Quorum Private Transaction

Private Transaction

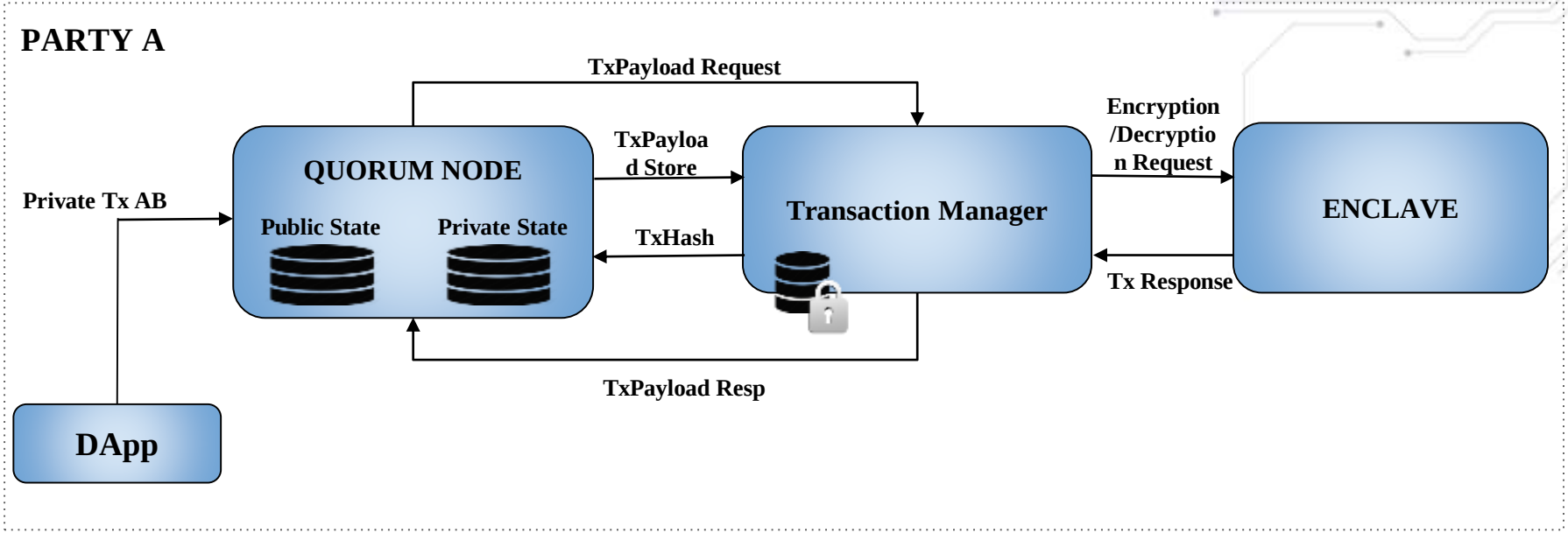
- Private transactions are facilitated through an API revealed to the Dapp that originates the transaction.
- It has a 256-bit hash in the data field.
- Not executed as per the Ethereum standard.
- EVM does not support encryption or decryption operations.

Components of Private Transaction

- **Recipient:** Authorized parties involved in the transaction, beneficiary of the assets.
- **Transaction Payload:** Contains the hash of the transaction data and the encrypted public key of the parties that are involved in the transactions.
- **Signer List:** Contains the sign of all the participants of a transaction.
- **An optional data field:** A 256-bit hash for a private transaction.
- **PrivateFor List:** A list of public keys that identify the parties involved in the transaction and identifies the transaction as private or not.

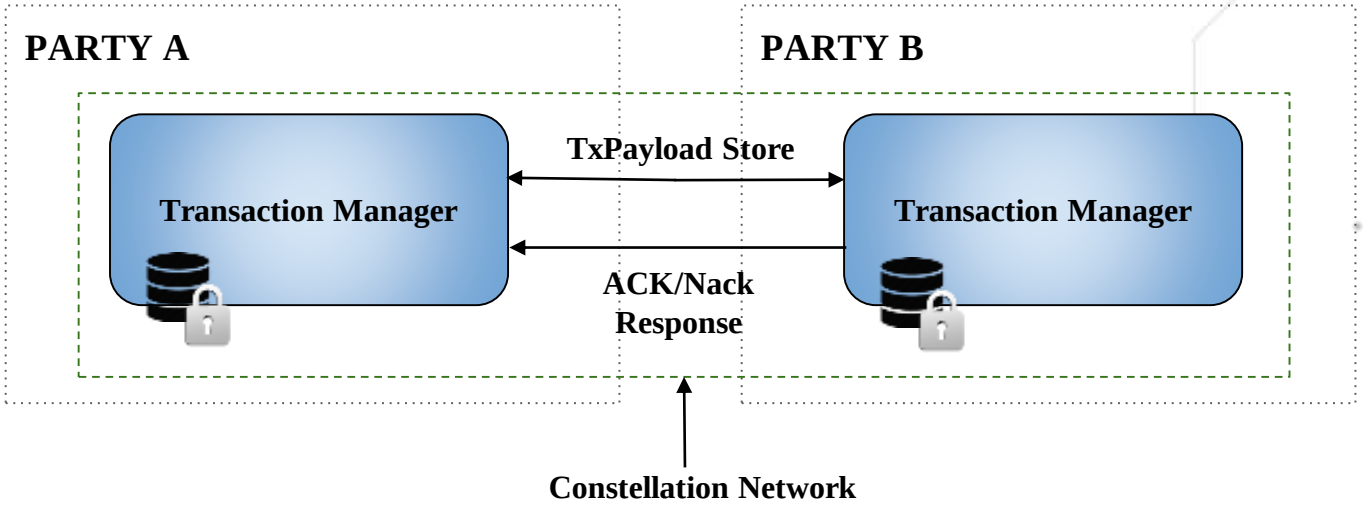
How a Private Transaction is Committed?

A. Transaction creation by the sender party.



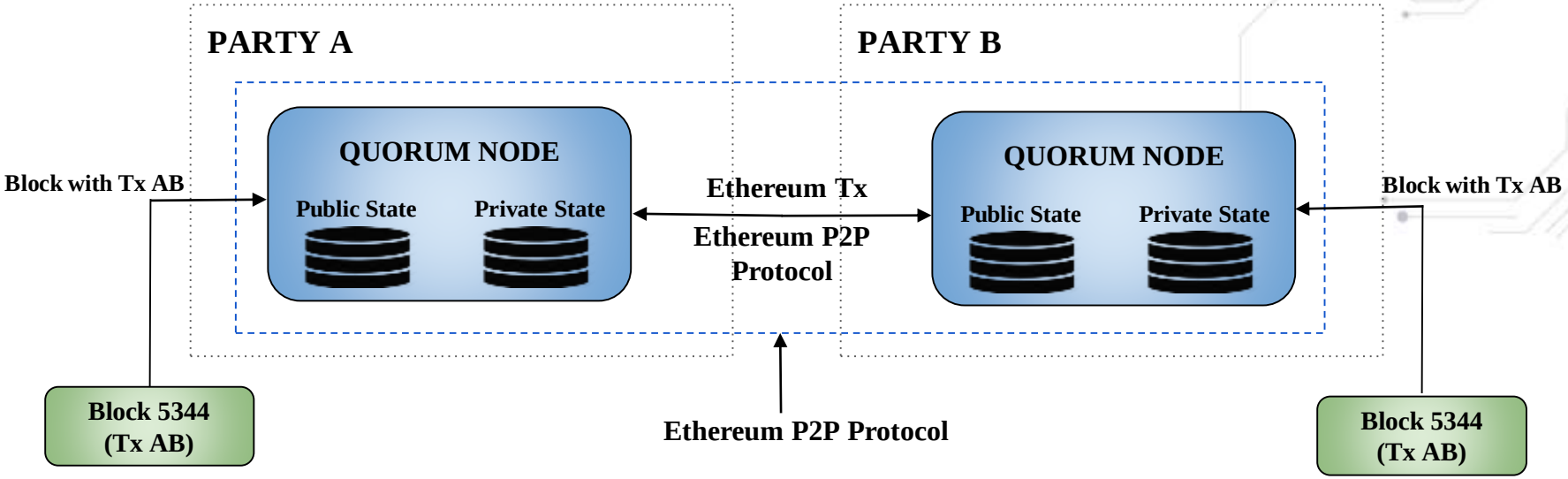
How a Private Transaction is Committed?

B. Transaction Manager of the sender party sends the encrypted transaction data to the Transaction Manager of the receiving party.



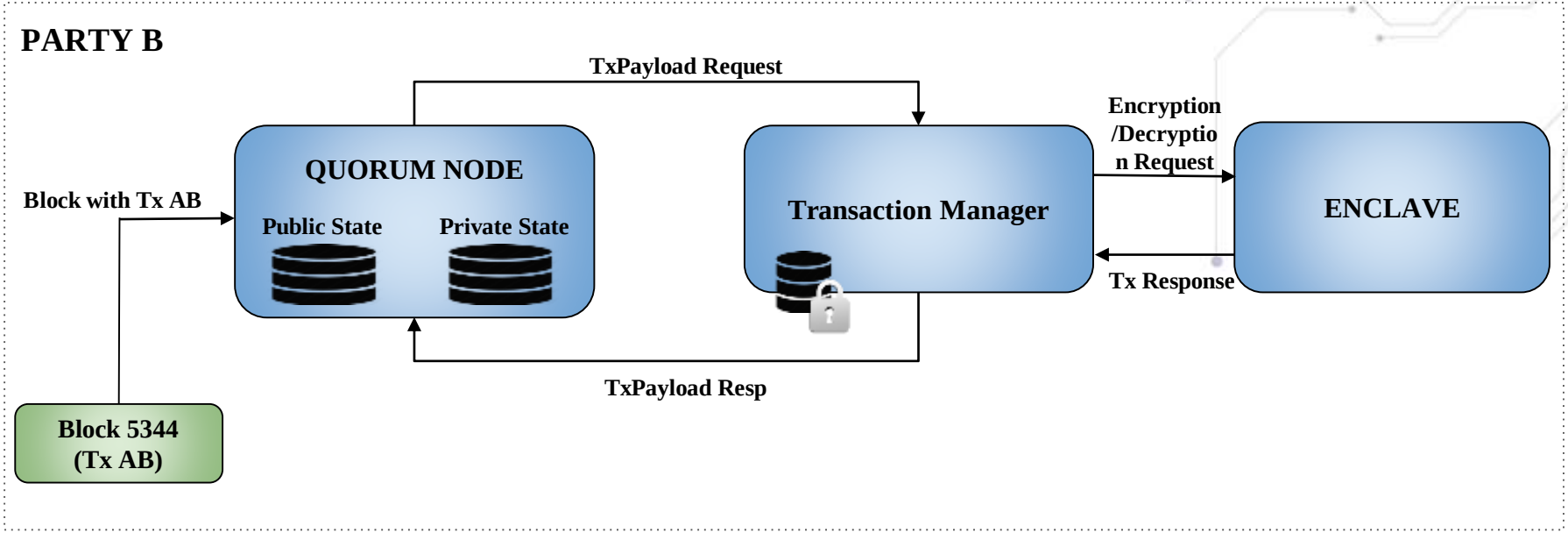
How a Private Transaction is Committed?

C. Transaction is propagated to the rest of the network using the standard Ethereum P2P Protocol.



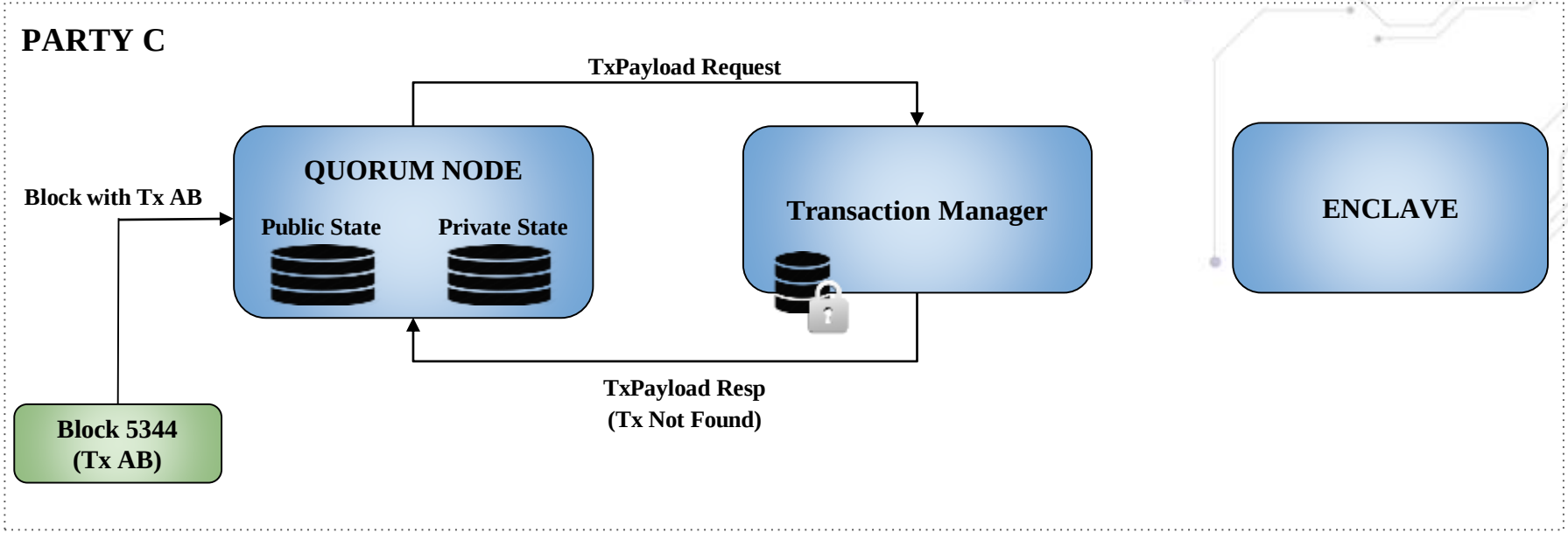
How a Private Transaction is Committed?

D. The Receiver Node makes a call to their local Transaction Manager to determine if they hold the transaction.



How a Private Transaction is Committed?

E. Other nodes make a call to their local Transaction Manager to determine if they hold the transaction.



THANK YOU!

Any questions?

You can mail us at

hello@blockchain-council.org