Transaction Malleability

Transaction Malleability Explained

By **Bisola Asolo** - October 30, 2018

Transaction Malleability Explained

Last Updated: 30th October 2018

Transaction malleability is the process of changing the unique identifier of a transaction by first changing the digital signature used to create it.

Commonly associated with Bitcoin, a transaction identifier (Tx id) is a unique 32-byte alphanumerical string of data that is used to reference a bitcoin transaction. The transaction identifier is formed by hashing **transaction data** through the SHA-256 hash function twice. That is:

$$\text{Tx id} = \text{SHA-256}(\text{SHA-256}(\text{Transaction data}))$$

The transaction data which is put through the SHA-256 function is composed of the following:

- Transaction Hash – Reference to the transaction containing the UTXO being spent
- Output Index – The index number of the UTXO being spent
- Unlocking Script – Script that satisfies conditions of the locking script
- Unlocking Script Size – Size of the unlocking script in bytes
- Sequence Number

All the data is serialized, i.e. it is translated into a format that can be more easily stored and transmitted across a network, and then put through the SHA-256 function twice to yield the transaction id.

What Makes Transaction Malleability Possible

Transaction malleability is made possible because the **unlocking script**, or scriptSig, containing the digital signature can be modified by an attacker. If the unlocking script is changed, the serialized transaction data will be different, therefore, the resulting transaction id will also be different. However, a bad actor can only alter the digital signature of the unlocking script prior to the confirmation of a block. After confirmation, the digital signature, and therefore the transaction id, are immutable.

To illustrate how a transaction malleability attack may be performed, consider the following:

Alice sends 1 bitcoin to Bob with a Tx id ***A***. However, before the transaction is confirmed, Bob alters the signature data of the transaction to produce a new Tx id ***B***. Having received the 1 bitcoin but with Tx id ***B***, Bob then informs Alice that he has not received the bitcoin. When Alice searches a block explorer using Tx id ***A*** to confirm Bob's claim, she cannot find the transaction. Assuming a failed transaction and that the 1 bitcoin was never sent, Alice sends Bob another bitcoin, resulting in a total of 2 bitcoins being sent to Bob.

Transaction malleability attacks have however been mitigated on the Bitcoin network via the implementation of a soft fork protocol upgrade known as Segregated Witness, or SegWit.

Segregated Witness

With the implementation of SegWit, the signature data in the unlocking script is moved and omitted when calculating the Tx id of the transaction data. The result of this is, if a bad actor modifies the signature data, the Tx id will remain exactly the same.

SegWit was successfully activated on the Bitcoin network on 21st July 2017.

Transaction Malleability & Mt Gox

Former cryptocurrency exchange, Mt Gox, released a statement on February 10th 2014, claiming transaction malleability as the reason why it was preventing customers from withdrawing funds. Bad actors had been using this exploit to steal funds from the crypto-exchange, an attack which eventually resulted in its insolvency.

Conclusion

To conclude, transaction malleability is an exploit that allows a bad actor to potentially acquire more of a cryptocurrency by changing the signature data in the unlocking script; an action which also results in a different transaction id.

Segregated Witness, or SegWit, is soft fork implementation upgrade that solves the issue of transaction malleability by moving and omitting the digital signature in the calculation of the transaction id.

Mt Gox is a famous example of how the transaction malleability exploit was used to steal bitcoins, an attack that eventually resulted in the insolvency of the cryptocurrency exchange.

TAGS Bitcoin Transaction Malleability

ABOUT US

FOLLOW US