Guang (光) Coin White Paper

1 Introduction

The development field of cryptocurrencies is rapidly evolving, in many directions. Whilst some of these evolutions use the blockchain as a consensus database of information other than value exchange (coins) as their main innovation, and some innovate very little, there are a number of *altcoins* which exist to push fundamental developments in cryptocurrency in various directions.

Particularly, now, it has become popular for coins to advertise their resistance to attacks from Quantum Computers - either due to the complexity of their underlying consensus structure (IOTA's[1] DAG-based Tangle for example), or via fundamental replacement of underlying cryptographic libraries (QRL's[2] Merkle tree construction for one-time signatures).

Many of these coins, however, throw away useful features of the existing blockchain development base, in producing an *ab initio* codebase with the new features inbuilt. Most of these coins also do away with Proof of Work schemes, replacing them with the newly-popular Proof of Stake approaches, which have uncertain security, and are potentially vulnerable to a number of targeted attacks.

光 coin ("guangcoin") takes a different approach - importing cutting-edge post-Quantum signature schemes, and low energy, Quantum-resistant Proof-of-Work, into a codebase derived from the best existing mature blockchain technologies as a firm foundation.

1.1 Coin Name

The proposed, and implemented, cryptocurrency here is named "光 coin", or "guangcoin". This is a play on words ("光" is a rough equivalent of "light" in Chinese, and we base our currency on the Litecoin codebase), and a statement of intent ("光" also has meanings associated with lustre, as of precious metals, and of honor). Least importantly, but a consideration: hanzi make easy coin logos!

Our suggested exchange symbol is **XGC**.

2 Post-Quantum Signatures

Almost all existing blockchain implementations draw the security of their transaction schemes from Elliptic Curve Cryptography (ECC) signatures, as used by the original Bitcoin[3]. Whilst ECC schemes are currently secure against attack by random oracles (ROMs) on non-quantum computers[4], there are attacks from Quantum computers which have been described[5], and only await the physical hardware to implement them. ECC schemes are also of uncertain security against inspection by Quantum random oracles, or QROMs.

On the existence of suitable hardware - which could be only years away - transactions would become significantly more vulnerable to spoofing, and private key derivation would be feasible for a determined attacker, undermining the security of all future transactions.

Therefore, any modern cryptocurrency must consider adopting transaction signature schemes with proven resistance to QROMs in order to assure its longevity.

2.1 Merkle constructions

One of the oldest known signature schemes - Merkle-Lamport one-time signatures[6][7] - is also provably resistant to attacks from QCs, including inspection by QROMs. The currently-in-development cryptocurrency Quantum Resistant Ledger (QRL) uses such signatures - and their descendants, Merkle-Winternitz[8] - as their key innovation in achieving a secure basis for a modern cryptocurrency.

However, Merkle signature schemes have one specific vulnerability, which renders them less than satisfactory as a signature scheme for a digital currency; they can only sign a limited number of messages. Specifically, the signer must pre-generate a Merkle-tree containing a large number of public/private keypairs. Each keypair can be used to sign precisely one message (one transaction), and must then be discarded. Once the pregenerated set of one-time signing pairs is consumed, an entirely new complete Merkle tree must be constructed.

Obviously, we would prefer to use post-quantum signature schemes which don't impose such a constraint, especially as any form of mining (Proof of Work, Proof of Stake or other) will ambiently consume keypairs through coinbase transactions in newly minted blocks, without any actual economic activity between accounts at all!

2.2 Unruh constructions

Luckily, there are other post-quantum signature schemes which can be proven resistant to QROMs, and do not come with limited signing power.

One such class of schemes are so-called *Unruh transforms*[9], which are specifically constructed to provide QROM-resistance, compared to the analogous and better-known Fiat-Shamir[10] transforms in the classical domain. Both of these approaches require an underlying cryptographic protocol to apply (this protocol is an interactive zero-knowledge (IZK) proof of the private key's existence - the transform converts this to a non-interactive (NIZK) proof suitable for use as a signature), and, for security, this cryptographic protocol must, itself, be QC resistant.

The recent work by Chase, et al[11], on the ZKB++ protocol provides just such a QC-resistant IZK, and demonstrates a fortuitous synergy with the Unruh transformation scheme which makes the resulting NIZK particularly efficient compared to others in its class. The resulting PICNIC algorithm is our choice of signature scheme for 光 coin.

We note at this point that one tradeoff of all post-quantum signature schemes is that signatures are significantly longer than the ECDSA signatures in bitcoin-family transactions. We address one approach to countering this later in the paper.

3 Post-Quantum Proofs of Work

The second key element of many cryptocurrencies derived more closely from bitcoin is the Proof of Work system. As well as providing part of the blockchain's sequential security (by confirming the hash of the preceding block, and providing a concept of time-ordering in the chain), the effort needed to solve the Proof of Work function is a fundamental component of the resistance of the blockchain to attacks on that hashing structure. The basic principle of Proof of Work provides that an attacker must do all the work of the chain after the point at which they wish to fraudulently amend the ledger, in the same time that the consensus community performs the single PoW for the next block, which is extremely hard (and asymptotically impossible with the depth of the amended transaction).

There are two issues with Proof of Work, as commonly used in bitcoin-derivatives, one general and one more specific. The general issue is that, by relying on "raw computational power" as the rate-limiting factor, most traditional PoW's also encourage the consumption of large amounts of energy (a negative factor for the future of human civilisation; from waste heat production, even if energy production grows exponentially), and the centralisation of power in specialised compute units (GPUs or ASICs) which are optimised to perform these calculations. The specific issue with many Proofs of Work is that they are simple hash-based searches, which are both easily encoded into ASICs, and are potentially attackable by improved, or postQuantum, search algorithms. (Compare the hashing rate of the entire bitcoin community in 2010, with the hashing power of a single ASIC designed for bitcoin mining in 2017!)

3.1 Why PoW?

Given the general attack on PoW above, you might consider the popular alternative of many modern coins - dropping PoW for Proof of Stake. Proof of Stake[13] schemes do not require that miners solve hard problems in order to successfully mint a new block; instead, they require that each miner "stake" a certain amount of the cryptocurrency in question in order to have a chance of being awarded the "right" to mint a block. (The weighted probability of each miner being awarded the right to mine a given block is proportional, at least, to the amount of cryptocurrency staked, and optionally, on other factors, such as the length of time that the miner has committed those funds for.)

Clearly, Proof of Stake schemes are more power-efficient than PoW schemes, as there is no computational work involved in minting; this also removes any demand for the development of ASICs or other arms-races. PoS schemes also have another benefit, for those who dislike the current popularity of altcoins as traded securities, rather than investments: the requirement to commit a significant chunk of crypto-wealth, via staking, in order to gain additional currency (and the right to participate in consensus), is a clear incentive for coin holders to avoid trading the majority of their coins in anticipation of future gains and influence.

However, the very lack of computational work, which makes PoS “power-efficient”, also makes it more vulnerable to attacks on the blockchain itself. [14]

3.2 Memory-bound PoW

An important realisation is that physical rate-limiting of work can be provided by something other than a limitation in the number of operations per second on a silicon chip. Memory-bound workloads, for example, can provide a limit to the speed at which a calculation can be performed, with a much lower energy cost, either through requiring large amounts of mostly-inactive storage to efficiently store lookup tables (so-called Proof-of-Capacity[15], as used in BURST), or requiring large numbers of memory lookups (memory-latency-bound PoW[16], as implemented in the Cuckoo Cycle PoW, or the Generalised Birthday Problem, as implemented in ZCash’s Equihash[17]).

Both of these approaches leave a CPU substantially idle, as transistor-switching rates have outpaced DRAM latency for almost a decade to date, resulting in much lower energy costs compared to hashing-based PoWs. As a side effect, they naturally also build in a degree of ASIC-resistance, as higher efficiency circuits will still saturate DRAM to the same degree as a general purpose CPU; the same limitations also prevent GPU solutions from being significantly faster. Whilst a Quantum Computer can, potentially, optimise PoW which involve searches via Grover’s algorithm, in practice the effect is only a halving of the number of lookups needed - not the quadratic improvement in other cryptosystems, meaning that such PoW are fairly resilient to disruptive QCs as well.

Of the two models of memory-bound PoW, we believe that memory-latency bound approaches, such as the Cuckoo Cycle PoW, have more stable performance limitations (storage and memory capacity continues to follow a Moore’s Law, whilst DRAM latency is nearly flat), and so we prefer this as a solution. Due to its extremely well-tested implementation, we adopt ZCash’s Equihash (with some tuning of parameters) as our PoW.

3.3 Proof of Burn, inflationary models

A final consideration for mining with PoW is the scaling of the block reward for creating a new block with a successful PoW solution. Bitcoin famously has a limited coin emission, where mining rewards halve at linear intervals for a given difficulty. Whilst this provides a limit to the total currency, and a deflationary model for value, people often forget that the original justification for this approach was to counteract Moore’s Law. (That is: computers should double in performance on linear intervals, so the rewards should also halve, so that the “relative effort” per unit of commodity CPU remains the same.)

We are already in a post-Moore’s-Law world, rendering much of the bitcoin justification on poor footing - and our PoW is specifically based on a physical limitation which has not significantly scaled in a decade - so we can reconsider the benefits of this approach.

One negative aspect of the exponential step-down in mining reward per block is the decreasing incentive for miners to do work - Bitcoin anticipates this, and allows transaction fees to be collected by miners to offset this, introducing another economic tradeoff as transactors are encouraged to spend more in order to ensure their payments happen expeditiously. For Bitcoin Core, transaction fees have grown substantially over time, and it is not clear that there is a sensible equilibrium in sight.

On the other hand, maintaining a constant incentive for miners, by maintaining a flat (or flatt*er*) mining reward, leads to an obvious inflationary effect on the currency. More coins being created dilutes the value of an individual coin as a fraction of the currency marketcap, a feature shared with fiat currencies, and generally disliked by the cryptocurrency community.

3.3.1 Proof of Burn

Proof of Burn[18] has been suggested as one way to provide an equilibrium against inflationary currencies. The Proof-of-Burn model, in general, allows mining/minting of blocks to be “powered” by the provable removal of coins from circulation - essentially, the inverse of a coinbase transaction, sending coins to a *null-address* which cannot correspond to any private key. This is, in effect, a stronger extension of PoS, where the stake can never be unmade. Clearly, the effect of Proof of Burn is strongly deflationary - and, if not countered by a source of coin generation, could eventually result in the complete removal of all coins from the currency.

In combination with a flat coin-emission schedule, however, Proof of Burn systems can produce a static equilibrium, where coins are destroyed at the same rate they are produced.

Whilst the above is sufficient reason to couple Proof of Burn with an existing Proof of Work system, we also note that Proof of Burn has some of the same weaknesses as Proof of Stake, and hence requires a physically-rate-limited process, like PoW, interleaved with it to maintain blockchain security. This is the implementation used in the only widespread adoption of Proof of Burn minting - the Slimcoin codebase, which allows PoW, PoS and PoB blocks to be mined, but with limits on the consecutive blocks mined by non-PoW methods.

We suggest an interleaved PoW/PoB mining mechanism, similar to Slimcoin’s, in which Proof of Burn blocks can only be minted immediately after a Proof of Work block. All coins which have been burned more than 100 blocks previously are eligible to mint a block by Proof of Burn, when a block is eligible for minting, and the selection process is via simulated lottery draw, with entropy generated from the blockchain to allow consensus.

We also implement coin burning on transaction fees; a minimum fraction of the transaction fees for any block (initially small and static, but eventually growing over time, mirroring the tail emission of coins in the mature phase of mining) must be allocated to the burn address (more may be allocated than the minimum by a miner, if they wish to), with the remainder going to the miner as is normal.

4 Post-Terra Chain Consensus

Whilst we’re considering future-proofing of cryptocurrencies, we should not become locked into assuming that just one fundamental change will occur. Disruptive changes often occur in clusters (or not at all), as much as they occur singly.

Other than the imminent emergence of practical Quantum Computing, then, we should consider other disruptive changes to human culture, which would affect blockchain-based currencies. Luckily, most upcoming changes do not fundamentally affect the blockchain (medical advances are irrelevant, for example); however, the growing development, and decreasing cost, of spaceflight does introduce wrinkles into some fundamental assumptions of consensus models.

Bitcoin, and the post-bitcoin blockchain models, are built on the assumption that consensus can be achieved by systems communicating relatively cheaply, and with relatively low-latency. Block-issuance times on the order of tens of seconds to minutes are vastly larger than the latency delays for contributors to the consensus, and so we can assume that all knowledge is evenly spread across the network, and all nodes agree (mostly) on the current time. (This is another way in which PoW helps to stabilise the chain - time in the chain itself is measured in terms of the computational effort needed to perform the Work, not linear time itself).

However, consider a situation in which some nodes in our network are no longer on Earth. Whilst this may seem farfetched, there are active groups developing asteroid mining technologies [19], and (for political reasons, as much as science) NASA[20] and other space agencies [21], and private individuals [22] are actively developing plans to land humans on Mars.

At planetary distances, communications delays become significant once more. The shortest possible round-trip communication delay between Earth and Mars is 6 light minutes at closest approach; the longest is over *40 minutes*, with the average range being in the tens of minutes range. At these kinds of communication delays, consensus mechanisms used in cryptocurrencies tend to become less stable, and prone to forking.

Whilst we could simply use different cryptocurrencies for different local environments, it would be useful if our currency allowed us to cope with these longer time delays in a more natural way.

4.1 Post-Linear Chain Models

An obvious approach to retaining a “cohesive” post-Terra cryptocurrency is to allow the blockchain to become non-linear - less of a chain than a more generalised network, or a Directed Acyclic Graph of some kind. Individual local chains could progress with more rapid local consensus, and less frequently synchronise with the “global” (“universal”?) consensus chain via multiparent joins.

DAG-based extensions to the blockchain are not new; they were first suggested in 2014 [23], and two actively developed implementations of complete “block-DAG” currencies exist - IOTA (mentioned previously), and ByteBall[24]. However, IOTA and Byteball both focus on the “Internet of Things” as their disruptive tech influence, and are considerably more centralised than we would like a blockchain to be.

One potential approach which improves on both IOTA and Byteball is the TETO[25] model for a DAGchain. TETO does not require a centralised authority like the aforementioned cryptocurrencies... but does require a fundamental shift in the nature of blocks. Each block in TETO supports a single transaction, which must be mined by its own sender (proven by signature on proof of work) - and this approach is required to maintain the security of the order of transactions on the DAG.

4.2 Off-chain models

As well as radical changes to the blockchain topology represented by DAG models, there has been considerable research on more conservative modifications to the blockchain which might apply in post-Terra latency regimes.

Methods of improving blockchain efficiency by introducing “subchains”[27], light-weight sequences of smaller “weak blocks” which are absorbed into conventional blocks regularly, providing lower-latency transactions, are at the least controversial end of the spectrum - but are least relevant to us. (At the most controversial is the very DAG-like Jute model[26].)

In the middle of this changes are the currently-controversial-to-Bitcoin “off-chain” transaction approaches - Segregated Witness[28] and Lightning Network[29]. Whilst new to Bitcoin, these approaches have been integrated into other cryptocurrencies - notably Litecoin[30] - for some time. In particular, Lightning Network transactions essentially act outside of the blockchain itself, with penalty-enforced transaction negotiations occurring via any external means that the negotating parties agree - the final result of the transactions as resolved is all that is recorded into the chain. A key benefit of Lightning Network transactions is that they limit the amount of data needed to be stored on-chain, a particular benefit to post-Quantum transaction signatures, which are larger than the less-provably-secure ECDSA signatures used in the Bitcoin family.

We, therefore, adopt and support Lightning Network transactions, using the Litecoin implementation.

4.3 Daughter chains from Proof of Burn

Our suggested sketch of the multichain scaling model is that daughter-chains should be created by explicit, special, transactions that allocate a subset of the total coinbase of the currency to the new chain.

From the perspective of the mother-chain, this transaction is a Burn transaction, to a unique burn address representing the specific daughter chain. From the perspective of the daughter chain, the image of this transaction in its chain is analogous to a coinbase transaction, creating precisely as many coins, and allocating them to as many txouts as the burn transaction has txins - the images of the transferred accounts.

(If the mother-chain also has an identifying burn address equivalent to coinbase transactions on its chain, we can also transfer funds the other way, into the original chain, allowing for a daughter-chain to periodically resync with the main chain, at a lower rate.)

This is currently only a sketch of the model we envisage, derived from existing uses of Proof of Burn to “bootstrap” new altcoins from other currencies. We expect most of the initial development work on 光 coin to be involved with testing, expanding, proving and implementing a secure version of this approach.

5 Contribution to Society

One final issue that we believe is important in any endeavour is to determine how our activities impact humanity as a whole. Whilst it can be argued that cryptocurrency development is, at worst, morally neutral (merely “enabling commerce”), it is not clear that this is sufficient.

Recent cryptocurrencies have suggested the concept of charitable “tithes” as a component of the blockchain function itself[31]. The cited example derives its moral justification from a Christian ethic, but we do not require anything more than a Humanistic justification to make the same commitment.

Whilst this is not a technical requirement, then, 光 coin makes the moral commitment, via coinbase transactions, to donate 5% of the block mining reward to a public, charitable address (the remainder of the coinbase reward is distributed to the miner). The value of the balance in this address will be verifiably transferred as a donation to a suitable charity - initially, Médecins Sans Frontières/Doctors Without Borders.

6 光 coin Schema and Future Work

6.1 Current design

Via the arguments above, we have chosen the current design for the initial 光 coin release to be:

6.1.1 Mature, featureful Codebase

Litecoin-based codebase - providing blockchain scaling improvements from SegWit and Lightning Network implementation.

6.1.2 Post-Quantum Signatures

PICNIC-10-30-Unhruh scheme, provably resistant to QROM attacks.

6.1.3 Improved Address Hash collision resistance

光 coin addresses are 224-bit Blake2b hashes of SHA-256 hashes of public keys, improving resistance to potential collision searches.

6.1.4 Post-Quantum Energy-efficient PoW + PoB

Modified Equihash PoW. Flatter coin emission, with small tail emission to limit transaction fee growth; approaching inflation-neutral due to Proof-of-Burn coin destruction incentives. [On launch, burn only applies to Transaction Fees; Proof of Burn blocks will be added at a later date, as they are also not necessary in the initial growth phase.] 5% of TX Fees burned as deflationary delta.

6.1.5 Humanist tithe

5% of block mining reward directed to charitable address from which regular donations to Médecins Sans Frontières/Doctors Without Borders will be made in a transparent and public manner.

6.1.6 Open Source development

The source code for 光 coin can be found on GitHub at: https://github.com/guangcoin/guangcoin

6.2 Future Work

6.2.1 PostTerra Post-Chain models

At present, the post-terra (post-linear chain) model is a field of active research, and will be the main focus of future efforts. As the basic scheme will involve a core consensus blockchain in every connected (low-latency) zone, the current blockchain will always remain canonical, as the “Earth-based” consensus chain.

This means that transactions on the currently released chain will always be valid. (In the worst case that a significant topology change would be required, we would transfer all coins to the new topology as part of the transition process.)

6.2.2 Enhanced Privacy

One deficit in the Litecoin codebase is in the privacy of transactions - whilst coin-mixing provides additional privacy, other cryptographic secrecy approaches (such as Ring signatures on transactions) would provide additional value. We are confident that we can build on existing implementations in privacy-based coins such as Monero[32], and improved Ring signature algorithms which post-date those coins [33][34] to implement such features quickly into 光 coin.

7 Contact Details

7.1 bitcointalk ANN thread

7.2 Reddit

7.3 Github

https://github.com/guangcoin/guangcoin

7.4 Donations

Whilst we are not holding an ICO for this coin, for moral reasons, donations to development can be made to the following addresses:

36a1c66mCp9rNGcqfuiJjT94zg6xRa9Afq **Bitcoin Core (BTC)**
SOON **Bitcoin Cash (BCC)**
SOON **Ether/Ethereum**
SOON **Gas (Neo)**

5% of each donation will be transferred to the currently selected 光 coin charity - at present, Médecins Sans Frontières/Doctors Without Borders.

References

[1] https://www.weusecoins.com/assets/pdf/library/Tangle%20-%20a%20cryptocurrency%20for%20Internet-of-Things%20industry%20-%20blockchain%20alternative.pdf

[2] https://github.com/theQRL/Whitepaper

[3] https://en.bitcoin.it/wiki/Secp256k1

[4] Vaudenay, Serge. ”The Security of DSA and ECDSA.” International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2003.

[5] Proos, John; Zalka. ”Shor's discrete logarithm quantum algorithm for elliptic curves”. QIC. arXiv:quantph/0301141

[6] Ralph Merkle. “Secrecy, authentication and public key systems / A certified digital signature”. Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.

[7] Leslie Lamport. “Constructing digital signatures from a one way function.” Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979

[8] Johannes Buchmann, Erik Dahmen, Sarah Ereth, Andreas Hulsing, and Markus Ruckert. “On the security of the Winternitz one-time signature scheme”. IA. Nitaj and D. Pointcheval, editors, Africacrypt 2011, volume 6737 of Lecture Notes in Computer Science, pages 363–378. Springer Berlin / Heidelberg, 2011

[9] D. Unruh “Non-interactive zero-knowledge proofs in the quantum random oracle model.” EUROCRYPT 2015, Part II (Apr. 2015), E. Oswald and M. Fischlin, Eds., vol. 9057 of LNCS, Springer, Heidelberg, pp. 755–784.

[10] A. Fiat, A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems.” CRYPTO (1986), pp. 186–194.

[11] S. Goldfeder, M. Chase, G. Zaverucha, “Efficient post-quantum zero-knowledge and signatures.” IACR Cryptology ePrint Archive 2016 (2016), 1110.

[12] https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

[13] BitFury Group. “Proof of Stake versus Proof of Work.”No Publisher (13 September 2015) http://bitfury.com/content/4-white-papers-research/pos-vs-pow-1.0.2.pdf

[14] https://download.wpsoftware.net/bitcoin/pos.pdf

[15] (SpaceMint is the original successor project for BURST) https://eprint.iacr.org/2015/528.pdf

[16] https://eprint.iacr.org/2014/059.pdf

[17] http://www.internetsociety.org/sites/default/files/blogs-media/equihash-asymmetric-proof-of-work-based-generalized-birthday-problem.pdf

[18] https://en.bitcoin.it/wiki/Proof_of_burn

[19] http://www.planetaryresources.com/

[20] https://www.nasa.gov/mission_pages/mars/main/index.html

[21] http://edition.cnn.com/2016/12/28/asia/china-space-program-white-paper/index.html

[22] http://www.spacex.com/mars

[23] https://bitslog.files.wordpress.com/2015/09/dagcoin-v41.pdf

[24] https://byteball.org/Byteball.pdf

[25] https://github.com/wildbunny/docs/blob/master/T.E.T.O-draft.pdf

[26] https://gist.github.com/Taek42/3e4f029261b5719e4587fe4972fb904a

[27] https://www.bitcoinunlimited.info/resources/subchains.pdf

[28] https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[29] https://lightning.network/lightning-network-paper.pdf

[30] https://litecoin.org/

[31] https://github.com/biblepay/biblepay

[32] https://getmonero.org/

[33] Fujisaki, Eiichiro (2011). “Sub-linear size traceable ring signatures without random oracles”. CTRSA: 393–415.

[34] Au, Man Ho; Liu, Joseph K.; Susilo, Willy; Yuen, Tsz Hon (2006). “Constant-Size ID-Based Linkable and Revocable-iff-Linked Ring Signature”. Lecture Notes in Computer Science. 4329: 364–378