frontiers | Frontiers in Blockchain

TYPE Mini Review
PUBLISHED 14 July 2023
DOI 10.3389/fbloc.2023.1205491

OPEN ACCESS

EDITED BY
Andrea Pizzoferrato,
University of Bath, United Kingdom

REVIEWED BY
Kaiwen Zhang,
École de technologie supérieure (ÉTS), Canada

*CORRESPONDENCE
Wei Zhang,
w.zhang@nchain.com

RECEIVED 13 April 2023
ACCEPTED 05 July 2023
PUBLISHED 14 July 2023

CITATION
Zhang W (2023), Miner ID: Facilitating bitcoin as a service.
Front. Blockchain 6:1205491.
doi: 10.3389/fbloc.2023.1205491

Miner ID: Facilitating bitcoin as a service

Wei Zhang*

nChain UK Limited, London, United Kingdom

Block production in Bitcoin, often referred to as mining, is becoming increasingly industrialized. Many nodes in the network are represented by registered business entities. The concept of Bitcoin as a Service is also pushing the industry to become more customer oriented. Services such as transaction validation, transaction status query or notification, and blockchain data indexing are in high demand among blockchain application providers and users. As service providers, nodes need to distinguish themselves from others and be identifiable. In this article, we introduce an efficient self-established identity system, called Miner ID, to enable nodes to be publicly identifiable. It is based on economic investment and active participation in the blockchain network. Moreover, Miner ID is optional for nodes, and it does not affect the consensus mechanism of the network. We explore use cases including instant transaction confirmation, blockchain attestation, public key infrastructure, and token recovery. Miner ID can also be used for secure communication with applications, services, users and peers.

KEYWORDS

utility-driven blockchain, instant transaction confirmation, public key infrastructure, self-established identity, bitcoin miners

1 Introduction

It was more than a decade ago when the first block of Bitcoin was published in 2009. While Bitcoin was originally used as a novelty payment mechanism, the underlying blockchain technology now attracts significant interest from businesses, government, and academia. Companies and individual developers are building numerous applications on Bitcoin that serve use cases relating to supply chain, healthcare, central bank digital currency, regulatory compliance, and many other areas. Most of them require Bitcoin nodes to act as service providers to ensure data authenticity, integrity, and immutability over time, in addition to being a transaction processor. These applications effectively interact with Bitcoin nodes. For more transparency, reliability and even functionality, we propose Bitcoin nodes use Miner ID to identify themselves, to facilitate secure communications with applications and users, and to build a reputation backed up by proof of work.

Traditionally, identity is issued by centralized entities, and the root trust is assumed with respect to those centralized entities. In contrast, Miner ID is a self-established identity, and the trust is derived from proof of work and the transparency of a blockchain. A Bitcoin node can link a public key to their identity by producing blocks. Trust in the network can then be extended to individual nodes with a good reputation for block production.

As part of background information, we describe some common approaches that may help to identify nodes in the network. A block is appended to the blockchain if it contains a proof that an expected amount of computational work has been done, called proof of work. The successful node receives a reward which is given in the first transaction in that block, which is called a coinbase transaction. The input of a coinbase transaction can be filled in with an arbitrary string of 100 bytes. Most nodes who wish to be identified will publish their

TABLE 1 A real example of a coinbase transaction (WOC, 2023).

Transaction ID	212aa62511c1e5db3ae6f9156eb113a2ef4f4569c1d9afe82d50743fd0ef284f
Input (arbitrary string)	https://taal.com
Output value (subsidy + fees)	6.25 + 9.70698093
Output script (public key hash)	18VWHjMt4ixHddPPbs6righWTs3Sg2QNcn

company name and other relevant information in this 100-byte space. The total output value of a coinbase transaction is the sum of the block subsidy at the time and the transaction fees from the transactions in that block. The nodes can set the locking script for their chosen public keys to secure the output value if they are successful in finding a valid block. Some nodes reuse their public key for their coinbase transactions. An example of a coinbase transaction is given in Table 1.

With the information in the input or the output of a coinbase transaction, most nodes can be identified publicly. This is also how block explorers identify nodes. Alternatively, analyzing messages gathered by using the Bitcoin peer-to-peer messaging protocol and peers' IP addresses may also help identifying nodes. However, none of these approaches gives a robust and secure way to identify nodes accurately. In this article, we argue that Miner ID is a stepping stone to drive the adoption of blockchain technology for utility driven applications (as opposed to speculation driven investment vehicles). We explain what is Miner ID and present a few use cases in which Miner ID can offer authenticity, data integrity, and many other features. In some of them, Miner ID is a critical enabler.

2 Miner ID

Miner ID is represented by a public key of a digital signature scheme, e.g., Elliptic Curve Digital Signature Algorithm (ECDSA). It is published in a coinbase transaction together with a digital signature in its data payload. This implies that one needs to mine a block successfully in order to establish a Miner ID and more blocks to maintain it or build their reputation. Nodes can use Miner ID to show that they continuously contribute to block production over a long period, indicating their economical commitment in the services they provide. This sets a high barrier to entry that can deter most spoofing and impersonation attacks. It is important that the message that is signed by the signature is dependent on the block that contains the coinbase transaction. This prevents any potential impersonator from replaying the signature in another block. The message can also contain a human readable alias of Miner ID, e.g., Good Node Company, and other information about the company.

One limitation that comes with such a high barrier to entry is the exclusion of nodes who have very little computational power to produce a block. Given the trend of the block production (mining) industry, the number of such nodes are becoming smaller and smaller. On the other hand, even with 1% of the total computational power of the Bitcoin network, the probability of a node finding a block within 72 h can be as high as 98.70%. Another justification for the potential limitation is the formation of mining pools. A mining pool offers better chance for nodes who has small computational power to gain rewards more efficiently. In this case, the nodes are contributing to a single miner ID representing the mining pool.

The public key representing the Miner ID can be updated regularly as part of a node's key management protocol. Each update will come into effect after the corresponding block is accepted by the network. The public key can also be revoked in case of the private key being compromised or lost. Instant revocation can be achieved via authenticated peer-to-peer messaging protocol (BRFC, 2023) or spending a dedicated Bitcoin transaction whose spending status is linked to the validity of the public key (Tartan et al., 2021).

The trustworthiness of a Miner ID can be primarily measured by the expected amount of computational power required to produce the blocks that contain that Miner ID, which can be computed based on public information including block headers and coinbase transactions. The first Miner ID reference implementation was released to the public in 2020 (RIR, 2022), and TAAL was the first Bitcoin node to adopt Miner ID (FCT, 2021).

3 Use cases

With Miner ID, we can build secure applications on a decentralized network without concerns over the lack of accountability. Moreover, Bitcoin nodes with Miner ID can also be seen as the equivalent of root certificate authorities in the public key infrastructure (PKI) that underpins the security of internet. We present several use cases to demonstrate the importance and usefulness of Miner ID. Each use case can offer a new revenue stream for Bitcoin nodes in addition to transaction fees as they are providing extra services. These revenue streams can be realized in traditional business models with settlement in fiat currencies, further hiding the complexity of blockchain technologies from the users. In some cases, the revenue streams may become so sustainable that the transaction fees can be reduced to zero, which is beneficial for many users.

3.1 Instant transaction confirmation

The block interval is set to 10 min in Bitcoin. It implies that it takes on average 10 min for a transaction to be published in a block. Accounting for the complication of block reorgs, where there are competing chains in the network, it takes multiple blocks for a transaction to be considered settled in the blockchain. Miner ID can be used to provide an authenticated response on the validity of a transaction or an authenticated notification that there is a double spend. The confidence in the response is based on the node following

the first-seen rule in which a valid transaction can only be accepted if its input is seen for the first time. When the input is seen again, the relevant transaction is considered a double spend from the node's perspective. As a result, the response can be instant, subject to network latency, and independent of block interval, as it only requires the node to validate the transaction before sending the response. Miner ID can also be used for nodes to specify API endpoints for users to connect to them directly, further facilitating the instant transaction confirmation process.

In many applications, especially those which have low transaction values, e.g., coffee payment or utility-driven nano-payment transactions, the instant response can be considered as a confirmation that the transaction will be included in the blockchain. The application users do not need to wait for the transaction to be included in a block. This significantly improves the user experience of the applications.

Another example that benefits greatly from instant transaction confirmation is Bitcoin-based token solutions that utilise Bitcoin transactions as a representation for token transfers. The value of bitcoin involved in such transactions can be as low as 1 satoshi, independent of the token values that are being transferred. With Miner ID, token users can get an authenticated confirmation on their token transfer immediately from a node or even multiple nodes without waiting for the next block. While the token value might be high, the value in bitcoin is negligibly low. Any double spending of bitcoin lacks incentives, and any double spending of tokens can be prevented by the token issuer. As a result, Miner ID allows such token transactions to be confirmed immediately even when the transactions are of high value.

3.2 Attestation to blockchain data

One data set is of particular interest is the unspent transaction output (UTXO) set held by a node. Bitcoin can only provide a definite proof that a transaction output is spent, e.g., a Merkle proof of the spending transaction. When an output is unspent, there is no efficient mechanism to prove it. With Miner ID, a certain level of trust in a node can be assumed. There are two main use cases to take advantage of a UTXO set from a trusted source.

The first one is initial block downloading. While Bitcoin scales, downloading and verifying the blockchain from scratch would take long time. Being able to trust the UTXO set for a recent block height, a new node can start to process transactions straightaway. Miner ID can ensure the authenticity and integrity of the UTXO set from a reputable node. The savings are not only computational but also economical. The amount of time saved in initial block downloading and verification can be utilised for mining new blocks, which would be weeks in the future and translates to several millions of US dollars revenue.

The second one is application specific. Many applications link the status of an object with the spending status of a transaction output. Querying the status of an object is equated to query the spending status of a transaction output. For example, in the UTXO for PKI paper [ref], when verifying a certificate, one queries the spending status of a transaction output. By connecting to one or multiple nodes with Miner ID, the verifier can be convinced that the transaction output is unspent, which implies that the certificate is still valid.

Both uses cases are enabled by Miner ID in an efficient manner. Miner ID helps a node to build reputation, then to offer authenticity and data integrity.

3.3 Public key infrastructure

Once the trust on individual nodes is established, the trust can be propagated to the ecosystem. While nodes focus on transaction validation and block production, they can use their Miner ID to issue public key certificates to blockchain information providers who obtain blockchain data from them. This includes the UTXO set for a given block height, a live UTXO set or live mempool data from the node, block headers, or even data from their peers. These blockchain information providers can be scaled to serve billions of users without affecting the core operations in transaction validation and block production. Further hierarchical layers can be added to create a layered network serving more devices such as IoTs. A node with Miner ID is like a root certificate authority with a root certificate in a traditional PKI. While a traditional PKI underpins the security of the internet, a PKI rooted in Miner ID can underpin the security of the Bitcoin layered network. The difference is that the trust on the nodes is from proof of work and transparency, while the trust on the root certificate authority is largely assumed.

3.4 Token recovery

While it is common to perceive that blockchain technology is about decentralization, it is certain that any new technology is subject to legal frameworks and laws. Some traditional laws are still behind technologies and waiting to be updated. According to Forbes, over 3 billion USD worth of digital assets are lost to hacks every year (Bambysheva and Linares, 2022), not to mention losses to ransomware attacks and other criminal activities. There was no legal mechanism to recover any of the losses. Digital Asset Recovery Alert (DARA) is a regulation technology tool developed to help victims to recover lost or stolen digital assets and for law enforcement to freeze or confiscate digital assets from criminals (Confiscation Transaction, 2022; DARA, 2022). Nodes with Miner ID can implement DARA to receive court orders and to programmatically send authenticated alerts to their peers informing them of the transactions in question, and to report to the court their compliance with the order. Miner ID allows nodes to be identifiable in a legal framework, to be held accountable for decisions in their operations, and to be trusted as a compliant legal entity.

There are many other use cases such as preventing bad actors from impersonating a reputable node, proving that a certain number of blocks has been produced within a timeframe as a key performance indicator, or even attesting to the redaction of blockchain data (Kiraz et al., 2022). The important point is that since Miner ID is a costly reputation to establish, any false attestation that is easy to verify will not be in the economic interest of the node.

4 Conclusion

This article explores the use of Miner ID in various scenarios to allow nodes to offer the best services to their customers and be

compliant with regulations. In some cases, Miner ID enriches the use cases which blockchain technology can offer. Although Miner ID is optional for nodes, it will certainly help their business to grow sustainably and be well-prepared for new regulations. One of the few missing pieces for mass adoption of blockchain technology is a robust and comprehensive legal system. Any new technology should come with accountability. This does not compromise the decentralization of a blockchain system, rather it embeds a decentralized system into a legal framework. Decentralization offers robustness, and the legal framework offers accountability. Trust in the system will be enhanced significantly as long as transparency is ensured.

Our future work will continue follow the development and adoption of Miner ID, gathering empirical data and statistics to understand the effectiveness of Miner ID and reflecting the evolution of regulations around blockchain technology.

Author contributions

The author confirms being the sole contributor of this work and has approved it for publication. All authors contributed to the article and approved the submitted version.

Acknowledgments

Miner ID was first proposed by Steve Shadders in 2018. At that time, the motivation was to protect nodes from impersonations for contentious protocol changes. Since then, the idea has been further developed at nChain to enable more use cases. We thank all who have contributed to Miner ID.

Conflict of interest

Author WZ was employed by nChain UK Limited.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Bambysheva, N., and Linares, M. G. S. (2022). Blockchain currency hacks. Available at: https://www.forbes.com/sites/ninabambysheva/2022/12/28/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/(Accessed April 12, 2023).

BRFC (2023). Bitcoin SV specifications - BRFC - miner ID. Available at: https://github.com/bitcoin-sv-specs/brfc-minerid (Accessed April 12, 2023).

Confiscation Transaction (2022). Specification for confiscation transaction. Available at: https://github.com/bitcoin-sv-specs/protocol/blob/master/updates/confiscation-transactions.md (Accessed April 12, 2023).

DARA (2022). Bitcoin SV release notes for DARA. Available at: https://github.com/bitcoin-sv/bitcoin-sv/releases/tag/v1.0.13 (Accessed April 12, 2023).

FCT (2021). First coinbase transaction with miner ID. Available at: https://whatsonchain.com/block/000000000000000000035359ba3b0e5098687944af769b5fff452aa8dc47c4a9b5 (Accessed April 12, 2023).

Kiraz, M., Liu, S., and Vaughan, O. (2022). *How to dynamically redact a hash preimage on bitcoin using ZKPs to be published*. Berlin, Germany: Springer.

RIR (2022). Miner ID reference implementation releases. Available at: https://github.com/bitcoin-sv/minerid-reference/releases (Accessed April 12, 2023).

Tartan, C., Wright, C., Pettit, M., and Zhang, W. (2021). "A scalable bitcoin-based public key certificate management system," in Proceedings of the 18th International Conference on Security and Cryptography - SECRYPT, 06-08 July 2021 (Portugal: SCITE PRESS), 548–559.

WOC (2023). A real example of a coinbase transaction. Available at: https://whatsonchain.com/tx/212aa62511c1e5db3ae6f9156eb113a2ef4f4569c1d9afe82d50743fd0ef284f (Accessed April 12, 2023).