Cada Blockhain

The Evolution will not be Centralized

John Williams

Abstract. Cada Blockchain is a cryptocurrency designed to be ultra-compact. Designed to remain Totally Decentralized. Designed to have no rulers. There are no miners and no ever-growing database. A simple yet powerful scripting language, Cascading Proof Chain, adaptive block scaling, and an innovative Proof of Work (PoW) backed user-centric blockchain algorithm that uses both on-chain and off-chain traffic for security. All Quantum Secure Cryptography. Small enough to run efficiently on your mobile phone. Everyone runs a Complete node. Forever.

1. Introduction

In 2008 Satoshi Nakamoto unleashed Bitcoin[1] and it changed the world. A revolutionary digital monetary system explicitly intended to be liberated from any overarching authority; a secure decentralized network where no one needed to trust a third party; the natural evolution of an antiquated monetary system so evidently fallible and easily abused.

The Problem:

Since then, many ingenious and powerful advancements have been made, but in our haste to build features, one single property, for some the most important property, is being side-lined in favour of scale and security: **Decentralization**. Bitcoins' original raison d'etre was for there to be no overarching authority 'controlling' the network, no single points of failure and no avenues for censorship built on top of a network resilient to distributed attacks; both digital and physical. Every single cryptocurrency operating today has sacrificed some or all decentralization in their race for increased scale and supposed security. Centralization causes huge efficiency gains after all. But if 1 group of users is paid to perform any 'task' on the network for the rest of the users (finding blocks, resolving disputes, etc.) this inevitably leads to centralization, as is shown by all of the major crypto networks. In essence decentralization matters because centralized networks are so easy to attack.

Current miner-centric networks rely on a relatively small number of users running full validatory nodes that process every transaction, ensuring that no one cheats the system and no one accepts an invalid transaction. But they are not involved in the construction of the blockchain itself, just its validation. A much smaller group of users, normally referred to as miners, run a full validatory and mining node, otherwise known as a Complete node. Since only this small group of Complete nodes is involved in the construction of the chain, only this small group decides which valid transactions actually make it into a block or not, and only this small group is involved in ensuring the liveliness[15] of the network and the prevention of censorship attacks.

How many compromised or coerced human beings would it take to seriously disrupt a cryptocurrency, or worse - render it entirely useless? To force mining operators to produce blank blocks or censor transactions, perform constant 51% attacks or stop DPoS delegates from confirming or resolving anything? The answer for almost all coins is surely less than 100, and for most far less than 21...

The Solution:

A network where every single user is an equal and Complete member. Where disrupting the network would require attacking, bribing or coercing 100's of millions, maybe billions of users. Orders of magnitude more than current crypto solutions. Total decentralization.

Can a secure, scalable, truly decentralized cryptocurrency be made with no overarching authority? Can every user be an equal on a cryptocurrency network? Can mining centralization be abolished? Can the need to outsource any critical aspects of the network to some third party become redundant?

Requirements:

- The protocol needs to be so resource-efficient that every user is able to run a Complete node at all times, as if it is of no consequence.

- It must remove the paid miners. The miner-centric fee-paying model always leads to centralization.

- It must be complete. Immutability of the protocol is a desired quality.

- Since it must be complete, the Protocol must

    - scale from inception
    - be Quantum Secure

for a future where it might matter.

- It must be small. It must be powerful. It must remain decentralized. It must be finished.

Enter Cada Blockchain.

2. Tx-PoW

Removing the miners requires the users themselves to secure the chain. User-based PoW security has been tried before. The DAG[3] style IOTA[8] allows users to perform a small amount of PoW work before they can send their transaction. Unlike Cada Blockchain, IOTA does not use a blockchain, instead opting for a transaction DAG or Tangle. Whether the Tangle can converge in a decentralized fashion is still a topic of debate and recently IOTA switched to a new system, in an attempt to rectify their current solution, a centralized checkpoint server.

Cada Blockchain uses a Tx-PoW blockchain, an idea first started with P2Pool[10], a protocol that allows multiple users to trustlessly perform small amounts of work and then sum all of those pieces up into a full block's worth of PoW. With a single PoW value equal to the sum of the smaller parts. Everyone benefits from the total work done. This would work well in a transaction based security protocol. All the transactions could do a small amount of work, and then sum all of that up into single blocks. This way Cada Blockchain removes the miners but keeps the blockchain as the single PoW-secured time-ordered list of events.

Each transaction in Cada Blockchain is PoW mined. The process is very similar to searching for blocks on any other PoW blockchain. When you find a Tx-PoW that satisfies the network allowed difficulty, 10s average work per device, your transaction may be broadcast, relayed across the network, and added to blocks. The network can determine the minimum Tx-PoW by averaging recent transactions. But, this is also how the blockchain is constructed, since if by chance your Tx-PoW value is high enough, determined by the network to be 1 Tx-PoW every 50 seconds, you have not only mined your transaction but you have also mined a block, that users can add to the current chain. The more transactions being sent the higher this block difficulty will be. Users wanting to send transactions, construct a Tx-PoW header that is foremost a record of their own transaction and as an adjunct a block header that represents their current view of the network. Since blocks only store the hashes of transactions, like Compact blocks in Bitcoin, they are of negligible size. A 10KB block would hold about 330 transaction hashes. Finding a block is the most secure action a user can do to safeguard their coins and honest blocks help sustain the health of the network. For the user, this is all seamless. Whenever a user sends a transaction, sometimes they also find a block.

The Tx-PoW chain lends itself well to GHOST[7] as transactions are added to blocks even if they themselves are blocks. With a complete list of the last n blocks, it is independently possible to calculate the block tree created by all the stale blocks included as transactions in the main chain. GHOST allows for consensus to be reached, with much faster block times than a simple Longest Chain Rule.

This type of system means that if there are no transactions then there can be no blocks. Cada Blockchain will need to reach a critical mass of transactions to sustain a secure blockchain. The transaction rate will need to be very high. Since all the security of Cada Blockchain is derived from the number of transactions, the more transactions there are, the more secure the network. There will be a bootstrap period until Cada Blockchain processes enough transactions to secure the network adequately.

Now – every single user is involved in not only validating the entire chain but also in maintaining the liveliness of the network and in preventing censorship attacks. All Cada Blockchain users perform both the validation and construction of the blockchain.

3. CADA

- Layer 1 does not scale.
- Layer 2 scales.

'...scales' – there is no upper bound on possible transactions per second.

The base layer of any cryptocurrency is known as layer 1 or on-chain. This is the layer every full member of the network needs to process. Solutions built on top of layer 1 occur away from the main chain, deliberately so, and are called layer 2 or off-chain. On layer 2, only those directly involved in the transaction need to process it, not the whole network. This is why layer 2 scales but layer 1 does not. The idea that everyone should process everything does not scale.

If most of the traffic is taken off-chain using the Lightning Network, Sidechains, Multi-Signature Federations or another method, then by definition most of the traffic is not even viewable let alone auditable on-chain. There is currently no mechanism that secures layer 1 with layer 2 traffic. No way to incentivise or force fees down from layer 2 operators and users to the miners on layer 1. For all miner-centric coins, this is a problem. How can trillions be transacted off-chain when only millions are spent in fee-paying transactions securing layer 1? Clearly, these layered systems are only as secure as the security of their lower levels. Less money spent equals fewer fees paid. So either layer 2 works, it scales, and everyone jumps off-chain, reducing layer 1 security by starving miners on-chain... or layer 2 does not work, users stay on layer 1, all the on-chain miners get paid, but it can't scale...

One solution is (very) high fees for layer 1 and thus very large transaction amounts, keeping all the smaller interactions off-chain. This does indeed secure layer 1 by paying the miners adequately, but makes it impossible for normal users to transact on-chain, since the fee alone would likely be larger than the desired transaction amount. Sometimes you have to use layer 1, it's not always a choice (if someone tries to force close your Lightning Channel and steal funds), and then what?

Another solution is to inflate the coin supply. Just print 1% extra per year and use that to pay the miners. A clean solution... that does indeed secure layer 1, but of course, you lose the hard cap on your total supply which is a very desirable quality if you want to be considered a Store of Value. Supply inflation is just a hidden tax on every user.

Cada Blockchain has an innovative and unique solution.

- Replace fee-based security.
- Make layer 2 secure layer 1.

Cada Blockchain runs over a Peer-to-Peer (P2P) network called Cadical. Every user on the Cada Blockchain network is connected to every other user. Cadical opens up this P2P backbone, via a simple network API, so that users can transmit any data they like, not just Cada Blockchain transactions, to other individual Cadical users, point-to-point and not flood-fill. This gives a method of communication that can be used by all the layer 2 protocols, such as the Lightning Network, Sidechains, Decentralized Exchanges etc.

Even better, users of Cadical who have no Cada Blockchain, no tokens, send no transactions and have no interest in layer 2 magic, can still help to PoW secure the network, by sending messages over Cadical. For instance, MaxChat, a simple low-bandwidth chat application that runs on Cadical, a resilient decentralized censorship-resistant P2P network, could bring countless users and there are countless other compatible applications that require network communication.

All Cadical users run Cada Blockchain. All messages pay PoW. All PoW secures Cada Blockchain.

We define a :

- Cada Blockchain transaction / on-chain / flood-fill / does not scale.
- Cadical transaction / off-chain / point-to-point / scales.

Cadical allows the transfer of small amounts of data for free, aside from the required PoW, but routing larger amounts of data is possible and can be paid for using Lightning. A simple technique encrypts the data with the same key as the Lightning invoice (the preimage of a hash). This way the recipient only gets access to the decrypted data once a payment is made. An atomic data exchange - where either both actions happen or neither happen.

As more and more fee-paying traffic is generated, Cadical incentivises users to set up Cada Blockchain routers, effectively a node with an external IP which other Cada Blockchain users can easily access, which is invaluable to the integrity of any P2P network. Instead of incentivising miners to use more and more energy finding coins, Cada Blockchain incentivises users to set up increasingly better routers that improve the integrity and quality of the backbone P2P network that runs Minima.

Cada provides value transfer. Cadical provides information transfer.

4. The Cada Network

Both Cada Blockchain and Cadical require users to perform a small amount of PoW when sending messages. The more messages, the more PoW. The more PoW, the more secure the network. But what if a user is not sending any messages? Can that user also help to secure the network? What if sending a message is time-critical, and there must be no delay before sending it – say a high-frequency trader? Cadical addresses both these concerns by repurposing existing technology, allowing users to do the work beforehand, and then present that work as proof when sending messages.

Most network protocols have a PING message. This is a message network peers periodically send to check the health and status of their peers. Network nodes send a PING message and peers reply, to show they are functioning correctly. But in a crypto network like Cada Blockchain far more information on the health and status of a node can be transmitted in a PING message. Add some PoW to a PING message, and you create a Pulse.

Every 10 minutes every Cada Blockchain user creates a valid Tx-PoW message, with its current correct block details, but leaves the transaction blank. Performs 10 seconds of work. Then sends this message to each of its peers. If the message is not a valid Tx-PoW message, the peer is kicked off the network. If a peer does not send a Pulse message every 10 minutes, the peer is kicked off the network. If the Tx-PoW message is also a block, on average 1 Tx-PoW message every 50 seconds, that is then forwarded on to the rest of the network

This has many benefits :

- Shares the peers' current mempool - the list of transactions it knows about not in the current longest chain. Any discrepancies can be resolved and missing transactions passed on. Peer data synchronisation.

- Shows the peer is a functioning Cada Blockchain node, has a working network connection, is a valid router for network messages and can help secure the network.

- Adds to the overall PoW security of the network.
- This is all off-chain. Only the immediate peers check the Pulse message and only a block is forwarded on to the rest of the network.

As the requirements to send a Pulse message are so small, should a peer not be able to send a Pulse message, there must be something wrong, so there is no point wasting resources. When they fix themselves, they can come back online, and rejoin the network. Those thinking they will not pay the PoW, will just be kicked off the network.

5. PoW vs Distributed PoW

Hash-rate does **not** equal security.

Since if this were the case, 1 miner with infinite hash-rate, would imply a secure network. It's not. It's called PayPal (a completely centralized payment gateway). No resistance to censorship attacks at all.

What matters is the **distribution of hash-rate**. This is self-evident when we consider the dreaded 51% attack.

PoW blockchains are always fearful of a 51% attack. This is an attack where some person or group has access to over 50% of the hash-rate and as such can reverse transactions, hold the chain to ransom with empty blocks, or censor transactions, by creating a longer valid chain with more PoW. In miner-centric PoW networks, miners are paid to acquire hash-rate. It is guaranteed that a small group of miners can create a 51% cartel. Trust is not the issue. Miners have strong incentives to play by the rules and not attack the chain, for fear of losing income. Coercion is by far the more likely attack. Governmental coercion at a state level.

Cada Blockchain, a distributed PoW blockchain, does not incentivise the acquisition of hash power, since there is no financial reward for finding a block and no advantages to doing more work than necessary. There is no small group or cartel of users that will have anywhere near 1% of the total hash-rate, let alone 51%. Hence coordinating this attack becomes very expensive as there is no use for the hardware required other than to attack the network, no mining rewards to recoup the initial investment. The cost of an attack must be less than the potential gains after all.

There is, of course, a caveat to the Distributed PoW Model. You need a lot of users.

6. HashCash and Burn

Adam Backs' HashCash[9] was the first weaponized version of PoW. A Denial-of-Service (DoS) counter-measure first deployed to prevent email spam. Sending millions of emails 'costs' nothing – hardware, processing, bandwidth, etc. A lone computer sitting on the internet can send millions of emails in almost no time, constantly. HashCash enforced that a PoW payment was included whenever an email was sent. To a single user sending emails every few minutes, this was utterly negligible, a background process that hummed for a few seconds after you press the 'Send' button. But to the spam-machine sitting on the internet trying to send millions of emails, this would require millions of seconds of work, an impossible task.

Negligible PoW stops DoS. Negligible PoW does not stop DDoS.

This email attack is a DoS attack because there is only one machine sending the spam. A DDoS attack, a Distributed DoS attack, is when multiple machines are used. A 50,000 strong bot-net of mobile phones, could each send a message every few seconds. A million messages is now only a few minutes of distributed work.

To prevent a distributed spam attack on layer 1 of a decentralized P2P blockchain network a small amount of PoW per message is not enough. Small amounts of PoW, to the individual users, are effectively free. Yes, they pay in power usage on their mobile phone, there is a time delay, but you do not notice it. You do not feel it. To prevent a DDoS attack we need something that is not 'free' to users.

On miner-centric chains, this is the fee (which serves multiple purposes). The fee must be paid for a transaction to be valid. 1 million messages now require '1 million fees'. The cost of the attack is now prohibitive – since the attacker must pay this, the bot-net only provides PoW. Should the attacker persist nonetheless, there is an ongoing and non-negligible cost to the attack, that cannot be sustained indefinitely.

On Cada Blockchain this is the Burn (which also serves multiple purposes). A Burn, when the outputs of a transaction sum to less than the inputs, is equivalent to paying every other user a very small fee. Since 'burning' reduces the total number of Cada Blockchain in circulation, since all coins are created at genesis, those coins that are left are more scarce and therefore more valuable. Unlike fees, the Burn has no minimum. There is no requirement for the total Burn to be large, and able to support the mining industry, that in turn secures the chain. The burn may be high during periods of heavy traffic or spam, and as it rises, traffic will decrease, and the system will self-regulate. The burn can be very low when traffic is at manageable levels as the total amount is not important, only the relative burn amounts in comparison to other transactions.

The Burn in Cada Blockchain serves multiple purposes:

- A strong incentive to propagate and process a transaction.
- A method for ordering transactions and regulating on-chain traffic.
- A mechanism for spam prevention by making DDoS attacks expensive.

HashCash is totally decentralized. Each user can independently perform the required PoW, by mining their own email, and every other user can independently verify the proof. No third parties are consulted, no miners are paid. Cada Blockchain is the same, but users mine transactions instead of emails.

Constructively, from the maelstrom of transactions fired across the **Cada** network, a single time-ordered interlocking chain of blocks emerges revealing the complete transaction history.

Cada Blockchain Consensus is driven by HashCash and Burn.

7. Energy

PoW blockchains are often criticised for using a lot of energy. Energy usage is a requirement for Nakamoto Consensus to work. It is precisely this that makes PoW chains objectively identifiable, verifiable and valuable.

In a competitive system, miners are incentivised to use the maximum amount of energy that is economically viable to mine digital coins they can sell for a profit, whilst securing the chain as a bonus.

In a cooperative system, users can use the minimum amount of energy required to secure the chain, as there are no incentives to use more.

Decentralized energy[16][17] is far more sustainable than centralized energy. Sustainable energy scales in time. Since users have only to do small amounts of work, rather than large mining operations doing large amounts of work, the users themselves can generate all the energy required, by using whatever means at hand to simply charge their mobile phones as usual.

Cada Blockchain is compatible with the concept of Free Energy. Energy you do not even pay for, since you generate it yourself (solar probably). If you give Free Energy to a single competitive miner he will be very happy, as he can now use even more energy to try and mine even more coins. Give Free Energy to all the miners, and the effect is nullified, mining is a zero-sum game after all, and they will continue to use the same amount of centralized power as well as the Free Energy.

8. *A C*ada *C*hain

The power of hashing ensures that an unbroken chain of blocks cannot be altered in any way. The power of hashing also ensures that sometimes someone will find a very high difficulty PoW when looking for a much lower one. If you take this into account pre-PoW you can construct block headers that reference multiple block parents at different levels of difficulty. Instead of having 2 difficulty values for a user to mine in the Tx-PoW, the Transaction Difficulty set to 10 seconds of work on average, and the Block Difficulty set to 1 block every 50 seconds, let us add 1 more difficulty, the Super Block Difficulty set to twice the current block difficulty…

Every block references its direct parent and the last Super Block. Now a Tx-PoW has 3 possible levels, Transaction, Block and Super Block. If the Block hash difficulty is high enough it becomes a Super Block (which is also a valid block). Eventually, all blocks and data are discarded and only a chain of Super Block headers is kept as a long term store of the total PoW in the chain. Now instead of only 1 Super Block Level, let us use 256. 1 for each bit in a 32-byte hash. Each level is twice the difficulty of the level below. These are the only difficulty values for each block, each linking back to its Super Block Level parent.

The proof chain grows logarithmically, so that an almost limitless amount of PoW can be stored in a finite chain of headers, since every level stores blocks that are twice as difficult as the level below. Thus, an exponentially shorter unbroken chain of more PoWerful blocks is kept in place of a longer unbroken chain of less PoWerful ones. Due to the nature of randomised hash mining, the sum of the Tx-PoW difficulty of the higher-level blocks will on average equal the sum of the Tx-PoW difficulty of the lower level blocks.

The cascading chain allows each user to keep the total cumulative PoW without requiring the storage of every block. Only certain lucky blocks are kept, all of which reference each other, to keep a short unbroken chain of ever-increasing total PoW.

Almost all blocks and transactions are pruned. Pruning has no effect on the security of the user doing-the-pruning. Once a transaction has been checked by a user, that transaction need never be checked again, a simple reference will suffice. Blocks are kept for a certain period of time, a week would be fine, before being pruned. This way any user that logs on to the network can always catch up a weeks' worth of blocks. So as long as a user logs on to the network once a week he can validate every transaction on layer 1 and run a Complete node, full validating and full TxPoW mining, without needing increasing amounts of storage.

For a new user, who has no previous history of the chain and no coins, Nakamoto Consensus can objectively and independently tell which chain is the current valid chain - the Cascading Chain with the most PoW.

9. Storage-less MMR UTXO

In the old world, every user kept track of every account in a big book (or database). Every user had a copy of this book. Whenever a user wanted to send a transaction, every user checked the transaction was valid, by checking the inputs were valid in the big book and updating the books' pages as necessary. The more transactions, the bigger the book.

In the new world, each user has a specific page in the book, with all their account details. That page is ripped out of the book and given to that user. Each user rips out their own page. Every user only keeps their own page and the spine of the whole book. Whenever a user wants to send a transaction, they add a copy of their page, which verifiably fits the spine, so that users can check if the transaction is valid, update the page, and update the spine ready for the next transaction. Now users only store their own transactions, and a cryptographic spine no thicker than a single page. Orders of magnitude less data.

Cada Blockchain does not have a database (or big book) that stores all the Unspent Transaction Outputs, instead, utilising Peter Todds' MMR[4] storage-less Proof DB. It allows for an almost limitless amount of provable data to be added and updated in a particular hash tree. It's a little bit like a SQL database with INSERT and UPDATE, but no SELECT or DELETE. The trick is that if you have data in the database, and are listening to all the additions and updates, you can always prove what data you know, your version of SELECT. Data proves it exists with a Merkle proof to the root of the MMR hash tree.

Each user keeps track of their own coins, rather than miners or even all users keeping track of all the coins. This is an infinitesimally small amount of data in comparison to an entire blockchain. But - each user must stay up to date with the blockchain. By doing so they can keep track of the Merkle proofs required to prove their coins not only exist but are unspent. This proof changes with every addition or update to the MMR. Should a user not keep track of his coins, they would not be lost, but he would need a third party to help recover them. He would need to find either an archive node that stores everything – for the purposes of selling the data in this exact scenario, or have previously set up a friend or chat group to keep track of extra coins (coin-proofs pose no security issues), and have them rediscover the individual MMR proofs for their coins.

Cada Blockchain goes MMR real-time. Each block commits to the current MMR state for that block. Each user sends his transactions with a recent MMR proof, to prove the transaction is valid. Users can check these details with their latest MMR database, and update as necessary when a block is accepted. This process will need to be made very fast. The MMR database stores multiple overlapping MMR states, one for each block, and it needs to be able to prune and un-prune MMR data and derive proofs quickly for multiple changing states. Fun.

10. Smart Contracts, Tokens and Transactions

Cada Blockchain operates a validatory network, like Bitcoin, rather than a computational network, like Ethereum[18]. Computational networks require far greater resources to operate than validatory networks. In fact, the computational resources required far exceed those available to the majority of network participants, hence these networks centralize around larger more powerful nodes. Cada Blockchain must allow everyone to run a Complete node.

- Validation is the minimum amount of useful computation.
- Logic can be computed off-chain and validated on-chain.
- Everyone computing or validating everything does not scale.
- Everyone validating a manageable amount on-chain to enable near-limitless capacity off-chain does scale.

Unlike Bitcoin, Cada Blockchain natively supports Tokens. Unlike Ethereum, no efficiency is sacrificed when processing tokens. As far as the network is concerned, token transactions are the same as Cada Blockchain transactions, are stored in the MMR Proof DB and do not increase storage requirements. You prove their existence like you prove your Cada Blockchain holdings. Tokens can be created by colouring a certain fractional amount of Cada Blockchain. All scripts applicable to Cada Blockchain are equally applicable to Tokens.

Transactions on Cada Blockchain are similar to Bitcoin transactions, yet upgraded in functionality and power. They include a list of inputs, a list of outputs, and some data registers for storing custom data. The sum of the outputs must be less than or equal to the sum of the inputs. Each input has an Address, Amount, TokenID, CoinID and can have various user-defined parameters. Each address is actually a Smart Contract, represented as the hash of a Cada Blockchain Script. This entire transaction can then be signed by 1 or more Public Keys. When sending a transaction, a user adds the MMR proofs showing that the inputs exist and are unspent, spends ~10 seconds mining, before sending the complete Tx-PoW message across the network. Each transaction is a self contained cryptographic unit that can be verified independently with just the recent MMR root hash found in memory. Very fast and efficient.

Cada Blockchain uses a simple yet powerful scripting language. A script will return TRUE or FALSE as to whether an output can or cannot be spent. An empty script returns FALSE.

A standard transaction:

An HTLC (Hashed Time Locked Contract) :

```
IF @BLOCK GT 102453 AND SIGNEDBY ( 0xEFDC56DCA87F ) THEN
        RETURN TRUE
ELSEIF SIGNEDBY ( 0x12345678 ) AND SHA3 ( STATE(0) ) EQ 0x87654321 THEN
        RETURN TRUE
ENDIF
```

Many powerful functions including :

- **MAST –** Merklized Abstract Syntax Tree, large scripts with short execution paths..
- **VERIFYOUTPUT** – check transaction Outputs, Covenants..
- **VERIFYINPUT** – check input data, complex multi-token scripts, Dividend payouts..
- **ADDRESS** – create scripts in script. Recursive Covenants, Vault addresses..
- **CHECKSIG** – check a signature in script, Oracles..
- **PROOF** – Efficient Merkle proof checking..

Cada Blockchain also includes simple state variables per transaction, accessible to input scripts, so that a sequence of transactions can occur whilst keeping track of changing variables. This allows for more complex 'stateful' smart contracts, like Ethereum, whilst maintaining and even increasing the speed and efficiency of Bitcoins' UTXO model transactions.

11. Quantum Secure

Quantum security is not an issue right now. But it will be in the future. If you want to remove the need for protocol developers because the protocol is advanced enough to take care of itself, and should not require any Hard Forks ever (there are no Soft Forks on Cada Blockchain as all users are also miners), you need to use Quantum Secure algorithms.

Cada Blockchain uses the KECCAK hash algorithm for Tx-PoW mining, block and transaction hashes, proof chains, and signing or verifying data. All of the cryptographic security of Cada Blockchain is provided by hash functions. The scripting language supports SHA2-256 to allow cross-chain hash lock contracts with legacy chains. The signing algorithm is the Winternitz One Time Signature scheme (WOTS). You can build hash trees of valid public keys, and process them in MiniScript, so that you can sign multiple times with the same root public key – the Merkle Signature Scheme[13].

Quantum security comes at a price. The signatures are at least 10-20x as big as ECDSA, used in Bitcoin. A one time use WOTS is 400-800 bytes. Cada Blockchain signatures are certainly large when compared to normal Bitcoin transactions, but they are not kept forever since almost all data is eventually pruned, so although a bandwidth issue, they are only a temporary storage overhead.

12. Block Size

Blocks in Cada Blockchain are small. As small as a transaction. All transactions are potential blocks. Blocks are just lucky transactions. Blocks only contain references to transactions (Compact blocks in Bitcoin), that have already been sent across the network, rather than the entire transaction. Cada Blockchain also uses an adaptive block size. The maximum size is set by the chain as twice the average block size of the last n blocks. This allows the users themselves to determine the block size. By filling their blocks higher than the average they will make the maximum size greater, by filling them lower, the maximum will be made lower. Users can drag the maximum block size up or down depending on whether they need it, or whether enough traffic is going Lightning[3] and beyond.

On a miner-centric chain, blocks must be full. If blocks are not full, there is no fee market for block space, and no requirement to pay any fees at all. If there are no fees there is no security, as the fees pay the miners and the miners secure the chain. Empty blocks are no good, half-full blocks are no good, only full blocks work. Block size must be restricted in some way to ensure this is the case.

On a user-centric chain, blocks can be empty, half full, or full, with no effect on the security of the chain. The security is determined by the total PoW generated by all the users. There are no 'fees' required to pay miners to secure the network. There is no requirement to restrict block size, as long as the overall network can handle the on-chain transaction per second rate. The 'Burn' acts as congestion control, to limit traffic at times of heavy load. Each user can determine the load they face independently on their local device and use that knowledge to build a block with a manageable size.

Cada Blockchain uses a Cascading Chain that aggressively prunes almost all data, whilst keeping a record of total cumulative PoW and the complete MMR Database, so blocks are not an ongoing storage overhead but only a short-term bandwidth and processing concern.

13. Block Speed

The security of a transaction is not improved by a faster block speed, since the amount of security is a function of the cumulative PoW of the parent blocks (hash-rates being equal 1 BTC block is worth 4 LTC blocks, since LTC runs 4x faster). A faster chain does increase the granularity of information[6] and allows a user to know sooner when their transaction is secure enough. The longer you wait, the more secure.

If the block speed is too fast you risk 'decoherence', when the chain cannot keep up with itself as too many blocks are found and multiple conflicting branches emerge, but if the block speed is too slow you ignore the benefits of higher information granularity.

Block speed can be much faster on a GHOST[7] chain and so Cada Blockchain is aiming for a 50 second block time[6].

14. Consensus, Forks and Immutable Protocols

In decentralized blockchain systems all full users need to agree on the rules. If there is no agreement on the rules there can be no consensus on the ordering and eventual outcome of actions. Current blockchain systems have 2 types of consensus changes available. This is because there are 2 types of 'full' user. The first helps in the construction and validation of the chain - Complete nodes (the miners). The second only helps in the validation of the chain - Full nodes (the validators). We ignore Wallet users, by far the largest group on these chains (unlike Cada Blockchain), who neither validate nor construct, and are simply swept along, whether they agree or not.

A soft fork is when the Complete nodes change the rules in ways that are still valid to the Full nodes. A soft-fork is a reduction in the chains' abilities. All Full nodes still see a valid block, just with a reduced solution space. Permanent censorship of a transaction or address is a soft-fork, since only those involved in the construction of the chain have any say. On fixed block size blockchains, a reduction in block size is a soft fork, as it still appears valid to all the Full nodes, just a smaller block. A hard fork is when all nodes need to agree to an increase in capabilities, adding an ability that was not there before. On fixed block size blockchains, an increase in the block size requires everyone to agree, as it is invalid to Full nodes given the old rules, that specified a lower maximum block size. Adding a new function or feature is a hard fork. Upgrading or fundamentally changing the protocol is a hard fork.

Soft forks are much easier to implement than hard forks since only a majority of the much smaller group of Complete nodes needs to agree. Soft forks can be imposed. The Complete nodes do not need the Full nodes' permission. Hard forks are much harder to implement. The larger the network the harder it gets. A decentralized protocol can only grow in adoption once it has stopped being updated, since it is impossible to update once deployed at scale. This is why the ossification of truly decentralized protocols occurs.

On Cada Blockchain :

- Everyone runs a Complete node.

- Everyone is involved in the construction and validation of the chain.

- Everyone needs to agree on everything because everyone is involved in everything.

- There are no soft forks, only hard forks.

The Cada Blockchain Protocol is complete from inception, containing all the scaling and functionality it will ever have or need. No soft forks allowed. No hard forks required - ever. No limit on the size of the network that can use it. POP3, SMTP, UDP and TCP/IP are examples of ossified global decentralized protocols. They don't change. That's the point. That's why they are the back-bone of the Internet.

15. Conclusion

Cada Blockchain is :

- A compact blockchain that runs completely on your mobile phone.

- A scalable, programmable, storageless, quantum-secure, proof-based, cascading Tx-PoW chain.

- A resilient, open, global, censorship-resistant p2p network with a built-in base-layer blockchain for trustless payment, token and contract processing.

- A fully decentralized crypto system of collaborating users, with no centralizing points of failure, able to sustain the largest network of Complete nodes ever assembled.

- A miner-less, cooperative, distributed PoW network immune to the trappings of a centralizing, miner-centric, fee-based paradigm.

Decentralization: Above all else Cada Blockchain strives to be a completely decentralized platform. Every user on the network runs the same code in the same way. Every user runs a Complete node. There are no special user classes, no master nodes, no delegates and no miners. The protocol uses a small amount of resources specifically so that all users are able to run a Complete node at all times. Any systemic attack on the network requires an attack on the entire user base. There are no centralized points of failure.

Security: Cada Blockchain is a Distributed PoW secured blockchain. The true PoWer of the Cada Blockchain Network comes from the scalable off-chain transactions, running over Cadical, that also contribute to layer 1 security. Layer 1 security is not compromised by traffic going off-chain to layer 2, it is in fact enhanced. All the cryptographic security of Cada Blockchain is hash-based, and as such, Quantum Secure. All nodes are Complete, so that light client attacks, where a user's lack of knowledge of the entire network is exploited, are nullified. Censorship and other block-based attacks are orders of magnitude harder to attempt.

Scalability: The Cada Blockchain Protocol allows for both on-chain and off-chain transactions. The block size is adaptive and can grow and shrink as the users see fit. Powerful off-chain protocols, some that already exist today, take traffic off layer 1 and onto layer 2. Layer 2 allows near-limitless innovation and throughput. Cada Blockchain can utilise current strategies like the Lightning Network and Sidechains, putting these abilities squarely in the hands of every user.

Sacrifice: In order to be runnable by all at all times, Cada Blockchain not only requires a large user base, but Cada Blockchain also asks for more from its users. Participation is a requirement. Cada Blockchain utilises an MMR database, maximal pruning and a Cascading Proof Chain. Essentially these techniques require users to connect to the network periodically, at best - constantly, at worst - daily or weekly. Then their MMR proofs can be updated, the validity of the chain's transactions can be verified independently and correct additions can be made to the Cascading Proof Chain, before the relevant data is discarded by the network. And of course, all users must work to send their transactions and participate in the network. All of this can be seamless to the user, buried under the application layer, but at a minimum, they will need to ensure they are connected to the network.

Cada Blockchain users have all the tools required to interact in a completely decentralized way. All users can independently track, store, share, validate and construct the blockchain. The burden of responsibility shifted squarely onto the users, with no miners, master nodes, delegates, coordinators or any other overarching authority to take the slack.

We're in charge. It's up to us.

Special Thanks to

The Indomitable Satoshi Nakamoto.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf

[2] Peter Todd: Making UTXO set growth irrelevant with low latency delayed TXO commitments. https://petertodd.org/2016/delayed-txo-commitments

[3] DAGCoin: A cryptocurrency without blocks. https://bitcointalk.org/index.php?topic=1177633.0

[4] Mini Blockchain: http://cryptonite.info/wiki/index.php?title=Mini-blockchain_scheme

[5] Gregory Maxwell: https://en.bitcoin.it/wiki/User:Gmaxwell/alt_ideas

[6] Vitalik Buterin: https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time/

[7] Secure High Rate Transaction Processing in Bitcoin: https://eprint.iacr.org/2013/881.pdf

[8] IOTA: https://www.iota.org/

[9] Adam Back, HashCash: http://www.hashcash.org/

[10] P2Pool: http://p2pool.org/

[11] GMSS signature scheme: https://www.cdc.informatik.tu-darmstadt.de/reports/reports/BDKOV07.pdf

[12] Eltoo: https://blockstream.com/eltoo.pdf

[13] Merkle Signature Scheme: https://en.wikipedia.org/wiki/Merkle_signature_scheme

[14] Channel Factories:
https://www.tik.ee.ethz.ch/file/a20a865ce40d40c8f942cf206a7cba96/Scalable_Funding_Of_Blockchain_Micropayment_Networks_(1).pdf
https://medium.com/chainrift-research/onboarding-the-masses-channel-factories-6e5c26b07cf1

[15] Liveliness: https://en.wikipedia.org/wiki/Liveness

[16] Decentralized Energy:
https://www.carbontrust.com/news/2013/01/decentralised-energy-powering-a-sustainable-future/

[17] https://www.power-technology.com/features/can-the-uk-ever-achieve-a-fully-decentralised-energy-system/

[18] Ethereum : https://www.ethereum.org/

[19] Proof of Proof of Work : https://eprint.iacr.org/2017/963.pdf