Mining major update.

<u>This major update of the mining system is not mandatory, current mining system « Exact Share system» remain functional and not impact old solo miners.</u>

I. Description of the « Exact Share » System of Xiropht:

Current mining system « Exact Share », require to found the every informations who provide the same block hash indication displayed on the current Blocktemplate and to respect mandatory static rules.

<u>Static rules :</u>
→ Never use numbers outside the range provided by the blocktemplate.
→ Never encrypt math calculations who provide a results outside the range or with results who contains floating points.
→ Respect the current mining method of encryption provided by the network.
→ Every informations inside your share to attempt to found the block need to be exact.

To found the current block, the Exact Share require informations equals of what the Blockchain expect.

He require :

→ To found the exact math calculation.
→ To found the exact result of the math calculation.
→ To encrypt propertly the math calculation with the current block encryption key and the current mining method.
→ And then once the hash of the encrypted math calculation is generated, the hash need to be equals of the Block Hash Indication of the Blocktemplate before to be sent to the network.

Bad :

→ Unfortunatly, this system can't provide any kind of pool supports. That is why I want to present a system who reuse the « Exact Share » system to provide a pool support.

Good :
→ Very resistant against ASIC's and dynamic.

II. Description of the « PoW » Share System of Xiropht :

To provide a pool support and keep every advantages of the current mining system, the new system will use shares who are not exact of the Block Indication by using a different process to generate a difficulty value of this share.

The new system is similar of Cryptonight, but require the « Exact Share » share system to work and also the current mining method of encryption.
Their is few mandatory rules on this system :

→ Nonce range 0 to 2,1 billions. Note : that's permit to provide to reuse 2,1 billions times the same share to try to generate a better difficulty share value, until the current block is found or renewed, by restart the same process with a different nonce at the start of the process. Fortunatly by using this techniques the amount of efforts will be the same comparing to use another share with a different nonce one by one. Their is more luck to use a new share to proceed instead to use the same one.

→ 32 bytes of the manipulated by nonce of the hash target (Block hash indication) + 32 bytes of the encrypted share used.

→ A mandatory AES encryption who use the current mining encryption with the current block encryption key.

→ After encryption, manipulate it by the current nonce again.

→ Use math result calculation and each math numbers arguments of the math calculation used to obtain the encypted share used on the « Exact Share » system process to compare each bytes of the block hash indication manipulated by nonce get their equality, depending that, the difficulty share is incremented or decremented.

→ The blockchain accept only a share with a PoW Value equals of the current network difficulty with a maximu of it 100,000000001%.

→ Pools should accept only job difficulty share equals of the job difficulty target. Example a miner sent a share difficulty of 1200, but he target a job difficulty of 1000, to ensure his work and his accuracy, this is better to accept only accurate difficulty share. Pool providers will decide. Of course if the difficulty share is what expect the blockchain, they should accept them.

Pow Setting : https://github.com/XIROPHT/Xiropht-Connector-All/blob/master/Xiropht-Connector-All/Mining/ClassPowSetting.cs

Algo Mining class example: https://github.com/XIROPHT/Xiropht-Mining-Pool/blob/master/Xiropht-Mining-Pool/Mining/ClassAlgoMining.cs

Check Share function example (pools) : https://github.com/XIROPHT/Xiropht-Mining-Pool/blob/master/Xiropht-Mining-Pool/Mining/ClassMiningPool.cs#L475

This mining method need to be approbated before to be fully spread on the network.