Addendum to the BRC-100 Risk Assessment

The Bitcoin White Paper's Identity Firewall and BRC-100

Purpose of This Addendum

This addendum supplements the previously released paper, **"BRC-100 Risk Assessment: Centralization, Surveillance, Security and Ecosystem-Control Risks."** That paper examined whether widespread BRC-100 adoption could create an ecosystem vulnerable to surveillance, identity gatekeeping, financial investigation, application control and loss of independent user autonomy.

After the paper was released and readers began digging more deeply into the issues it raised, an important additional question emerged:

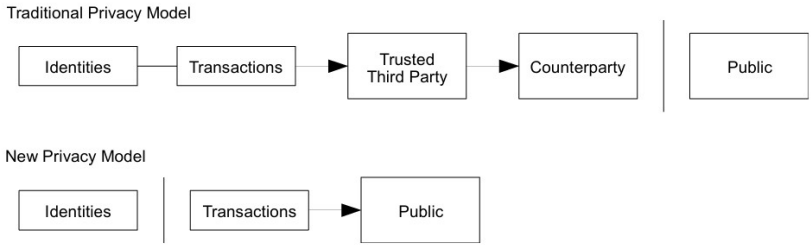
> **"Is identity firewalled from public keys under BRC-100 in the manner described in Section 10 of the Bitcoin white paper?"**

This question deserves separate treatment because it goes directly to the relationship between BRC-100's persistent identity architecture and the privacy model originally described for Bitcoin.

Section 10 of the Bitcoin White Paper

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

The Question, again:

"Is identity firewalled from public keys under BRC-100 in the manner described in Section 10 of the Bitcoin white paper?"

The Response:

No, not by default.

The white paper's privacy model, as defined in Section 10, relies on two core principles:

1. Public keys remain anonymous, with no link to a real-world identity.
2. Fresh key pairs are used for each transaction so that activity cannot easily be linked to a common owner.

BRC-100 introduces a persistent public identity key as a first-class element of the wallet interface. Applications can request this key (subject to permissions), and BRC-52 certificates can bind real-world attributes—such as name, nationality, age, or national digital identity information—to it. Every wallet request also carries the originating application's domain.

It is important to be precise about the cryptography. BRC-100 does not place the identity key or the application domain on-chain. BKDS (BRC-42) is deliberately different from BIP32: knowing only the identity public key does **not** allow an outsider to derive child keys or determine whether an observed on-chain key belongs to that identity. Derivation relies on an ECDH shared secret. Fresh derivation prefixes and suffixes are generated for actions and outputs (as implemented in the reference Wallet Toolbox and specified in BRC-29). Key-linkage revelation (BRC-69) is not public by default; a wallet must deliberately disclose the necessary material.

A BRC-100 implementation can therefore still use derived transaction keys and keep the root identity key private. The standard supports that separation.

However, the architecture makes the identity key readily available and encourages its use across applications. Simply disclosing the identity key or a certificate does not reveal the user's derived transaction keys. What it does create is a persistent, identified reference point. That reference point can later be combined with transaction participation, wallet or application metadata, retained derivation records, or a deliberate BRC-69 linkage revelation.

The cryptographic separation between identity and transaction keys therefore remains intact against unauthorized public observers. **BRC-100 nevertheless adds standardized, permission-controlled paths that allow authorized — *or potentially compelled* — parties to bridge that separation.** As a result, preserving the broader identity firewall becomes partly a policy, permission, and implementation decision that users, wallet developers, and applications must actively maintain.

That is one of the central risks identified in the original BRC-100 Risk Assessment.

[continued next page]

Why This Matters

The Bitcoin white paper did not claim that transaction privacy would come from hiding the public ledger. It proposed breaking the flow of information between public transaction keys and real-world identities.

BRC-42-derived transaction keys can still help preserve cryptographic non-linkability of the on-chain keys themselves. The concern is that BRC-100 adds standardized mechanisms through which identity keys, certificates, application origins, and key relationships may be requested, disclosed, or correlated by the relevant parties *(applications, certifiers, storage providers, and anyone who can compel them)*.

This does not mean that every BRC-100 transaction is automatically linked to a legal identity, nor does it create a public derivation graph visible to pure blockchain observers. It means that the separation described in the white paper is no longer maintained solely by the transaction architecture. Its preservation now depends on:

- Whether applications request the root identity key
- Whether identity certificates are required
- Whether the same identity is reused across applications
- Whether key-linkage functions are enabled
- Whether wallet and application metadata are retained
- Whether users understand and refuse unnecessary disclosure requests

The risk is not that BRC-100 completely destroys the white paper's privacy model, nor that it creates public on-chain cryptographic linkage of the kind BIP32 would allow.

The risk is that it turns the hard separation between identity and transaction keys into something optional — something applications can easily request and cross.

Conclusion

BRC-100 can be implemented in a manner that preserves substantial separation between identity and transaction keys. It does not preserve that separation automatically.

Developers who wish to remain consistent with the privacy principles described in Section 10 should avoid requesting the root identity key, use application-specific and transaction-specific derived keys, keep certificates optional, disable unnecessary key-linkage functions and minimize all metadata capable of reconnecting identities with transactions.

The central question is not simply whether BRC-100 supports fresh transaction keys or prevents public derivation of child keys from the identity public key alone. It does both of those things.

The more important question is:

> **Does BRC-100 preserve the firewall between those transaction keys and the user's persistent identity—or does it make crossing that firewall a routine feature of the application ecosystem?**