



AUDITCHAIN

Decentralized Continuous Audit
& Reporting Protocol Ecosystem

WHITEPAPER
VERSION 1.0



Decentralized Continuous Audit & Reporting Protocol Ecosystem

CONTENTS

- Abstract3
- Problem.....3
- System and Organization Control Audit “SOC”4
- Solution5
- Token Sales.....5
- Decentralized Continuous Audit and Reporting Protocol Ecosystem “DCARPE™”6
- Technology Stack7
- Smart Contracts.....7
- Enterprise Initialization7
- Audit Committee Resolution7
- Digital Identity7
- Enterprise Implementation8
- Scoping Analysis8
- Testing.....8
- Certification9
- Transaction Lifecycle.....9
- Regulatory Compliance for Tokens10
- Regulatory Compliance and Use Case for Enterprise and Government10
- Decentralized Autonomous Organizations10
- Extensible Business Reporting Language “XBRL”11
- Utility and Description of AUDT Tokens & AUDT Fees11

AUDT Token Economy	11
Rights.....	11
Application and Service Providers	12
Staking Incentive for Nodes	12
Value Exchange	12
Mining Rewards	12
Utility Fees	12
Token Supply	13
Network and Consensus Governance	14
Federated Nodes	14
Non-Federated Nodes	14
Value Proposition	15
Value Proposition for Issuers of Securities and Tokens	15
Value Proposition for Investors	15
Value Proposition for Regulators and Tax Payers	16
Conclusion	16
Challenges and Considerations	17
DCARPE™ Alliance	19
Business Summary	19
References	20
Glossary of Terms	21

Abstract

A written audit opinion on the financial and operational condition of an enterprise is the end result of a backward looking independent analog and digital examination of the financial and operational condition of an enterprise as well as its internal reporting controls. Audits and preparation for such are costly and time consuming. As part of the audit process, a randomized selection of data is examined and estimated by the independent auditor pursuant to audit procedures to assess the fairness of reporting data, which is based in part on the representations of the management of the enterprise and subject to management's assessment of the adequacy and effectiveness of internal reporting controls. Current global regulatory disclosure frameworks make the presentation of financial statements untimely, highly conditional and subjective.

Using a distributed ledger smart contract network with a node layer that captures, and validates a straight through accounting treatment ("STAT") and reporting of enterprise transaction data along with a second node layer that independently and continuously audits and certifies every data block pursuant to SSAE 18(12) and IASE 3402(13) standards can theoretically substantiate the reduction of the time lag, conditionality and subjectivity of enterprise data reporting and financial statement presentation. This process would provide a substantial value proposition for issuers of tokens and securities as well as investors and regulators.

Such a process theoretically becomes the basis of a decentralized continuous audit and reporting protocol ecosystem ("DCARPE™") suitable as an infrastructure for networks of enterprises as well as constellations of other network ecosystems.

Problem

It has been estimated that theoretically, the larger, more complex and automated the enterprise, the higher the likelihood that anomalies are detectable using standardized independent audit assessments, as independently performed and will likely lead to the ability to arrive at a fair representation of system and data integrity. Anomalies provide clues that enable the detection of error and fraud. The substantiation of this theory is based on the relative reliability from a historical point of view of independent assessment using these and other "through the computer" standards and methods but its reliability is also dependent on the prevention of unauthorized console intervention⁽¹⁾. Additional audit practices suggest that the theoretically high probability that volume, repetition and uniformity of accounting and ERP systems data is sufficiently deterministic in order to arrive at a reliable independent conclusion⁽²⁾. Such conclusion is an opinion and is based in part on written representation by management of the enterprise that are further conditional upon and subject to management's internal evaluation of internal reporting and disclosure controls.

To the extent that tighter regulations such as the adoption of Sarbanes-Oxley⁽⁴⁾ have increased audit scrutiny and the likelihood of audit liability is the extent that auditors have been able to, in subtle manner, relinquish "ownership" liability of certain work product reports and process performance back to enterprise management on the basis that auditor ownership of such would jeopardize independence but this is a subjective approach, not a statutory prohibition. The deferral is conditional in part upon the level of malpractice insurance carried by the auditor and also the confidence of the level of capabilities the auditor possesses. The deferral also poses a risk of defeating the purpose of independent audit exercise and review yet it is, in practice, frequent and acceptable.

In order for an audit conclusion to be reached by the auditor and for a final comprehensive audit report to be issued, management of the enterprise must first perform its own evaluation of internal controls over financial reporting based on standards set by the **Committee of Sponsoring Organizations of the Treadway Commission**. Management must represent, not prove, that reporting controls are sufficient and effective and that such an evaluation was performed. Management also needs to share their assessment with the auditor which must include a list of all material weaknesses and deficiencies identified in the assessment.

The written conclusion of a typical comprehensive audit provides a statement by the auditor which includes opinions on evidence of fair representations, not statements of accuracy. For example; the following statement concludes the report of independent registered public accounting firm PwC dated February 22, 2017 which is included as page 64 in the annual report of Exxon Mobil Corporation for the period ending December 31, 2016; "Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate".⁽³⁾

This is an ominous warning and illustrates the potential deficiencies of both internal audit process and independent audit process. There are clearly no assurances that material misstatements will be detected by the enterprise nor is there an assurance that they will be detected by the auditor. Our coverage of these subjects illustrates the highly subjective and conditional disposition of conventional accounting, audit, reporting and disclosure standards.

Financial markets rely heavily on the expertise of the human performance of these independent review and audit processes in order to establish trust that the results of such work will disclose, in a timely manner, an accurate representation of financial assets. Furthermore, the Securities Act of 1934⁽⁹⁾ as well as most international securities laws require the review, audit and disclosure of the operational and financial condition of such assets.

Regulatory framework only requires the enterprise or asset to provide full and fair disclosure and take **reasonable steps** to assure the detection and prevention of error and fraud. As evidenced by countless instances of fraud and the restatement of filings by publicly traded enterprises, no existing accounting, audit or regulatory system mechanically **perfects** the detection and prevention of error and/or fraud in a trustless manner.

System and Organization Control Audit "SOC"

Service organizations such as banks, financial services firms and data centers rely heavily on highly complex technology environments to capture and process data. Service organizations submit to service organization control "SOC"⁽¹²⁾ under standards set by SSAE 18⁽¹²⁾ in the US and IASE 3402⁽¹³⁾ outside the US. Reports are issued as the result of the engagement of the services of highly specialized auditors separate from financial auditors to assess the effectiveness of system controls.

SOC audits include two "Types"; In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives.

In a Type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable **but not absolute assurance** that the control objectives were achieved during the period specified.

SOC audit reports are performed and issued usually once per year. The rapidly changing and evolving networked environments of 21st century business give rise to the theory that conventional standards, methods and frequency of SOC certification are not sufficient. The capabilities under the required frequency of conventional SOC standards to assess systems have not kept the pace of the current and evolving speed of network commerce⁽⁹⁾.

What constitutes a material event is often the culmination of a series of naturally occurring non-material events and/or actions taken by management⁽⁸⁾. The time lag of conventional disclosure and reporting standards has become an opportunity for Auditchain when taking into account the evolving time compression of the occurrence of material financial and operational changes and events.

Solution

Auditchain proposes to embody an ecosystem that includes a blockchain protocol and an open source library of accounting smart contracts sufficient to capture, process, audit and report enterprise data and performance data on a real time continuous basis under a continuous independent audit exceeding current accounting, audit and control standards. A public facing and/or permission based presentation layer proposes to render in real time, at the close of every block; balance sheet, income statement, cash flow and statement of changes in stockholders' equity reports that has the capacity to far exceed the reliability of existing reporting standards.

Token Sales

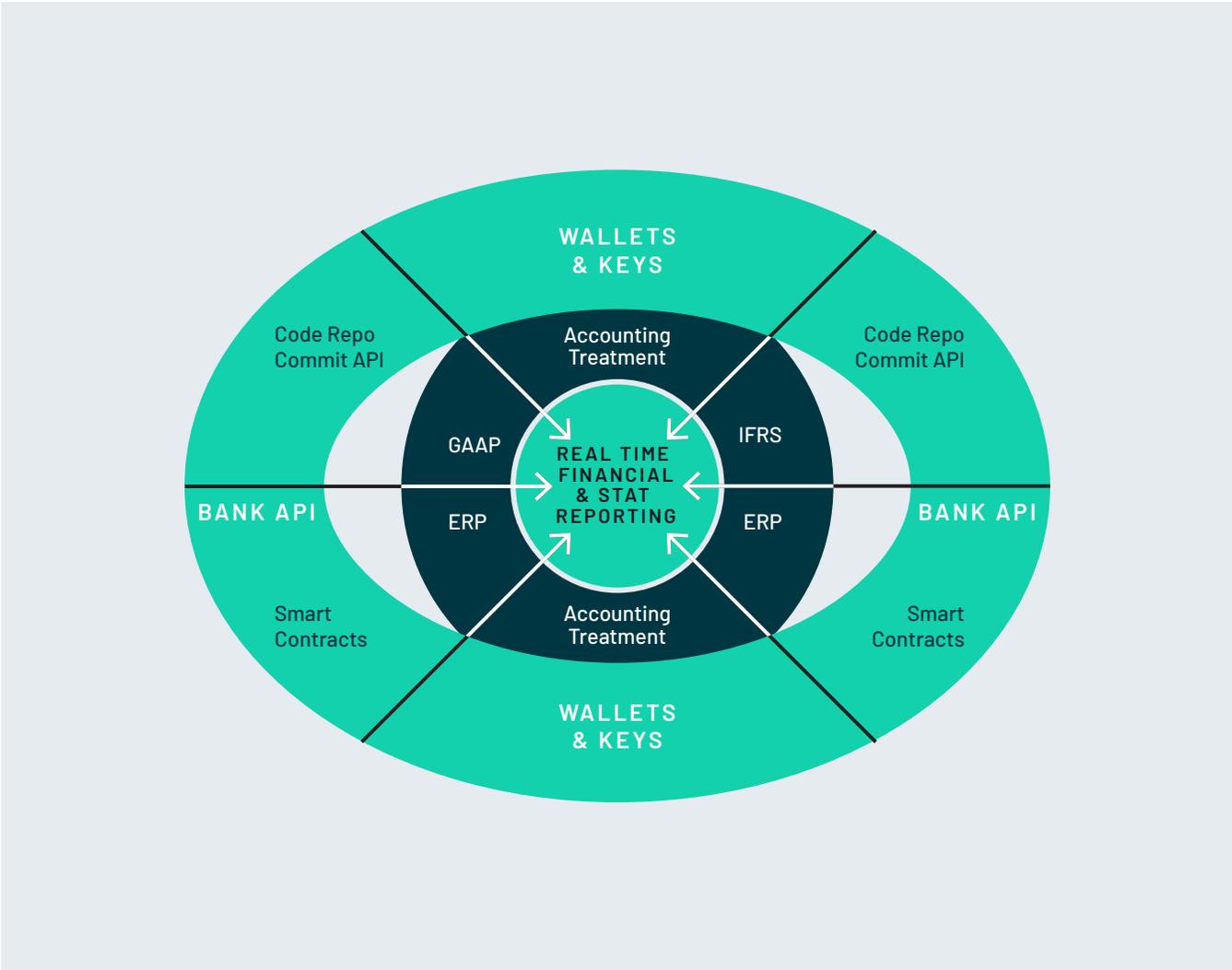
For token sales, code repository integration as well as network integration will make it possible for real time reporting of development statistics and network statistics for ongoing performance reporting and disclosure for token sales and token utility, respectively.

Decentralized Continuous Audit and Reporting Protocol Ecosystem “DCARPE™”

Self-auditing state of a distributed ledger and the validation of transactions first occurred on January 4, 2009 with the launch of the genesis block of the Bitcoin blockchain⁽⁵⁾.

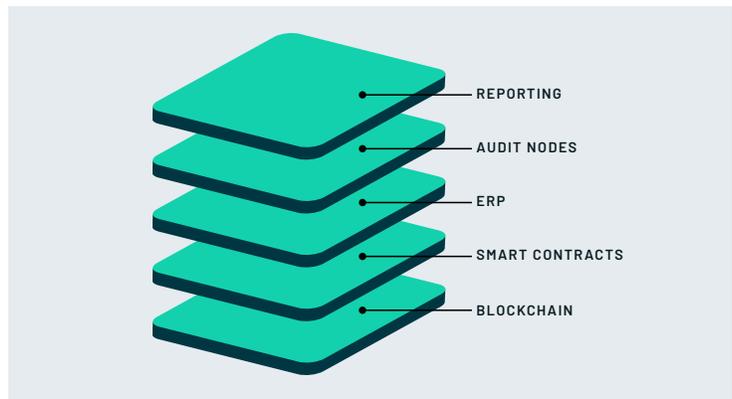
Continuous audit is evolving in theory and practice. Its practice is limited mainly to internal reporting controls. The application of jurisdictionally compliant accounting treatment to transactions and reporting system risk controls occurring in most business processes is now theoretically possible concurrently within and subject to a decentralized continuous audit environment pursuant to SSAE 18⁽¹²⁾ and IASE 3402 standards through the use of configurable “Ricardian” type smart contracts⁽⁶⁾⁽⁷⁾. Such contracts, as proposed in this paper, do not hold custody of value but instead execute commands for how legal conditions and value are treated based on a fixed or evolving arrangement.

DCARPE™ implementation leverages the self-auditing state of a blockchain with these additional layers of high extensibility specifically for the development and deployment of decentralized enterprise applications designed to offer stakeholders with real time presentation of financial, operational, development and network statistics reporting **every block**.



Technology Stack

Auditchain supports a full stack which includes the base protocol layer, GAAP, IFRS and GAAS smart contract layer, application layer, audit node layer and real time (per block) public facing or permission based financial statement, audit analytics and statistical reporting presentation layer.



Smart Contracts

An open source library of smart contracts will be developed containing an implementation of a variety of GAAP, IFRS and Government Accounting and Audit Standard “GAAS” accounting treatment protocol and jurisdictional tax treatment protocol for all enterprise transactions.

Earlier stage and venture backed enterprises spend a high percentage of accounting resources on equity compensation and convertible instruments. A priority will be placed on the development of a sample of FAS 123R (FASB ASC Topic 718)⁽¹⁹⁾ accounting treatment contracts associated with equity based compensation plans. In addition, convertible debt accounting treatment contracts under FASB ASC Topic 470⁽²⁰⁾ will also be considered a priority for development.

Enterprise Initialization

Audit Committee Resolution

The audit committee of the board of directors of the enterprise designates the individual responsible for oversight of all systems and controls proposed to be implemented and deployed on the Auditchain network. The designee is responsible for the initiation process.

The designation of the designee is formalized through the entry into a simple smart contract which serves as the resolution of the audit committee. The resolution designates the access level to the designee(s). Initialization of membership on the network cannot proceed until the audit committee resolution is submitted, confirmed and validated by the network. All votes of the members of the audit committee are recorded and the resolutions are legally bound and Auditchain membership has been initialized. Upon initiation, an initial collateral of AUDT tokens are staked. AUDT fees are deducted from the collateral stake in connection with the confirmation and validation of the resolution of the audit committee and paid to all validating nodes.

Digital Identity

Upon validation of the resolution of the audit committee, the designee assigns digital identities to the enterprise itself as well as additional enterprise designees. Each identity contains detailed personal information of the user. Each identity is assigned an access level designating the nature and level of permission to access the enterprise profile on the Auditchain network.

The assignment of each identity and its designated access level are confirmed and validated by the Auditchain network. AUDT fees are deducted from the collateral stake and paid to validating nodes in connection with each identity validation and the designation of access level for each identity.

Upon deployment, a complete map of the enterprise implementation is associated with the enterprise digital identity. Private keys associated with the enterprise digital identity relate to all enterprise related hashes on the Auditchain base layer.

Digital identities are required for all users on the Auditchain network. All users must pay AUDT fees for the creation and validation of all digital identities.

User types include:

- Federated Nodes
- Non-Federated Nodes
- Service Providers
- Enterprises
- Enterprise Designated Users

Enterprise Implementation

Initialization is complete upon validation of (i) the resolution of the audit committee containing the designated administrator(s), (ii) the validation of all enterprise users and (iii) validation of all digital identities.

Scoping Analysis

A scope of the prospective implementation may now be conducted by a sufficiently skilled designee(s) of the enterprise. A profile of the enterprise is created and staged by the user in the Auditchain UI. The profile contains a detailed list of all customers, vendors, employees, bank accounts and cryptocurrency wallet information. For dApp and network development projects, code repositories are also included in the enterprise profile. The completed profile becomes associated with, and supplements the digital identity of the enterprise.

A selection of Open Source standardized smart contracts (such as GAAP, IFRS, GAAS, etc.) and services (such as accounting, payroll or human resources software) available through the UI are made by the enterprise user based on the size and complexity of the enterprise and its accounting and tax treatment election for all transactions. Input data is imported and/or implemented into each contract based on the pre-existence of contract and accounting data. The final selection of accounting treatment contracts, services and proposed implementation is mapped and submitted to the network in a test environment.

Testing

The operational objective of the proposed implementation is tested to verify its functionality. AUDT fees are deducted from the collateral stake in connection with testing and paid to validating nodes.

During testing, an evaluation of controls by Federated Nodes will determine the operational objective of the implementation and whether the controls are suitably designed to achieve the specified objectives. Upon confirmation and validation, the implementation, as proposed, is certified by Federated Nodes. A deduction of AUDT fees is made from the AUDT collateral stake in connection with the SOC certification and paid to Federated Nodes.

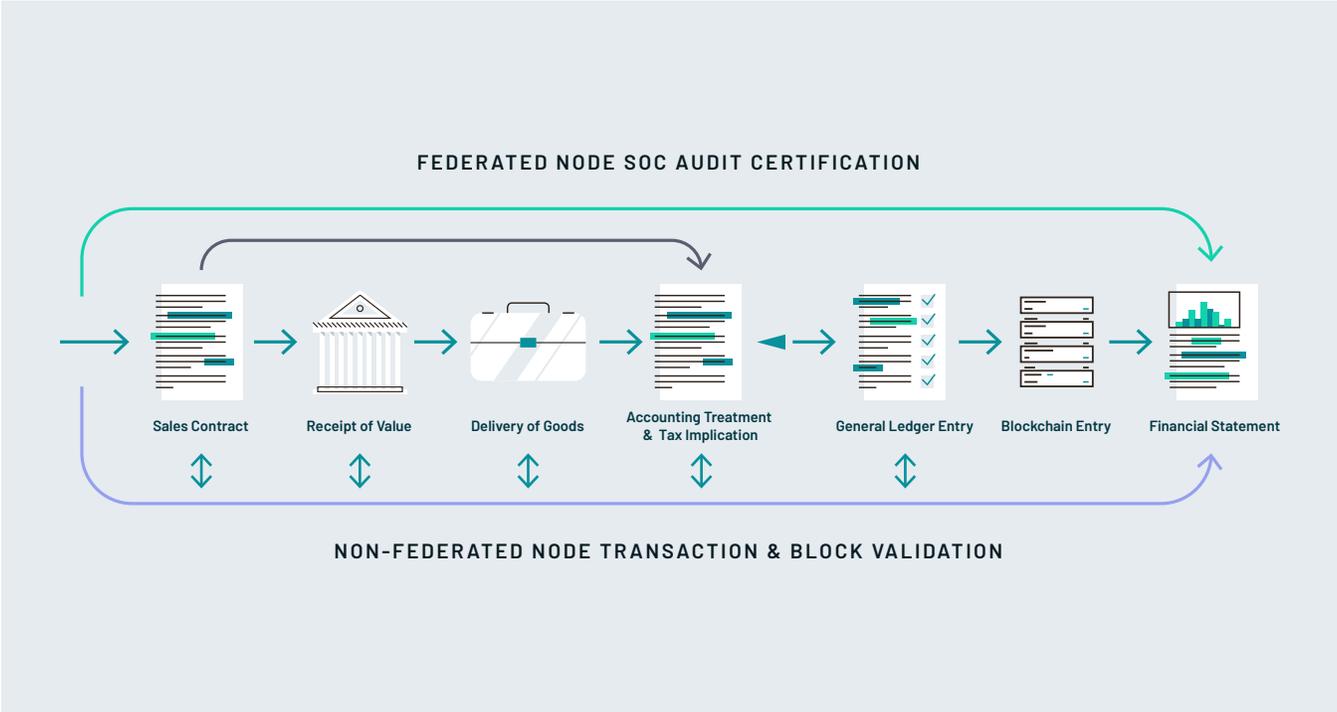
Certification

Upon successful testing, the implementation is submitted as a live deployment proposal to the Auditchain network. The proposed implementation is confirmed and validated by Non-Federated Nodes and SOC certification of the deployment is made by Federated Nodes. The final state of the implementation at deployment supplements the digital identity of the enterprise. AUDT fees are deducted from the collateral stake and paid to validating nodes in connection with the validation of the deployment. Additional AUDT fees are deducted from the collateral stake in connection with SOC certification and paid to all Federated Nodes.

As new transaction types and additional services are contemplated by the enterprise as the result of expansion, new services and/or smart contracts from the library are selected, configured, installed, tested, certified and deployed. AUDT fees are deducted from the collateral stake in connection with the expansion deployment and paid to validating nodes.

Transaction Lifecycle

Public facing and/or permission based financial statements are impacted by every enterprise transaction and are validated with straight through accounting treatment (STAT) resulting in books and records that are considered as audited in real time.



Every business contract and transaction is processed through the appropriate accounting treatment contract and written to the general ledger. Additionally, each transaction as well as accounting and tax treatment data is hashed and timestamped as the third entry to the blockchain. The total STAT impact of every transaction is applied and pushed out to the P & L, balance sheet, cash flow and statement of changes in stockholder equity.

Regulatory Compliance for Tokens

Pursuant to the investigative report of the Securities Exchange Commission dated July 25, 2017⁽⁹⁾ and assuming that token sales conducted in and from the US are in compliance with the Securities Act of 1933⁽¹⁰⁾, APIs for network statistics and development statistics for tokens are being proposed for the purposes of heightened levels of compliance with current information requirements of the Securities Exchange Act of 1934⁽¹¹⁾ and their extraterritorial equivalent.

It should be noted that the definition of current information for cryptographic tokens was not clarified by the SEC in its July 25, 2017 report. DCARPE™ proposes to deal with this challenge to help standardize what constitutes current information for dApp tokens considering the fact that dApp tokens lack financial statements.

DCARPE™ proposes to support real time reporting of current information for tokens which we believe includes dApp development statistics prior to network launch and network statistics post launch. Voluntary disclosure of these statistics by those engaged in ICOs may ease regulatory pressure when “resales” occur of tokens after their initial purchase.

Regulatory Compliance and Use Case for Enterprise and Government

Publicly traded enterprises rely on centralized accounting, internal audit and reporting data processing systems to manage, measure and report the throughput of performance. Quarterly and annual reports are compiled and required to be filed with the Securities Exchange Commission. Additionally, audits are also required to be performed for many types of enterprises including governments.

Auditchain proposes to automate and decentralize accounting, audit and reporting throughput while substantially reducing the cost of compliance for:

- Public Companies
- Venture Backed Private Companies
- Private Equity Backed Private Companies
- Investment Funds
- Not for Profit Foundations
- Provincial, Local, State and Federal Governments

Decentralized Autonomous Organizations

There exists a belief that over time, the security design of decentralized autonomous organizations⁽¹⁷⁾ will reduce the attack surface and will lead to feasible deployment. Theoretically, in order to support business processes and the interoperability of micro services within constellations of DAOs, the infrastructure of decentralized continuous audit and reporting protocol, as proposed herein must be implemented as a part of their foundational design in order for its ecosystem to effectively function and evolve.

Extensible Business Reporting Language “XBRL”

The use of XBRL⁽¹⁸⁾ has been required and universally applied to all financial statements and reports filed with the SEC since 2009. Its utility has also been significantly expanded to include a wide variety of compliance reporting.

Auditchain will include an implantation of an XBRL layer for enterprise internal reporting and compliance **and** as a tool for research and analytics. The implementation will allow researchers and stakeholders the added benefit of configuring financial statement data in a manner that allows the automated production of proprietary and thesis based reports.

Immutability under real-time SOC certification combined with real-time presentation of financial statement, development and network statistics reports when combined with the implementation of XBRL will enable reliability and insights into enterprise, development and network performance on a dynamic basis in a manner not previously possible.

Utility and Description of AUDT Tokens & AUDT Fees

AUDT is the base currency or “utility tokens” that are used by users to access and pay for the services of the Auditchain Network. AUDT are ERC20 compliant and will be distributed pursuant to a token generation event (“TGE”) to early adopters of the Auditchain network. See “Terms of Token Generation Event “TGE”.

AUDT Fees are Auditchain Network based units of value and are pegged to the local currency of each respective jurisdiction. Transactions on the Auditchain Network are paid for using AUDT Fees which are deducted from the staked account.

Upon the launch of the Auditchain network, the AUDT ERC20 tokens held by holders will be exchanged for native Auditchain network AUDT tokens and migrated onto the network.

AUDT Token Economy

Subject to protocol adjustments and improvements, AUDT tokens will be purchased staked by each enterprise. AUDT is used by each enterprise to join Auditchain. AUDT is deducted from the stake account of each enterprise to pay for implementation, smart contract deployment, transaction validation, continuous audit and enterprise expansion.

Rights

Holders of AUDT will have rights to access and use the services of the Auditchain network. AUDT will also be used to associate with a digital identity application which will identify each enterprise user and each Federated Node operator. AUDT will not bear any voting rights or any rights to current or future equity in Auditchain or the network.

Application and Service Providers

Any user may develop and/or provide a service to the Auditchain network for consumption by other users. The developer or provider of any such service or application must pay AUDT Fees for network certification, installation, testing, validation and SOC certification of such service or application using AUDT. Upon launch of the service or application, users will pay AUDT to the developer for the use of the service or application and the developer will earn AUDT. In addition, transaction fees associated with the use of the service or application are earned by nodes on the network for providing the computational power to complete the transactions provided by the service or application.

Staking Incentive for Nodes

Federated and Non-Federated nodes are required to purchase and stake AUDT. A collateral stake is posted by every node to a secure multi-signature wallet to insure uninterrupted services are provided to the Auditchain network by each node. Any node that ceases to provide service to the network will be penalized through the deduction of AUDT from their staked account. Deductions will be determined by the level of service and length of time service is not provided by the node. Additionally, deductions are made from the staked account for non-compliance with network and service protocol.

Value Exchange

AUDT is the unit of value exchange in the Auditchain network. AUDT is the creator and driver of the transactional economy of the Auditchain network and the services provided.

Similar to gas on the Ethereum Network, AUDT Fees are the Auditchain Network atomic unit of value determined by the network for the payment of fees for transactions, computations and certification. AUDT Fees, unlike Ethereum gas are valued in local currencies. In one example; subject to network conditions and priority USD \$.0001 worth of AUDT may be paid to the validating Non-Federated node for a single transaction in the US.

Mining Rewards

Auditchain is secured through a Proof of Work (PoW) Proof of Stake (PoS) consensus mechanism. Auditchain mining rewards will be allocated as follows: 42.5% of the block reward goes to Non-Federated nodes (PoW miners), 42.5% go to Federated nodes (PoS miners) and 15% is allocated to Auditchain and its affiliate for continued development of the network and education of the Auditchain community.

Utility Fees

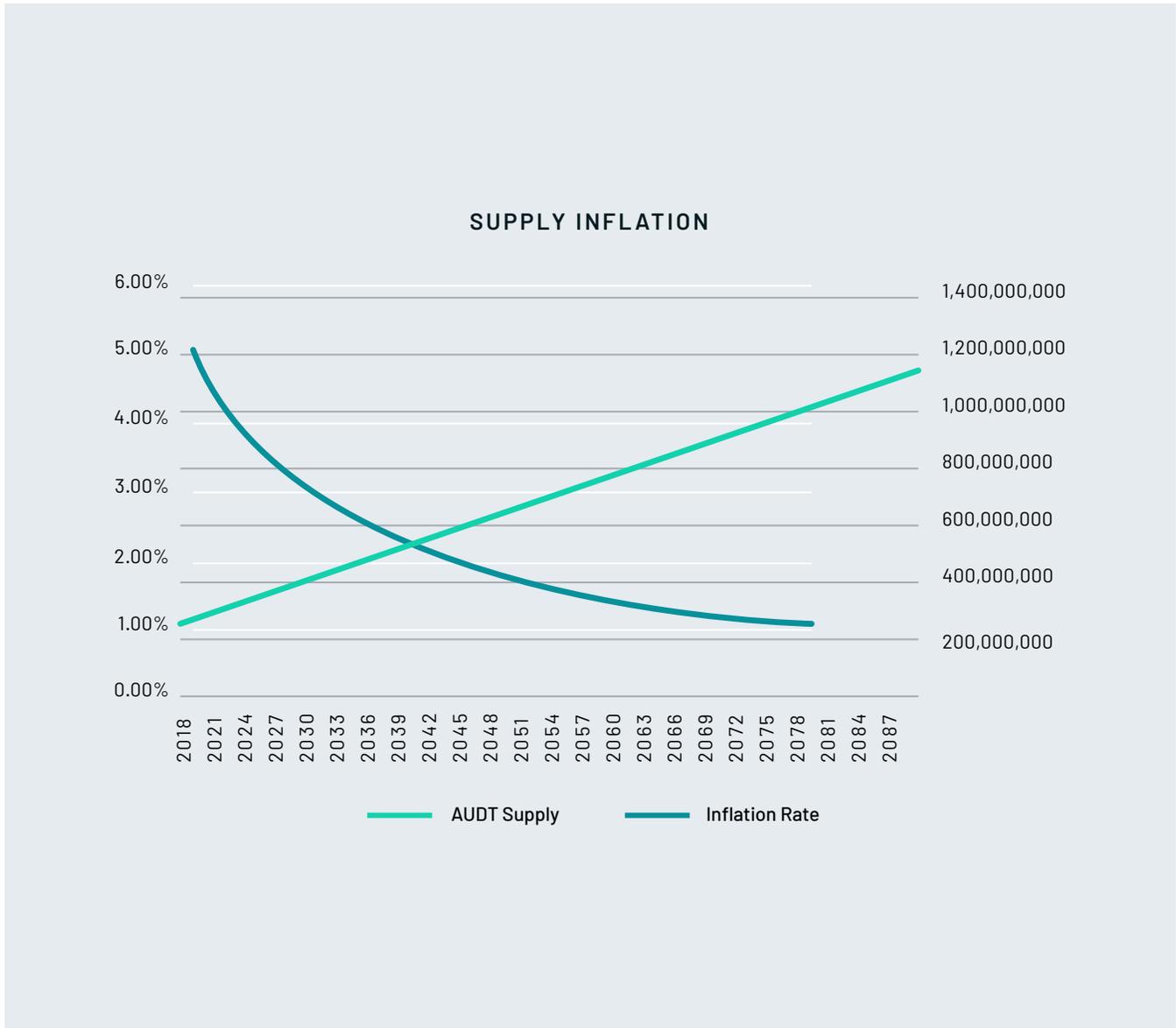
AUDT is paid by enterprise users to all nodes for the computation of transactions effected by the enterprise on the network. A priority fee is added to the cost paid by the enterprise for transactions requiring a higher priority.

Token Supply

The total supply of AUDT at the genesis block will be 250,000,000 which includes (i) 160,000,000 to be sold in the TGE, (ii) 25,833,333 to be distributed to the team, (iii) 25,833,333 reserved and distributable to advisors, (iv) 25,833,333 reserved and distributable to partners and providers of applications and services to the Auditchain network and (v) 12,500,000 reserved and distributable in connection with bounties. See "Token Allocation".

In addition to the initial AUDT token supply and subject to block times, consensus proposals and improvements, approximately 12,500,000 additional AUDT tokens will be rewarded to all Federated and Non-Federated nodes per year which amounts to approximately 237 AUDT tokens per block.

Below is a chart of the inflation curve which results in the debasement of the initial supply of 250,000,000 AUDT at the initial rate of 5% per annum which is disinflationary.



Network and Consensus Governance

Two types of nodes will govern and enforce the network protocol. The governance system is similar to other protocols⁽¹³⁾ using this structure. Each node type will be required to run a dedicated server and be required to exclusively run the latest version of DCARPE™ software within a data center certified under SSAE 18⁽¹²⁾ standards in the US and ISAE 3402 standards outside the US.

Federated Nodes

Federated nodes are deployed and operated by qualified SOC auditors and members of the **Public Company Accounting Oversight Board** "PCAOB" in the United States and the **International Auditing and Assurance Standards Board** "IAASB" outside the United States. Each federated node operator must be certified in each of their respective jurisdictions to conduct SOC audits pursuant SSAE 18⁽¹²⁾ and ISAE 3402⁽¹³⁾ standards.

Federated nodes are full nodes and must provide a minimum level of service to the network and stake AUDT as collateral to participate. Conditional upon regulatory clearance or an exemption therefrom, Federated nodes will earn AUDT fees while providing the following services which we believe exceed standards under SSAE 18⁽¹²⁾ and ISAE 3402⁽¹³⁾;

1. Continuous audit of the state of the network as a whole.
2. Continuous audit of the state of all deployed smart contracts on the network.
3. Continuous audit of non-federated node activity and behavior.
4. Continuous audit of network enforcement by non-federated nodes.
5. Certification of original installation, state and expansion of each user.
6. Supervision and enforcement of new regulatory implementations
7. Continuous certification of network, node and user state.

Federated nodes provide the above services on the network and in return are paid additional AUDT. Subject to network consensus, Federated nodes are paid 42.5% of all block rewards.

Non-Federated Nodes

Non-Federated nodes will be admitted to operate nodes and mine AUDT. Non-Federated nodes must also provide a minimum level of service to the network and stake AUDT as collateral to participate. Non-Federated nodes will include, but will not be limited to, members of the accounting, investment and financial reporting community. Conditional upon regulatory clearance or an exemption therefrom, enterprise users may also be admitted to deploy and operate nodes which may offset the costs of network service usage.

Non-Federated nodes shall earn AUDT tokens through mining and perform the following services under strict SSAE 18⁽¹²⁾ and ISAE 3402⁽¹³⁾ standards;

1. Monitoring and validation of all transactions.
2. Monitoring and validation of all blocks.
3. Monitoring and validation of the state of all smart contracts.
4. Monitoring and validation of all user installation and expansion.
5. Notification of user non-compliance.
6. Supervision and validation of remediation.
7. Enforcement of consensus.

Non-Federated nodes provide the above services to the network and in return are paid AUDT. Non-Federated nodes are paid 42.5% of all block rewards.

Block rewards will vary according to the current total count of active nodes on the network. Daily payments are calculated pursuant to the following formula:

$$(n/t) * r * b * a$$

Whereby;

- n is the number of nodes an operator controls.
- t is the total number of nodes.
- r is the block reward
- b is number of blocks in an average day.
- a is the average node payment (85% of the average block amount)

Value Proposition

Value Proposition for Issuers of Securities and Tokens

- Higher likelihood of SEC "current information" compliance for tokens.
- Greater access to capital.
- Accurate valuation.
- Attractiveness to investors.
- Substantial reduction in compliance and audit costs.
- Substantial reduction in the possibility 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.
- Cost offset through node deployment and mining.

Value Proposition for Investors

- Immediate access to real time development and network statistics for tokens.
- Immediate access to real time corporate performance.
- Substantially higher issuer and market compliance and transparency.
- Substantially lower instances of issuer and accounting fraud.
- Highly informed investment decisions.
- Substantial reduction in market dislocation.
- Market correlation to corporate performance.
- Substantially higher levels of stability.
- Higher degree of confidence.
- Promotes wholesale positive investor behavior.

Value Proposition for Regulators and Tax Payers

- Permissioned access to issuer and exchange reporting protocol.
- Real time remediation.
- Real data analytics driven surveillance.
- Substantially higher issuer and market compliance.
- Fullest and fairest issuer and market disclosure framework.
- Substantial reduction in review with refocus on process.
- Reduction in operating and administration budgets.
- Substantial reduction in budget appropriation requests.
- Substantially higher levels of productivity.
- Substantial reduction in regulatory conflict.
- Substantially lower instances of issuer and accounting fraud.
- Substantially lower enforcement activity and costs.

Conclusion

The current market for accounting and audit infrastructure software is dominated by large scale enterprise resource planning systems. The majority of solutions are usually cost prohibitive for most small and medium sized enterprises.

The individual enterprise user cost to install and use the DCARPE™ Network protocol software may prove be substantially less expensive as the result of the decentralized cooperative cost structure of all services provided by the Auditchain network. Additionally, the flexibility and scale of the DCARPE™ architecture may theoretically accommodate any size enterprise user.

Depending on the number of Non-Federated nodes deployed by the enterprise, mining for AUDT may theoretically offset the entire cost of the accounting, audit, compliance and reporting obligations of the enterprise.

Financial markets will benefit through the reliability of immutability, real-time assurance, real-time presentation of financial performance and insights into enterprise, development and network performance on a dynamic basis in a manner not previously possible.

Auditchain represents a substantial evolution towards new accounting, audit and reporting methods. Furthermore, early adopters may enjoy a competitive advantage through cost savings and capital attraction as the result of its implementation.

Challenges and Considerations

Adoption of the Auditchain network will be dependent upon a shift in organizational and operational culture. Traditional operational and accounting process can be characterized by a wide range of post transactional and post contractual accounting treatment determination which is highly judgmental.

Consideration must be taken to observe and assess the impact of the implications of an Auditchain network implementation. Tight controls and real-time disclosure requires careful advanced planning and a shift to a preemptive execution strategy in advance of contractual and transactional events. In other words, advance judgement needs to be considered based upon the anticipation of the increasing speed of transactional and contractual environments.

TRANSITION

The expansion and evolution of decentralized voluntary based ecosystems will require a transitional period. Gradual adoption may take the form of segmented implementation which does not constitute a fully audited status. Some enterprises may only perform a partial implementation to assure operational objective of a single control only for the purposes of complying with an agreement.

EARLY STAGES OF SMART CONTRACT IMPLEMENTATION

Ricardian type contracts have a limited history of implementation in live production environments. One of the challenges of the deployment of these types of controls will be complexity and security. The more complexity, the wider the attack surface. Similar to any to any other decentralized protocol, the larger the number of mining and validator nodes, the more decentralized the network is and therefore, the more secure.

COMPETITIVE RESISTANCE POTENTIAL

Additional challenges exist from a competitive perspective. Traditionally, enterprise tends to conceal activities in an effort to gain an element of surprise or a delay in the disclosure of materially negative trends in performance. The time lag of periodic reporting allows these subjective and conditional activities to occur. Current regulations allow for the space to apply corrective measure through accounting judgement but they also provide for the preannouncement of both materially positive as well as negative events.

Time compression of network and enterprise growth and evolution combined with attributes of the Nash Equilibrium may suggest the possibility that the superior competitor may be incentivized to provide an early look at prospects. Apple is famous for its leaks while it seems AMD would rather we forget they exist.

REGULATORY CHALLENGES

Additional challenges exist with regulatory innovation. While typical financial statements contain narratives such as management's discussion and financial analysis, a real-time reporting culture would suggest that such narratives have the capacity to evolve to a new form of fact and financial information reporting. The evolution of the utility of XBRL seems to suggest that such narrative can be mathematically expressed with a simple UI that produces thesis based reports.

While a wholesale regulatory movement to stimulate and/or incentivize real-time enterprise reporting is not anticipated in the near term, there are liberal alternative disclosure protocols practiced by thousands of enterprises. Some exchanges allow unaudited periodic reporting and may welcome a real-time reporting solution.

DEVELOPMENT AND NETWORK STATISTICS PERFORMANCE REPORTING

Recent guidance by regulators have yet to make clear what constitutes an exemption from registration when holders of tokens purchased or mined wish to sell. Depending on the type of digital asset held, it may be clear that such asset is a security. In such a case, the laws are clear. In other cases, utility tokens may or may not be deemed as securities, however, in the interest of full and fair disclosure it may be prudent to make preemptive disclosures to cryptocurrency ecosystem participants. Challenges exist where the creators of the networks choose not to make such development performance disclosures for the future tokens.

With respect to the real-time disclosure of development statistics by dApps or new blockchain projects, challenges may exist with community resistance to forced disclosure. The open source community, however, prides itself on keeping its code in an open GitHub or another repository for the world to see. Challenges may exist in the interpretation of code commits into an audited measurable presentation of performance for non-technical readers on an internal procedural level and on terms that would gain regulatory acceptance. Network utility, adoption and monetization statistics may be easier to capture and present but also would pose additional regulatory acceptance challenges.

Major challenges also exist for statute interpretation efforts made by the legal community and also for regulators when considering the application of aged legislature to assets that may not be able to provide current information as that term is defined by most statutes. Until new legislature is passed the question of what current information is acceptable as a substitute for traditional financial statements in order to be eligible for traditional registration or exemption has yet to be answered.

DCARPE™ Alliance

Auditchain will be the founding member of the DCARPE™ Alliance (“Alliance”). It is expected that the Alliance will be formed as a not for profit entity in Switzerland. The Alliance will consist of globally diversified members of the investment, accounting, audit, legal and financial reporting community.

The purpose of the Alliance will be to engage the regulatory community and begin collaboration on the adoption of regulatory standards that include accommodation for and codification of accounting and regulatory principles that promote the benefits of real time audit and financial reporting.

The Alliance will also collaborate with its members on matters such as implementation, adoption, scaling and integration. The Alliance will help drive the adoption of Auditchain through events and symposiums as well as educate the investment, enterprise, regulatory and network community about the benefits of Auditchain real time audit and reporting. Alliance members will also operate Federated and Non-Federated nodes on the Auditchain network.

Business Summary

Auditchain is being structured as a for profit GmbH based in Switzerland. Auditchain expects to foster adoption to the Auditchain Network through a combination of collaboration with the Alliance and direct marketing to and early collaboration with the enterprise community.

We believe that Auditchain currently enjoys a first mover advantage as a decentralized continuous audit and reporting protocol ecosystem for enterprise and decentralized networks.

Auditchain expects to generate revenue through the receipt of fees in connection with services and transactions on the Auditchain Network. Although it is premature to project the level of revenue and the magnitude of growth, we believe we can draw preliminary comparisons. The typical Fortune 100 enterprise generates more transactions per minute than all transactions combined on a per minute basis on the Ethereum and Bitcoin Blockchains.

We believe that block rewards and AUDT Fees on the Auditchain Network have the potential to exceed the level of all transaction fees on a per block basis than the two largest public Blockchains with a single large enterprise or 10 medium sized enterprises.

References

1. Auditing with the Computer, Wayne S. Boutell. University of California Press, 1965
https://books.google.com/books?id=nFCJgwaMSeMC&pg=PA62&lpg=PA62&dq=Felix+Kaufman+wrote+Electronic+Data+Processing+and+Auditing&source=bl&ots=hyfwHqvEsf&sig=EsDxwkZ4l_NA-Im58RdHrGW14T8&hl=en&sa=X&ved=0ahUKEwiNgPKQ6L3VAhXszIMKHepvDIEQ6AEIMTAB#v=onepage&q=Felix%20Kaufman%20wrote%20Electronic%20Data%20Processing%20and%20Auditing&f=false
2. AICPA: Evolution of Auditing. 2012 Authors; Paul Eric Byrnes, Abdullah Al-Awadhi, Benita Gullvist, Helen Brown-Liburd, Ryan Teeter, J. Donald Warren, Jr., Miklos Vasarhelyi http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_evolution-of-auditing.pdf
3. 2016 Annual Report of ExxonMobil <https://www.sec.gov/Archives/edgar/data/34088/000003408817000017/xom10k2016.htm>
4. Sarbanes Oxley Act of 2002 <https://www.sec.gov/about/laws/soa2002.pdf>
5. Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. 2009. <https://bitcoin.org/bitcoin.pdf>
6. Ricardian Contract https://en.wikipedia.org/wiki/Ricardian_contract
7. The Ricardian Contract. Ian Grigg. http://iang.org/papers/ricardian_contract.html
8. Rethinking the Role of the Standard Financial Statements. Rutgers University Galileo Disclosure Model. Michael Alles, Miklos A. Vasarhelyi <http://raw.rutgers.edu/node/13.html>
9. SECURITIES AND EXCHANGE COMMISSION, SECURITIES EXCHANGE ACT OF 1934. Release No. 81207 / July 25, 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO <https://www.sec.gov/litigation/investreport/34-81207.pdf>
10. Securities Act of 1933. <https://www.sec.gov/about/laws/sa33.pdf>
11. Securities Exchange Act of 1934. <https://www.sec.gov/about/laws/sea34.pdf>
12. Statement on Standards for Attestation Engagements No. 18 IACPA <http://www.aicpa.org/InterestAreas/FRC/AuditAttest/Pages/AttestClarityProject.aspx>
13. International Standards for Assurance Engagements (ISAE) No. 3402 and Service Organization Control (SOC) reporting <http://isae3402.com/>
14. Public Company Accounting Oversight Board <https://pcaobus.org/>
15. DASH Whitepaper. Authors; Evan Duffield and Daniel Diaz. <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/5472261/Whitepaper>
16. DASH Whitepaper. Authors; Evan Duffield and Daniel Diaz. <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146945/Mining>
17. Decentralized Autonomous Organizations. Richard Brown <https://www.ethereum.org/dao>
18. Benefits and Potential Uses of XBRL. IACPA Extensible Business Reporting Language – Use Cases and Benefits
19. Compensation—Stock Compensation (Topic 718) Financial Accounting Standards Board <https://asc.fasb.org/imageRoot/85/51831185.pdf>
20. FASB Accounting Standards Codification Topic 470 Delloitte 2017 <https://www.iasplus.com/en-us/standards/fasb/liabilities/asc470>

Glossary of Terms

DAO – Decentralized Autonomous Organization

dApp – Decentralized Application

DCARPE™ – Decentralized Continuous Audit and Reporting Protocol Ecosystem

ERP – Enterprise Resource Planning

GAAP – Generally Accepted Accounting Principals

IAASB – International Auditing and Assurance Standards Board

IASE 3402 – International Standards for Assurance Engagements (ISAE) No. 3402

IFRS – International Financial Reporting Standards

PCAOB – Public Company Accounting Oversight Board

PoW – Proof of Work

PoS – Proof of Stake

SOC – System and Organization Controls

STAT – Straight Through Accounting Treatment

SSAE 18 – Statement on Standards for Attestation Engagements No. 18, Attestation Standards: <http://www.aicpa.org/InterestAreas/FRC/AuditAttest/Pages/AttestClarityProject.aspx>

XBRL – eXtensible Business Reporting Language