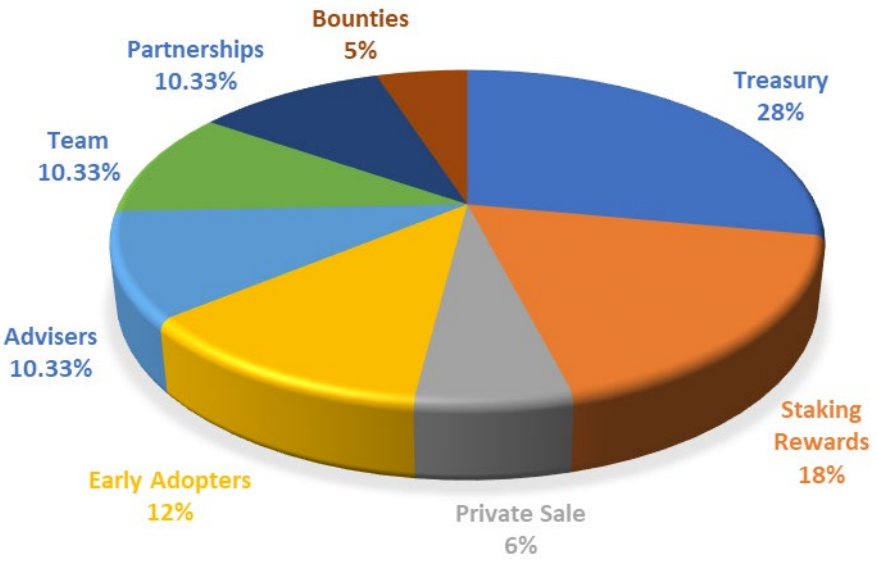
Cohort

Changes may be made to the percentage of validators in a cohort that are required for a validation to occur.

AUDT Token Generation Event

Initial Supply

The AUDT token contract begins with **ZERO** pre minted AUDT. The initial supply of AUDT minted will be triggered by claims of up to, (i) 15,000,000 minted to adopters in a private sale, (ii) 30,000,000 minted to early adopters, (ii) 70,000,000 minted and held in treasury, (iii) 45,000,000 minted in connection with staking (iv) up to 25,833,333 minted to the team, (v) up to 25,833,333 mintable to advisors, (vi) up to 25,833,334 mintable to partners and providers of applications and services and (v) 12,500,000 mintable in connection with bounties.



Subject to on-chain governance, the maximum number of additional AUDT tokens will be set by the community of AUDT holders through governance.

Value Proposition

We believe the Protocol has the potential to provide substantial benefits for the audit profession, issuers of digital assets, traditional enterprises as well as governments, non-profit organizations, investors and regulators.

Potential Benefits for the Audit Profession

- Substantial increase in efficiencies
- Higher confidence in audit trail data
- Higher reliability on audit evidence
- Substantial reduction in costs
- Reduced conflicts
- Higher independence
- Enhanced audit performance
- More effective internal oversight over audit quality
- Quantifiable audit cost analysis

Potential Benefits for Issuers of Securities and Digital Assets

- Higher likelihood of current financial information compliance for digital asset issuers.
- Greater access to capital.
- Higher valuation accuracy.
- Attractiveness to institutional investors.
- Substantial reduction in compliance and audit costs.
- Substantial reduction of the occurrence of fraud.
- Qualitative and Quantitative fraud detection and prevention.
- Substantial increase in effectiveness of internal controls.
- Substantial reduction of redundancies.
- Substantial reduction of error.
- Substantially higher operational efficiency.
- Promotes competitive advantage.

Potential Benefits for Investors in Securities and Digital Assets

- Immediate access to real time corporate performance.
- Substantially higher issuer and market compliance and transparency.
- Substantially lower instances of issuer accounting and financial statement fraud.
- Supports substantially higher levels of informed investment decisions.
- Substantial reduction in market dislocation.
- Promotes market correlation to corporate performance.
- Substantially higher levels of stability.
- Promotes higher levels of confidence.
- Promotes wholesale positive investor behavior.

Potential Benefits for Regulators and Taxpayers

- Permissioned access to real time issuer and exchange reporting data.
- Earlier detection of regulatory anomalies.
- Real time remediation.
- Real audit data analytics driven surveillance.
- Substantially higher issuer and market compliance.

- Automation of full and fair issuer and market disclosure framework.
- Substantial reduction in review with refocus on process.
- Reduction in operating and administration budgets.
- Substantial reduction in regulatory budget appropriation requests.
- Substantially higher agency performance quantification.
- Substantially higher levels of productivity.
- Substantial reduction in regulatory conflict.
- Substantially lower instances of issuer and accounting fraud.
- Substantially lower enforcement activity and costs.