International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Cryptocurrency: Failure's and Ways to Deal it

Shreya D. Poojary, Swastika A. Singh
ASM's Institute of Management and Computer Studies (IMCOST),
Thane, Mumbai, Maharashtra, India

ABSTRACT
The Crypto currency is a digital currency, it is created managed through the use of advanced encryption techniques known as cryptography. In 2009 the Bit coin software made available to the public for the first time. In April 2013 it captured significant investor and media attention. Their flow is determined entirely by market demand and they are not controlled or regulated by some singular authority. Crypto currencies were designed as decentralized systems because it lack a central authority to mediate transactions. In Bit coin if you had invested just $1,000 in first year, now you would be richer to the tune of $16,000.

Now you don't want to wake up one day and find that someone hacked your machine and took off with $10,000 of your hard-earned money. Cryptocurrencies are decentralized. Making everyone's life nightmare because there is no middle men, no centralized "trusted" entity.

But with great power comes great responsibility. There's nobody to call to get your money back. You can't dispute the transaction. There's nobody to reset your password if you forget it.

This Paper is mostly about dealing with a technical failure in a block chain by using the governance layer.

INTRODUCTION

In crypto currency there are many ways that a block chain can fail. It's good to think about what kind of failure looks like in block chain let us see 1) how poor it might be, 2) how to recover from failure 3) how to deal with failure.

Knowing how it is possible to recover and what things can fail. I feel like it's generally important as a life lesson, but here is some more economic example: If you're buying insurance, you will be willing to pay more if you have more fear of the outcome being prevented.

Two classes of failure's in crypto currency:
1. Governance Failures.
2. Technical Failures.

How can a block chain fail?
The block chain can have many kinds of technical failures. The failures are not necessarily exhaustive:

1. Reversion blocks expected to be consensus.
2. Consensus occur on invalid blocks.
3. Unavailability of consensus occurs on new blocks.
4. Censorship of transactions/blocks.
5. Unavailability of block.

1. Reversion of consensus blocks (51% double spend)

In Block chain, Reversion of blocks "51% double-spend attack".

Imagine: After waiting for more than 5(or 100) confirmations, your transaction which has been confirmed becomes unconfirmed.

This is normally understood that the result of an attack with majority of hash rate* because the only way in proof-of-work to reverse a block is to present a heavier chain without that block.
*Technical note: Due to network asynchrony it can also occur.

Recovery method:
In a block chain, the protocol is that nodes which always choose with the most proof-of-work block chain. The story is that the less official side of light clients and even full nodes have check pointing.

If there would be a large number of blocks are reverted, then may be the damage would be high and that it justifies attempting to improve the original block chain's transaction history.

If there would be a small number of blocks are reverted, then may be the cost was not too high and the network won't mind the reversion.

Preventive measures
Recovering a reversion attack which requires the governance layer, there will be *always a* more honest hash power than malicious hash power, that it make sure that the longest chain keeps growing. Not even once for a few days there should be more malicious hash power than honest power, to completely prevent 51% attacks!

CONCLUSION:
It is easy to prevent a reversion attack to consensus on which chain came first if the community governing the block chain. And it is easy to alleviate with non-reversion rules. 51% attacks are only very frightening if you cannot rely on the governance layer to damages.

It seems that to recover and to prevent one from a reversion attack it would likely be more efficient, particularly with well-financed adversaries and low governance costs.

2. Consensus on invalid blocks
Consensus on invalid blocks is a failure mode wherein the heaviest fork incorporates invalid blocks.

Recovery method:
If the community uses enough full nodes to provide enough offerings, then there will be a monetary incentive for the miners to mine on a sequence this is frequent by way of full nodes. This incentive ought to be high sufficient for miners not to willingly and knowingly mine on an invalid block chain. Its miles up to the governance layer to make sure that that is the case—if it fails, then we can also see consensus on invalid blocks. Light customers do now not validate blocks, and so have to be helped greater-protocol. This could be carried out with checkpoints. However, the best issue to is for the governance layer to cause miners to produce a legitimate longest chain.

Preventive measures
The governance layer has to make sure that miners have enough incentive to mine best on valid blocks. the very best way for it to do that is to orphan invalid blocks through using full nodes to discriminate between legitimate and invalid blocks (being orphaned could be very costly, for miners).It manage be realistically unthinkable to discourage 100% of miners from overmuch mining distorted blocks, yet this perhaps a action where recovery right to useful all over but the shouting node behavior is as good as prevention.

CONCLUSION:
Consensus on invalid blocks ought to be avoided and recovered from by means of network's use of complete nodes which validate blocks. The overall nodes will no longer synchronize with the invalid heaviest chain, and need to offer sufficient incentive to miners to go back to mining on a legitimate chain. The governance layer should do its exceptional to hold light clients secure, at some stage in the complete manner.

3. Unavailability of consensus on new blocks
Unavailability of consensus on new blocks is a technical failure wherein consensus on new blocks does now not shape.

This may be because no new blocks are mined (issue too high, possibly), or due to the fact no one can mine on pinnacle of the longest chain (network asynchrony, perhaps).

Recovery method:
Since proof-of-work can't "get caught" (you can constantly upload a block to a sequence, if you can mine it), it is difficult in practice for an attacker to make sure that nodes are seeing wonderful heaviest chains. The answer right here is straightforward:

The governance layer has to make sure that there's sufficient mining power mining on the same chain, and that the chain is being propagated to clients (that blocks are being discovered, and being propagated rapid/well enough to permit them to be chained).

Preventive measures

The governance layer has to ensure that miners are properly related to each different and to the network of full nodes to prevent the unavailability of latest blocks, and additionally to make certain that the miners do now not all fail en-mass, in order that we may also a developing Block chain.

CONCLUSION:

Proof-of-work block chains have a relatively simple liveness story. As conceive as the longest chain is getting longer, and everyone someday sees entire is the longest handcuff, earlier there is common consent on new blocks. As by all of the "invalid blocks" flaw, prevention and recovery mechanisms are the same: making solid that there is enough above suspicion hash power on a well-enough-connected network.

.

4. Censorship of transactions/blocks

In this assault, we are able to consider that a majority coalition of miners conforms to most effective mine on chains that either don't include blacklisted transactions or only consist of white listed transactions. which method that blocks from miners who are not hereafter this practice are as orphaned, so there may be a large incentive for non-censoring miners to add one name to up for the censoring coalition.

Recovery method:

The first issue that desires to take place to reverse censorship is to understand that censorship is taking place. This will be non-trivial if the mempool is complete and the transactions suspected to be being censored have low prices. But, it has to be feasible to detect censorship of transactions with high fees (if the network isn't too asynchronous).

After censorship is detected, the governance layer needs to decide on a course of movement: make certain that a majority coalition which does not censor takes energy, or do not anything and be given the censorship (wait it out, perhaps).

If a majority coalition doesn't censor, then miners who refuse to mine on blocks who don't observe the censorship coverage will have their blocks orphaned. If a majority does censor, then miners who are not following this approach are having their blocks orphaned.

There are profuse ways that the governance protect bouncecel act making strong that there is a non-censoring age of consent coalition. They can add above suspicion hash power to the network. They can have brought pressure to bear or money existing miners to discourage censoring. They can when push comes to shove the hashing algorithm in a fashion that obsoletes ASICs, in a stake to figure it easier to depose the censoring cartel.

Preventive measures

To save you censorship, the governance layer desires to assure that no majority coalition will ever form and choose to censor transactions/blocks.

CONCLUSION:

Reversing censorship requires that the day care protect bust the censoring cartel. Preventing censorship requires that the governance layer prevent censoring cartels from forming. This can manifest in a couple of ways and isn't always guaranteed to be easy, however is the most effective manner to prevent and get over censorship attacks.

5. Block unavailability

Block unavailability is a lack mode where the heaviest block chain has blocks which are not available. An unavailable block is scary because we don't realize whether or not an unavailable block is legitimate.

Recovery method:

Protocol-following complete nodes will reject forks containing unavailable blocks, and will stay on a fork with available blocks.

If the community uses enough full nodes to offer enough offerings, then there might be a financial incentive for the miners to mine on a series that is prevalent by means of complete nodes. This incentive ought to be high sufficient for miners no longer to willingly and knowingly mine on an unavailable block chain. Its miles as much as the governance layer to make sure that that is the case—if it fails, then we may additionally see consensus on unavailable blocks.

Mild customers do no longer make certain that blocks are available, and so ought to be helped more-protocol. This may be carried out with checkpoints. But, the proper aspect to is for the governance layer

to purpose miners to supply a legitimate longest chain.

Preventive measures

The governance layer has to make sure that miners have enough incentive to mine handiest on to be had blocks. The perfect manner for it to do this is to orphan unavailable blocks.

CONCLUSION:

Consensus on unavailable blocks in a POW block chain ought to be averted by the governance layer thru using complete nodes which validate the supply of blocks. The entire nodes will not synchronize with the unavailable heaviest chain, and need to provide enough incentive to miners to go back to mining on an available chain. The governance layer has to do it's nice to maintain light customers safe, throughout the whole manner.

References

1. Canis, B. (2015). Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry Washington: Congressional Research Office.
2. Carvalho, S. (2015, February 24). Firms see drone sales in Gulf surging after U.S. eases export policy. Retrieved from Reuters.com:http://www.reuters.com/article/2015/02/24/
3. mideastusa-drones-idUSL5N0VY2GU20150224 Brennan, C., & Lunn, W. (2016, August 3). Blockchain. Retrieved from Finextra: https://www.finextra.com/finextra-downloads/newsdocs/document-1063851711.pdf
4. Clancy, T. (2016, January 20). Ecommerce at Large Coming Around to the Idea of Bitcoin. Retrieved from Cryptocoins News: https://www.cryptocoinsnews.com/ecommerce-atlarge-coming-around-to-the-idea-of-bitcoin/
5. CNBC. (2015). The top Hispanic entrepreneurs in America. Retrieved from CNBC: http://www.cnbc.com/2015/05/01/the-top-hispanic-entrepreneurs-in-america.html?slide=8