ARTICLE

The Lightning Network: Where No Auditor Has Gone Before

by Noah Buxton, Nick Ward

December 08, 2021

While the Lightning Network enhances the scalability of the Bitcoin blockchain, it presents new and untested challenges in tracking transactions and bitcoins. Here, the Digital Assets team ventures into untested territory and shares their insight into auditing this novel payment channel.

What It Is

The Lightning Network (Lightning) has been considered a game-changer in bitcoin's evolution from a technical innovation with limited processing capacity to a payment method used on a daily basis. Lightning was developed as a scaling solution for the Bitcoin blockchain to decrease transaction processing times while reducing the associated costs. It also offers a high degree of transaction privacy that is similar to using cash.

The network's ability to offer payment channels with high throughput while maintaining users' financial privacy creates auditability and tracking challenges for management, compliance teams and financial statement auditors. As Lightning enables the use of bitcoin for routine consumer payments, its inevitable growth will require best practices, as well as tools to support auditability, asset management, accounting and financial reporting.

Why It Matters

Companies and partnerships have varying levels of accounting, compliance and financial reporting obligations, depending on their structure, domicile, accounting standards and audit requirements. Two types of entities that would be impacted by adoption of Lightning would be crypto native companies such as exchanges, wallet applications and other crypto projects that already transact in digital assets, and non-crypto native companies that are dipping their toes in or starting to integrate a revenue stream, existing financial product or the like to transact in crypto. This article focuses on crypto native entities as they will be most directly impacted by tax, audit, compliance and financial reporting changes from adopting Lightning.

Below are three of the five key assertions included in a financial statement audit engagement. Each assertion brings unique challenges to the auditor's ability to test and management's ability to demonstrate an audit trail.

Rights and Obligations

The "rights and obligations" assertion relates to management's ability to demonstrate dominion, control and ownership of the assets on a company's balance sheet. This is an important area for internal accounting processes, but also a key area of testing in financial statement audits to ensure the balance sheet is fairly presented.

With bitcoin and other similar digital assets, dominion and control of an asset is demonstrated by holding the private key/s to company wallets. One of the advantages of bitcoin and digital assets is that if a company maintains its private keys securely and confidentially, they ultimately have control of those assets. Ownership of a company's digital wallet can be tested multiple ways: by signing a message with the private key or by executing a small value transaction on the network. Signed messages can be verified by an auditor using the public key, and test transactions will appear on the blockchain, both providing suficient audit evidence that the company has control of the specified wallet.

When thinking about how management accounts for bitcoin assets on the Lightning Network (or how they can prove ownership to an auditor), the message signing or test transaction process noted above is insuficient. Lightning channel transactions will only be reported on-chain once the channel is closed (and the assets are settled to the wallets participating in that given channel).

However, given the current practices of exchanges, wallet operators and other fintechs using Lightning, management teams may want to leave payment channels open. It's not optimal to close the channel simply to align with a period end or financial reporting deadline. As a threshold matter, where the value of assets in the channel (whether representing an asset or a liability) is material, management may well need to consider

operational processes to settle open channels for month, quarter or year-end accounting, reporting or audit. This is especially true for public companies.

As another consideration of how a company can provide suficient audit evidence to test the balance sheet, a company would need to sign with the private key of the Lightning node, and the auditor would then search for Lightning channels open with that node to provide confirmation that the entity is participating in channels with suficient bitcoin or suficient USD value worth of bitcoin.

Specifically, the auditor requests the company to sign a message the auditor has provided. That signed message is sent to the Lightning node address. By proving ownership of the node, the external auditor, or internal accounting or audit team, can gain comfort over the related channel balances of that node. By viewing the signed message, the auditor can verify that the message was signed by the entity with their private key/s.

In this scenario, context is important because the entity's participation in the channel could be related to revenue, expenses or some combination of the two. While signing and validating a signature of a Lightning node is a process that can aid the conclusion that management owns some or all of those assets, it does not represent the same level of proof as a non-Lightning wallet signature or transaction.

Accounting and finance teams should work closely with their product and engineering teams to help communicate the complexity created by using Lightning.

Existence

Management and accounting teams have been grappling with existence and proper accounting entries for bitcoin and digital assets for many years now. Demonstrating existence, and the auditor testing existence of a given company's bitcoin assets, have both presented stumbling blocks as the record of existence is recorded on a distributed ledger, not a third-party-maintained ledger where that third party confirms the existence for the auditor or management.

Therefore, when recording accounting entries for bitcoin assets, the source of truth is the blockchain. With a bitcoin wallet address, the auditor can view the unspent bitcoins at that address using their own bitcoin node (which will contain a copy of the complete ledger) or through the use of an explorer (a software allowing easy searching of historical on-chain transactions and balances).

But how can management and auditors obtain comfort over the existence of bitcoin assets or liabilities that have been committed to a Lightning channel? Similar to how invoices and proof of payment for traditional goods or services can be reviewed, auditors can examine the transactions that took place within a Lightning channel to verify existence of some or all of

the assets in the channel. However, the record of transactions and net obligations in a Lightning channel are not available for all to see on-chain or through an explorer tool. Instead, details need to be pulled from nodes and/or counterparties to validate balances.

Pulling Lightning data for use by accounting teams and auditors requires that the entity be a member of the channel and also that the individual has a special skillset and knowledge. More tools, including explorers and message signing technology to enable complex audit engagements, are being developed to tackle the challenge of exploring Lightning channels.

Completeness

Management of any company should want their financial accounting and reporting to be complete. In presenting audited financial statements, completeness is a key assertion that management must make to the auditor, and the auditor must therefore test.

In evaluating completeness, an auditor will seek to verify that the company's reported income and expenses as well as balance sheet assets in bitcoin are presented with all relevant transactions included, and that the transactions that make up those line items are reasonably accurate. When considering the use of bitcoin in commercial transactions, presenting complete and accurate financials requires accounting teams to have the tools to properly record journal entries based on information from the specific blockchain.

This is one area where blockchains generally increase the ease of auditing for completeness — knowing an entity's bitcoin wallet addresses reveals a complete and reliable ledger of all historical transactions, their nominal amount in bitcoins as well as the historical balance of bitcoins at any given block height (time).

However, if Lightning is considered a layer on top of the Bitcoin network where only certain transactions are visibly anchored to the base chain, the inherent completeness of on-chain bitcoin transactions is now complicated by Lightning.

While obtaining suficient information regarding completeness is not impossible, there are a few key steps needed to do so. Relevant procedures include understanding the entity's internal process and control of Lightning channels, approved transactions over Lightning as well as approvals for maintaining assets and/or liabilities in those channels. As members of channels can see Lightning transactions in that channel, management and audit teams can also review in-channel activity and reconcile that activity with management's accounting records to assess completeness.

In the case of completeness, management may not need to close payment channels for the auditor to complete testing. However, periodic rolling of channels can aid both accounting

teams with closing processes and auditors in their testing of company records.

Final Thoughts

The challenges and solutions presented here are not an exhaustive list. Many challenges remain in proper accounting and audit of Lightning transactions, including the impact of gain or loss on assets in Lightning channels or settled from those channels. Overall, the approaches discussed can be thought of as best practices and emerging methodologies that accounting teams and audit teams can leverage to understand the impact of their organization's use of the Lightning Network for financial transactions.

For questions or assistance, contact our Digital Assets & Crypto team.