documentation on that, but I trust him). That's 16 out of 2^256, so not a huge deal, but still.

Bitcoin Calculator | Scallion | GPG Key | WoT Rating | 1QGacAtYA7E8V3BAiM7sgvLg7PZHk5WnYc

theymos
Administrator
Legendary

Activity: 5544
Merit: 14203

Re: Dealing with SHA-256 Collisions
June 14, 2010, 06:09:58 AM #5

> **Quote from: lachesis**
> Wouldn't all the old transactions then be compromised (because they could be trivially recomputed)?

After thinking about this some more, I've realized that breaking the hash function used in blocks would be more disastrous than I had originally thought. But it should still be possible to change the hash function "on-the-fly" by including secure hashes of each real block in the old chain with the new BitCoin release. Some mechanism of doing this (hopefully more elegant) would also have to be used for a gradual hash change.

> **Quote from: Xunie**
> Wouldn't the users lose their coins?

Everyone's balance is publicly available, so it should always be possible to preserve this data, no matter what changes are made to BitCoin.

1NXYoJ5xU91Jp83XfVMHwwTUyZFK64BoAD

satoshi
Founder
Sr. Member

Activity: 364
Merit: 7750

Re: Dealing with SHA-256 Collisions
June 14, 2010, 08:39:50 PM #6
Merited by Raja_MBZ (3), ABCbits (2), vapourminer (1), bitcoinPsycho (1), vjudeu (1), livecoins (1)

SHA-256 is very strong. It's not like the incremental step from MD5 to SHA1. It can last several decades unless there's some massive breakthrough attack.

If SHA-256 became completely broken, I think we could come to some agreement about what the honest block chain was before the trouble started, lock that in and continue from there with a new hash function.

If the hash breakdown came gradually, we could transition to a new hash in an orderly way. The software would be programmed to start using a new hash after a certain block number. Everyone would have to upgrade by that time. The software could save the new hash of all the old blocks to make sure a different block with the same old hash can't be used.

EricJ2190
Full Member

Activity: 134
Merit: 102

Re: Dealing with SHA-256 Collisions
July 19, 2010, 12:44:17 AM #7

> **Quote from: lachesis on June 14, 2010, 01:01:11 AM**
> A mathematician friend of mine pointed out that there are very few if any hash protocols that have survived for 10 years or more. What would Bitcoin's solution be if SHA256 were to be cracked tomorrow?

SHA-1 lasted over ten years before being significantly weakened. Now, even 15 years in, full SHA-1 still has no known collisions. RIPEMD-160 has also held up for over ten years, as has GOST, Tiger, and probably others.

Cdecker
Hero Member

Activity: 489
Merit: 505

Re: Dealing with SHA-256 Collisions
July 27, 2010, 09:02:22 PM #8

As I understood it the Hash algorithms that are used are completely replacable, and should the demise of SHA-256 become apparent we could switch to another Hashing algorithm, starting a new chain, and users would buy that new currency with their old coins, creating an inflation of the old coins and creating request for the new version, just like creating new services that rely on BC does now.

I don't think moving to a new version would be hard