Ulster
University

The Financial Auditing of Distributed Ledgers, Blockchain and Cryptocurrencies

Hosted by the Finance and AI lab, Queens Business School

Professor Daniel Broby

Ulster University, Accounting, Finance and Economics Department, Ulster University Business School, Belfast, BT15 1ED, Northern Ireland, United Kingdom

Introduction

- The Internet and digital money transfers are reshaping financial audits.
- This presentation critically evaluates the auditing of assets in distributed ledgers, blockchain technology, and cryptocurrencies.
- It explores the self-verifying nature of financial data in these systems, challenging traditional audit methods.
- It highlights areas where audit has to change to accommodate blockchain based assets.

The Promise of Self-Verification

- Distributed ledgers and blockchain offer self-verification mechanisms.
- Reduction in reliance on traditional auditing procedures.
- Potential for greater efficiency and transparency.
- Despite self-verification, blockchain has inherent weaknesses:
- Vulnerabilities in smart contracts.
- Lack of standardization.
- Regulatory and compliance challenges.

The role of AI

- Auditing blockchain is a complex task due to its unique features and challenges.
- AI technology provides powerful solutions to enhance the auditing process.
- AI can analyse vast amounts of blockchain data efficiently.
- Detect patterns, anomalies, and potential fraud in real-time.
- Identify suspicious transactions and activities.
- Mitigate risks in real-time.

Need for Audit Adaptation

Ulster University

- Traditional auditing examines financial accounts and records.
- Principles include responsibilities, knowledge, standards, and code of conduct.
- Current auditing norms face disruption from blockchain, cryptocurrencies, and distributed ledgers.
- The audit must evolve to accommodate the distributed nature of digital financial information.
- Current international auditing standards do not fully address these new digital assets.
- Technological complexity intensifies audit risk, with field auditors challenged to detect material misrepresentations.

Blockchain

Ulster University

- A blockchain consists of blocks with multiple transactions and references to the previous block.
- Immutability and verification are key blockchain properties.
- It serves as a distributed ledger, continuously validated by participants.
- Every blockchain transaction is a form of self-audit.
- Participants ensure credits result from permitted debits.

Transaction malleability

- Financial reporting's core functions: Revenue recognition, cash safeguarding, expense recognition, and procurement control (Rogers, Marsh, & Ethridge, 2004).
- Transaction malleability allows post-transaction alterations.
- Addressed by Andrychowicz, Dziembowski, Malinowski, & Mazurek (2015) in the context of Bitcoin's transaction ID algorithm.
- A relay party can modify a transaction without changing its contents, making it hard to detect changes.
- Blockchain auditors face two primary impacts due to malleability:
  - Unique Identifier Challenge: Malleability can lead to transactions being broadcast with a different transaction ID than initially generated.
  - Double-Payment Fraud: Auditors must be vigilant about potential double-payment fraud.

Challenges of Auditing DAOs (Digital Autonomous Organizations)

Ulster University

- DAO-type structures pose various audit challenges, especially concerning entity jurisdiction.
- DAO's legal position is unclear since it lacks legal entity status.
- Enforcing judgments against a DAO is complex; funds cannot be taken without majority shareholder agreement or compliance with smart contract rules.
- Auditors dealing with DAOs should recommend:
  - Clear definition of asset access and spending requirements.
  - Legal and jurisdictional clarification for DAO entities.
  - Enforcement mechanisms in case of disputes or judgments.

Blockchain forks

- A blockchain fork occurs when there is a fundamental disagreement within a blockchain network about the rules governing the creation and validation of new blocks.
- In the case of a contentious hard fork, it can take time for the network to resolve the situation.
- This disagreement can lead to the blockchain splitting into two or more separate chains, each with its own set of transactions and history.
    - Long-term blockchain forks pose a significant challenge to auditing.
    - Short term forks are common, but long-term forks are of concern.

Example: London Hard Fork

- August 2021. Ethereum network was upgrades to make transactions more predictable, and ensure the network's long-term sustainability.
- The London Hard Fork introduced several significant changes to the Ethereum network, with the primary goal of improving the network's security, scalability, and user experience.
  - EIP-1559 changed the fee mechanism for Ethereum transactions. Previously, users would manually set gas prices for their transactions, leading to congestion and unpredictable fees.
  - EIP-3554 moved Ethereum transitions from a Proof of Work (PoW) to a Proof of Stake (PoS) consensus mechanism.

Forks: The challenge for auditors

- Blockchain forks challenge the stability of financial audits.
- Auditors need to adapt to the dynamic nature of blockchain communities and rule changes.
- A deep understanding of blockchain forks is essential for accurate and reliable auditing.
- Auditors dealing with blockchain audits should:
    - Stay informed about blockchain communities' consensus and rule changes.
    - Understand the implications of long-term forks on transaction histories.
    - Develop audit procedures to address the complexities of auditing across forked chains.

Short term forks

- When two miners simultaneously discover valid solutions for the next block, one becomes the successor, and the other becomes an orphan.
- Short-term blockchain forks are a regular occurrence, especially in networks like Bitcoin.
  - Blockchain PoW accepts longer chain at any point in the future if it exists, with no guaranteed time period for the finality of transactions.
- Auditors face more frequent challenges due to these short-term forks.
- Auditors must ensure that the audit only covers blocks with sufficient proof of work, making future re-arrangement of those blocks infeasible.
- Introduction of longer chains can result in double-spending potential and transaction reorganization.

Auditor's Role in Blockchain Custody

- Auditors play a crucial role in ensuring the reliability of central asset ledgers in distributed ledgers.
- Verification of distributed ledgers is essential to bridge the gap between the digital and real world.
- Auditors can adapt blockchain explorers to facilitate this verification process.
- Auditing distributed ledgers involves timestamping, validity, and robustness.
- Multiple blockchains exist in the distributed world, challenging the perception of a single immutable record.

Navigating Multi-Location Audit Risks

- The internet operates across multiple jurisdictions, posing audit challenges.
- SAS No. 107 outlines factors to consider when addressing jurisdiction issues in multi-location audits.
- Auditors must consider the nature of assets and transactions, centralization of records, control environment, monitoring frequency, and materiality of location.
  - Real-time auditing is possible, but context is crucial.
  - Ownership and transaction coding in a digital context may not align with the physical world.

Permanent establishment (tax)

- In July 2017, a French court granted Alphabet Inc (Google's parent company) a tax reprieve.
- The court ruled that Google's subsidiary, Google Ireland Limited, did not have a "permanent establishment" in France.
  - The term "permanent establishment" typically refers to a fixed place of business where a company carries out its business activities. In the context of multinational corporations like Google, it's crucial to determine whether their activities in a particular country go beyond mere sales and marketing, reaching the threshold of having a permanent establishment that is subject to taxation.
- The audit trail played a crucial role in determining jurisdiction.

Self-Verification in Blockchain

- Blockchains are designed with properties like immutability and self-verification, which can benefit auditing.
- However, auditors must explore the robustness and reality of self-verification processes.
    - Blockchain technology employs cryptographic hashes within decentralized networks. Typically, 6 confirmations are considered sufficient for most large transactions, resulting in approximately a 60-minute delay after a transaction is featured in a block. During adverse blockchain conditions, such as mining nodes not validating blocks properly, users are advised to wait for a higher number of confirmations. In some cases, this wait could be as long as 36 confirmations, corresponding to a 6-hour delay.
- AI can play a vital role in automating the confirmation process.
- AI algorithms can analyse blockchain data, monitor network health, and assess the risk of blockchain forks.

Silent transactions

- Blockchain-based cryptocurrencies allow for silent transactions.
- Parties can create and generate transactions from any location with access to the required keys.
- Malicious parties with private key access can silently generate valid transactions, even remotely.
- Transactions can be broadcast from any node on the network without physical presence.
- Traditional bank accounts often require transactions to be initiated from specific terminals or with approved signatories physically present.
- In blockchain, possession of private keys or knowledge of the appropriate hashlock condition is sufficient to initiate transactions from anywhere.
- AI can be used to continuously monitor transactions and look for unusual or suspicious activity.

Effective Auditing Requires Defined Periods

- Auditing must be bounded within a finite time period, ensuring no transactions fall between audits.
- Blockchain, with discrete time intervals, simplifies this process using block generation time.
- Transaction presence in a block doesn't guarantee the exact time of creation and broadcast.
- Complexities arise in auditing internal controls for transaction initiation, as pre-authorized transactions can be broadcast later.
- Auditors should include the movement of all blockchain-based funds between wallets (public keys) in the audit process.
  - Verification of fund control by the organization.
  - Prevention of historical fraudulent transactions from being re-broadcast in the future.

Volatility of Cryptocurrencies

- Rapid price volatility of cryptocurrencies poses a significant challenge for audit.
- The overall number of coins held may remain constant, but their value can fluctuate drastically.
- Limited liquidity and market manipulation possibilities make price and market stability uncertain.
- Auditors must identify how funds held within exchanges are stored and assess their vulnerability to market fluctuations and trading orders.

Challenges of Third-Party Holding

- Auditors face challenges when funds are held by third parties in a distributed online environment.
- Funds may be deposited with exchanges or online wallet services where private keys are accessible to third parties.
- Security concerns arise as third-party holding may lead to discrepancies and potential deficits due to cyber-attacks or insider theft.
- Funds within online exchanges and wallets often lack a blockchain-based audit trail. Eg FTX

Transfer of Private Keys

- The audit process needs to ensure the correct recipient was specified and that the receiving address can be substantiated based on documentation.
- Blockchain transactions involve public key hashes (addresses) corresponding to cryptographic identities.
- Private keys used to access a wallet can be transferred between parties, complicating the verification of the party operating an address.
- Best practice advises using each public key (address) only twice: once to receive funds and once to transfer funds out.
    - This security measure protects the user's public key until a spend transaction is created.

Time-Locked Transactions

- Smart contracts with timelocks can be part of blockchain transactions. Auditors may find time-locked transactions signed by parties, promising funds based on a time condition.
- These transactions should not be considered valid, as the initiating party can reverse the payments by moving funds from the sending address before the time condition is satisfied.
- Once the transaction is invalidated due to a double-spend, the recipient will not receive the funds.
- These transactions should be treated as non-binding IOUs in the audit process.

Multi-Signature Transactions

- Auditors traditionally verify authorized signatories in the physical world.
- Auditors play a crucial role in verifying the integrity of multi-signature setups and ensuring that only authorized parties have control over funds.
- In blockchain, funds received, known as Unspent Transaction Outputs (UTXOs), can have restrictions on spending, often involving multi-signature requirements.
- Multi-signature schemes require multiple private keys to spend funds, enhancing security. The solution we propose for audit is “Arbitration-style contracts”, an approach not dissimilar to that proposed by (Treleaven & Batrinca, 2017).
- Auditors must ensure that keys for multi-signature wallets are in place and that funds can be accessed.
  - Verify that no keys from individuals who have left the organization or should no longer control the funds are present.
  - Check N-of-M signature schemes (e.g., 2-of-6 managers), audit key-holders to prevent collusion by departing members before key rotation.

Micropayment Contracts

- Auditors must adapt to micropayments in blockchain for small fund transfers.
    - Sender holds a dual-signed "refund" transaction with a time-lock.
    - A "bond" transaction is formed, requiring both parties to sign for fund release.
    - The "bond" transaction is sent to the blockchain.
    - Parties keep updating the "refund" transaction outside the blockchain.
    - The recipient can broadcast their "refund" transaction to claim funds before the time-lock expires.
- Micropayment channels permit repeated transactions within larger ones, updated dynamically.
- Use of a time-locked transaction combined with a 2-from-2 multi-signature contract.
- Micropayment funds should be audited with caution.
- Contract completion depends on broadcast and inclusion of the release transaction in a blockchain block.

Hashlock Contracts

- Hashlock contracts restrict the spending of received transactions until a specific pre-image is provided.
- To spend the locked funds, the transaction must include the input to a one-way function, yielding a predetermined output.
- Auditors must closely review UTXOs (Unspent Transaction Outputs) protected by hashlocks.
- Funds in hashlocked transactions are inert until the corresponding pre-image is revealed.
- Auditors should confirm the organization's control and access to hashlocked funds.

Chain Obfuscation and Coin Mixing

- During an audit, the use of transactions for obfuscation or coin mixing can pose challenges.
- CoinJoin and coin mixing are techniques used to obscure the origin and destination of cryptocurrency transactions.
- Techniques for obfuscating transaction origins and destinations can hinder audits.
- Auditors may face challenges in verifying the true destination of funds.

Cross-Chain Transactions

- Audits become more complex when involving multiple cryptocurrencies and indeed future retail CBDCs.
- Different cryptocurrencies have independent blockchains.
- Cross-chain transactions occur during exchanges between two different cryptocurrencies, adding audit challenges.
- Auditing cross-chain transactions requires considering both blockchains.
- The scope of the audit may significantly increase when multiple cryptocurrencies are involved.

Conclusion

- Traditional audit processes are insufficient to address the complexities of digital money transfer and storage in blockchain and cryptocurrency environments.
- Auditing is transitioning from a traditional double-entry bookkeeping approach to a more versatile triple-entry bookkeeping model.
- Auditors must adapt to the distributed and multijurisdictional nature of blockchain assets, redefining rules and procedures to accommodate the intricacies of these systems.
- Challenges, including transaction malleability, blockchain forks, and the emergence of Digital Autonomous Organizations (DAOs), necessitate dedicated audit professionals to address these issues.
- AI is pivotal to addressing these challenges.

Ulster University

Questions