Lance Aaron See
CSCI 531 – Sp 2018 – Den Project
What if Bitcoin used SHA1 instead of SHA256?

Introduction:

SHA1 was recently broken by researchers at Google and CWI Amsterdam via a collision attack. With cryptocurrencies such as bitcoin relying on hashes such as SHA256, it is beneficial to observe the effect that this attack would have if bitcoin had relied on SHA1 instead.

Background:

There are various attacks on hashes such as first and second preimage attacks, which are a bigger threat to bitcoin, but since existing attacks on SHA1 are mainly based on collision attacks, this paper will only focus on those. Collision attacks occur due to the nature of hashes: since the output size is fixed, there is a chance that two different inputs can eventually lead to the same hash result. The collision attack on SHA1 showed that an efficient algorithm was able to find a collision with significantly less work than brute force techniques.

SHA256 is used in two primary locations in bitcoin: in the main hash and in the address hash. The main hash is implemented by applying SHA256 twice (H(H(n)), and is mainly used for the proof of work calculations that occur during mining operations, where miners try to find a nonce that will fit into a certain format when hashed. The double hashing adds some collision resistance to the main hash. The main hash is also used by signatures, as signatures occur on messages that have been hashed by the main hash. In the address hash, SHA256 is used in conjunction with the RIPEMD160 hash to determine addresses for both withdrawals and deposits.

Effects of Collisions on Bitcoin:

If SHA1 was used in place of SHA256 in bitcoin, the resulting successful collision attacks would have minor effects on the main hash. Similar to when two miners solve the proof of work problem at the same time, a fork would be created, which theoretically could allow a user to double spend his/her funds. However, this would mostly be resolved since transactions are usually take at least 6 blocks before being confirmed, and by then, consensus will have been arrived at, with the longest chain considered legitimate. In addition, a collision attack would affect signatures by allowing adversaries to possibly steal or destroy coins. In essence, an attacker would first generate a signature for a normal transaction, and use the signature to send a signed malicious transaction[1]. Since the two transactions would result in the same hash digest in a successful collision attack, the malicious transaction would also be properly signed.

The effects of collisions on the address hash are more subdued due to the use of two different hash functions, and since an adversary would only be able to access the public keys but not the private keys[1]. Essentially, a collision attack on the address hash would allow for an adversary to claim that their coins were stolen. The adversary would present another preimage key that was used to sign a transaction as proof[1].

Due to the structure of how hashes are used in bitcoin as well as the cost of executing the SHA1 collision attack, the use of SHA1 would not be extremely detrimental to bitcoin. The issues with the SHA hash breaking only amount to catastrophic levels when preimage or second preimage breaking of the algorithm occurs (this has still not occurred for SHA1). In these cases, one could steal coins and cause the possible failure of the blockchain. A failure of digital signatures (ECDSA) or RIPEMD160 in conjunction with a failure of SHA256 would also result in catastrophic failure of the blockchain, allowing adversaries to steal coins, change existing payments, and double spend coins.

1. On Bitcoin Security in the Presence of Broken. Cryptographic Primitives. Ilias Giechaskiel, Cas Cremers, Kasper B. Rasmussen. 21st European Symposium on Research in Computer Security(ESORICS),. Heraklion, Crete, Greece, Sep. 2016.