GoldCoin
The Gold Standard of Digital Currency

Version 0.7

www.gldcoin.com | www.gldtalk.org | October 11 2013

GoldCoin Patch Announcement

Welcome to the GoldCoin minor version 7 announcement. We have some fantastic news for you folks today. We have at last solved the greatest problem having to do with crypto-currency, 51% network ownership, whilst keeping standard proof of work!

The more people update to this version the less vulnerable to 51% attacks we are. Therefore this is a mandatory update.

What is a 51% attack

In a nut shell, a 51% attacker controls the majority of the network's mining power, and since the network automatically chooses the longest blockchain to be the correct one, this gives the attacker control over transactions. This allows them to repeatedly spend the SAME coins on an exchange over and over again.

A 51% attack is a fundamental problem with all proof of work coins that has existed up until today. Even Bitcoin has not managed to solve this problem. No more will there be multi-mining-pools that simply mine a coin while the difficulty is low and thereafter immediately dump, and no more fear from hash-power attacks because of some server farm!

The impossible made possible

We've been told over and over again, almost to the point of being brainwashed, that there is no solution to the 51% problem with coins that use the proof of work system(Ie: GoldCoin, LiteCoin, BitCoin). That changes today, you may wonder how -but do not fret, everything will be explained below in great detail.

This is a soft forking update. this minor version will be dictating the blockchain regardless of greater lengths in lower versions. However the older versions are forward compatible with this one as long as they remain on the same chain. As of this release we are the only coin to date that can claim resistance to 51% attacks, and post block 100,000 we can claim virtual immunity from them!

CRYP2NOVA



"For the longest time the crypto-coin community had to deal with cyber-bullies getting in the way of innovation, -not anymore though with GoldCoin…"

- GoldCoin Dev Team

Archived copy · cryp2nova.com

How a 51% Attack Works

To understand how our defense works, you must first understand how a standard 51% attack occurs. When an individual, company or group wish to profit unethically or if they simply wish to destroy a coin, they will do something similar to the following. (The most common and profitable form of 51% is listed below)

Consider the following:

GLD Network hashrate is : 100Mh/s
Attacker's mining hashrate is: 300Mh/s

GLD blockchain is at block 7000.

The attacker has 100,000 GLD in his wallet.

Step 1:

The attacker starts his mining rig at home on a separate local chain only he has access to at block 7000.

Step 2:

The attacker transfers 100,000 GoldCoins to an exchange, for the purposes of this example we will use Cryptsy. It is included in block 7001 on the main GoldCoin blockchain.

Step 3:

The attacker waits for 6 confirms, the coins confirm on Cryptsy and are added to his virtual balance.

The main GoldCoin blockchain is at block 7007.

Step 4:

The attacker now spends his balance and converts it to Bitcoin and transfers it to a cooling off address.

The main GoldCoin blockchain is at block 7007.

The attackers private blockchain is at block 7014.

Step 5:

The attacker broadcasts his blockchain to the world.

Step 6:

GoldCoin clients all around the world switch to his blockchain because it is longer.

The initial transaction the user made to Cryptsy never happened in this chain, the attacker now has both his GoldCoins and the Bitcoins he traded them for initially (essentially twice what he had initially).

Step 7:

If the attacker wishes, he will repeat again, starting at block 7014.

The coin has now lost a great deal of its buy support, faith in the coin is lost and users leave for another coin.



Archived copy · cryp2nova.com

51% attack in diagrams

Lets assume that this is the network prior to the 51% attack, with the attacker in red, ordinary GoldCoin users in gold, and the exchange in green.



This is what happens after the attack, the clients switch to the attacker's blockchain and the exchange is left with worthless coins sent to it by the attacker that will never confirm. Purple meaning users of a bad chain, and pink meaning double spending victim.



Archived copy · cryp2nova.com

How GLD's 51% defense system works

Here is how our revolutionary 51% defense system works:

It is based on a few simple facts,

Fact 1:
A block requires 6 confirms on an exchange before being fully confirmed.

Fact 2:
All blocks have timestamps that are universally convertible.

Fact 3:
Building and communicating a blockchain across multiple peers, with each peer holding a separate chunk of the blockchain is difficult. (also works in this case)

Fact 4:
An attacker must outrace the network's main chain in order to be successful.

Knowing this, our main developer (akumaburn) came up with a few simple laws or precautions clients could take to ensure a 51% attack fails to propagate to > 99% of the network (depending on total number of nodes). **In fact it grows exponentially more difficult for the attacker to spread his chain to more nodes as the number of nodes he has spread his chain to grows.**

Law 1:
No one peer may transmit more than 5 blocks every 10 minutes, regardless of their origin.

Law 2:
A clause to the first law is if the block number is less than 100,000. If so, then permit blocks to be transmitted faster if and only if, those block's have timestamps that is not within 10 minutes of the current system time.

Law 3:
Another clause to the first and second laws is if the last block transmitted has a timestamp that is not within 2 minutes of current time permit it anyhow, unless we are past block 100,000.



CRYP2NOVA

GoldCoin Development Group

Official Website

www.gldcoin.com
contact@gldcoin.com

Official Forum

www.gldtalk.org
contact@gldtalk.org

Archived copy · cryp2nova.com

Defense Scenario

Now that you understand how a 51% attack works, lets go over the same scenario above:

Consider the following:

GLD Network hashrate is : 100Mh/s
Attacker's mining hashrate is: 300Mh/s

GLD blockchain is at block 7000.

The attacker has 100,000 GLD in his wallet.

Step 1:

The attacker starts his mining rig at home on a separate local chain only he has access to at block 7000.

Step 2:

The attacker transfers 100,000 GoldCoins to an exchange, for the purposes of this example we will use Cryptsy. It is included in block 7001 on the main GoldCoin blockchain.

Step 3:

The attacker waits for 6 confirms, the coins confirm on Cryptsy and are added to his virtual balance.

The main GoldCoin blockchain is at block 7007.

Step 4:

The attacker now spends his balance and converts it to Bitcoin and transfers it to a cooling off address.

The main GoldCoin blockchain is at block 7007.

The attackers private blockchain is at block 7014.

Step 5:

The attacker broadcasts his blockchain to the world.

Step 6:

GoldCoin clients all around the world switch to his chain, download 5 blocks, notice the 51% attack is occurring and ban the peer - leaving them with 7005 blocks, of which 5 are bad and delay the next block transmission for two minutes(locally).

Step 7:

To the attacker's demise, the very system that allowed his attack to take place will also cancel it out. Since the main GoldCoin blockchain is at block 7007 or more, the affected nodes that were directly connected to attacker will now switch back to the main chain.

The end result?
The attacker has accomplished nothing except slightly lagging the nodes it was directly connected to.
This defense becomes stronger and stronger the more nodes there are on the network running this client version. (soon this version will become the protocol minimum)

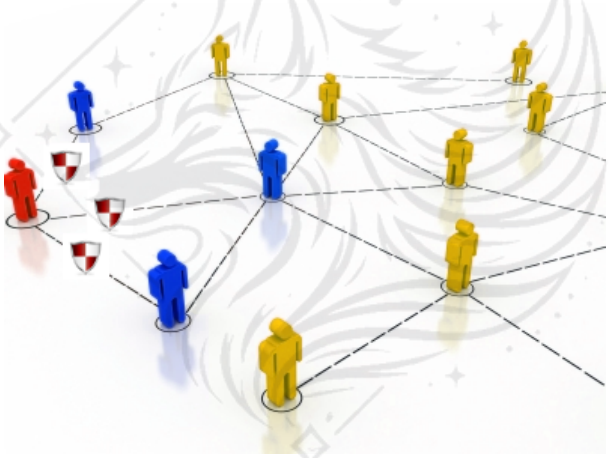
Archived copy · cryp2nova.com

51% defense in diagrams

Lets assume that this is the network prior to the 51% attack, with the attacker in red, ordinary GoldCoin users in gold, and the exchange in green.



This is what happens during the attack. Blue meaning users that have had their 51% defense triggered.



This is what happens after the attack, the clients switch back to the main chain and leave the 51%er banned and checkpoint the main chain ahead of his chain.



Archived copy · cryp2nova.com