MOAT: turning Bitcoin Mining into an Energy Oracle for Power Protocols

kinnard
<kinnard@cryptocastle.company>

Bitcoin is at the advent of becoming critical infrastructure for the world. After a decade long struggle, the locks blocking you from using Bitcoin's power have finally been broken off. But this isn't about Satoshi's Power, or Bitcoin's Power. This is about your power.

Our goal is to make history and strike the spark of this new era by launching the first true (feature-complete) token on top of Bitcoin by transforming Bitcoin Mining into a decentralized energy oracle thereby enabling people to transfer power on chain. We want to revitalize and re-innovate mining for this new era with a next generation on-chain tokenized mining pool with a payout structure based on the energy of computation.
We can finally program Bitcoin full-power— smart contracts are finally unbounded on top of Bitcoin. But mining does not reflect the “unbounded” nature of Satoshi’s Vision. The training wheels have been taken off, but mining is still constrained by the thinking of the past era. By doing this we hope to make Bitcoin mining a popular endeavor again. And to do for power production what Bitcoin has done for money production. Our goal is to help you see your power.

In order to understand more about Bitcoin's power, first you must understand more about what Satoshi figured out.
How could Satoshi know what kinds of transactions what diversity and multitude of conditions people would desire and invent? He couldn't have. He recognized this and so he needed to make Bitcoin a tool of general power.

In order to understand what Satoshi figured out you must first understand what Turing figured out.

“Turing figured out something entirely different . . . he figured out that mathematicians unlike carpenters only needed to have one tool in their toolbox, if it were the right sort of tool. Turing realized that it should be possible to build a meta-machine that could be reconfigured in such a way that it would do any task you could conceivably do with information. It would be a protean device that could turn into any tool you could ever need.”

It took decades for Turing's invention—the Computer— a high water-mark for human consciousness, a super-weapon which was built to crack Nazi crypto and win World War II, to make it into the hands of people with the Personal Computer Revolution.

Today a new invention is working it's way into the hands of the people— Bitcoin.

Satoshi needed a 'machine' that could validate or invalidate an arbitrarily general set of conditions for transactions.
It's as if the components necessary to support the basic required feature-set for Bitcoin to be viable— multi-signature (a basic necessity for individual recovery even before multiparty), time conditionality (which is required for Bitcoin mining itself) or for more than one payment target type (pay to pubkey vs pay to pubkeyhash, a practical requirement) —emergent together, acted like a Miller-Urey Experiment of sorts and required Bitcoin to be generally powerful— like the Turing machine. Except Satoshi's Machine is a giant tape machine in the sky that's everywhere and nowhere and that's made of virtual gold.

So, Satoshi figured out something like what Turing figured out– a new tool, with general power.
When he did this, he invented —or discovered— the World Computer.
Miners are the peers who took up Satoshi's call to build this giant Turing machine in the sky.

Satoshi included a language for programming bitcoin, for programming this World Computer called Bitcoin Script.
But there are people who have been trying to stop you from using this new tool— from wielding it full-power.

You can think of the pieces of this giant Turing gold-tape machine in the sky as coins of course. They're really like punch-marked coins.
Little plates of gold than can be punched and repunched.

A piece of Bitcoin also known as a UTXO is stamped with a magical spell that locks the bitcoin and encodes the rules for unlocking and manipulating it. This spell is known as the locking script. In order to unlock and spend or otherwise manipulate the bitcoin you must cast a corresponding spell that satisfies the locking script and unlocks the coin, this spell is know as the unlocking script. You may then place a new locking script on the coin (or not— up to you).

These scripts are a special type of computer program puzzle where the script is broken into pieces. The pieces of theses puzzles are the opcodes and data that. When the game is played the pieces of the puzzle pushed onto and popped off of a stack according to the mathematical rules of the game. If after the whole program has played out if the last thing on the stack is "true" then the bitcoin are unlocked and can be spent. It's something like the Towers of Hanoi except with infinitely many potential problems and solutions instead of just one.

You can also think of a utxo like a state machine that transitions from locked-to-unlocked-to-locked according to the state transformation rules encoded in the lock

script.

Or you can think of them like pieces of virtual gold tape, that can be written, read and rewritten according to the instructions encoded on them.

Every Bitcoin transaction is a smart contract. Bitcoin transaction are actually the most fundamental, prototypical smart contracts. But there are some people who want to limit the kinds of transactions, that is contracts, you can write to the chain.
Contracts have been limited on top of bitcoin by a bevy of arbitrary constraints. Among them the contract size limit, the opcode number limit, and the AND & OR OPCODES, among many, being turned off.

Instead of being able to program Bitcoin full-power using the language which Satoshi built into the core of Bitcoin, the people who want to stop you from programming bitcoin full-power have tried to limit you to a few template transaction types— ostensibly to keep you safe.

But "a programming language should, above all, be malleable. A programming language is for thinking of programs, not for expressing programs you've already thought of."

". . . the only real test, if you believe as I do that the main purpose of a language is to be good to think in (rather than just to tell a computer what to do once you've thought of it) is what new things you can write in it. So any language comparison where you have to meet a predefined spec is testing slightly the wrong thing.

The true test of a language is how well you can discover and solve new problems, not how well you can use it to solve a problem someone else has already formulated."

With these locks on the language essentially you were gagged, you could not cast whatever script you want on bitcoin, you could not program Bitcoin full-power. But like Aristotle's laws of thought, because language is ultimately a tool for the mind, this gag is ultimately like a trick that's been played on your mind.

The locks that were on Bitcoin and on the language that's used to program bitcoin not only constrain what programs you can write to the blockchain, they constrain what programs you can think of.

The locks needed to be broken off of Bitcoin in order for you to see your true power for the same reason humans needed to abandon Aristotle's laws of thought in order to build the computer.

This being the case notion of the "work" that a miner does has been wrong-headed just like the locks on Bitcoin were wrong-headed.

With the locks taken off and general contracting now possible on top of Bitcoin the "work" that a miner does has changed in fundamental ways, it takes significant work to run & validate a block of transactions/contracts.

Miners need a way to account for the whole work of the mining process now that the relative weight of the first component of the mining process has changed. The nature of the work required to validate a block of transactions and build a block header is very different than the work required to find a winning block header hash. For miners whose endeavours are rapidly commoditized over time the difference between accurately accounting for this work and not accurately accounting for this work can mean the difference between being in the black or in the red.

But there's a problem, how do you accurately account for the work that a miner does at any precision? As previously discussed Bitcoin contracts can now finally be arbitrarily general and the work involved is not merely hashing but the storage, running, validation, and processing of Bitcoin contracts. Running computer programs. In order to measure the work that goes into a bitcoin transaction, and thereby the work that goes into a block of transactions, and all the work of mining and Bitcoin altogether we need a way to measure the work that goes into general computation. You need a way to measure computational work that is sufficiently general.

• **We have a problem and we need a solution that is sufficiently ... general.** •

There are many possible ways to approach this problem but we propose a novel cryptoeconomic method. There is one way to measure work that is easy to validate and hard to fake: power. Computation, whether hashing, block validation, transaction validation requires energy. Block acceptance requires a dynamically self-adjusting cryptoeconomically enforced amount of work and miners must expend energy to do this work. Due to Bitcoin's nature, we can measure power and energy with cryptoeconomic guarantees.

We propose a novel protocol consistent way to mine, which brings mining on chain in order to better reward miners for their work through a novel pool payout structure based on the energy necessary to do the computational work of mining thereby enabling real-time on-chain power accounting, without a trusted-third-party transforming Bitcoin mining into an energy oracle. And to reveal to you your true power— with personal-power accounting software.

We incentivize succinct snapshots from your Grandma’s Bitcoin miners about their power consumption (Attestations). Then with power flow analysis we can validate or invalidate attestations and reward accurate ones, and build the accurate ones up to a picture of the energetics of the entire network, in other words we can create an energy oracle.

These snapshots also serendipitously serve as proof-of-delivery of electricity. Allowing us to build on-chain marketplaces for electricity and power-backed tokens.

You can think of it like a pipe network with flow-meters: the laws of physics allow you to deduce the state of water in a closed system.

For example due to the law of conservation of mass without some additional inlet it's impossible for there to be more water down-pipe than was supplied up-pipe, so a flow-meter making such an assertion is either lying or mistaken. The more nodes upstream and downstream concur with a flowmeters attestations, the less likely the flow-meter is mistaken or lying. If all the nodes up and down concur then it becomes extremely unlikely. Certain things are simply impossible and others are extremely unlikely. Through a combination of accounting rules like these—the deterministic and probabilistic rules of pipe network analysis–we can rule in or out flow-meter attestations about the water flowing in a system and thereby do on-chain Water Accounting without a trusted-third-party.

Our plan is to work like-wise, using the deterministic and non-deterministic rules of power network analysis, from Bitcoin miner power-use attestations for power networks.

Instead of pointing at a classical centralized pool miners point their hardware at our pool contract in return for the incentive of our better payout structure. In order for miners shares to be accepted they must at dynamically determined intervals submit energy attestations of their own power-consumption as they mine. Miners pass a contract around to each other and append their attestations and shares to it, and sign off on the prior upstream attestation, with the winning miner finalizing the contract on-chain. In this way miners are mining on-chain as well as co-operatively building a power oracle.

In this way miners iterate the coinbase contract rather than the nonce a NOVEL, but protocol-consistent way to mine.
We hope this will allow us to redecentralize mining by replacing pool operators with smart contracts and make mining more cpu friendly by incentivizing more useful cpu-friendly computation so that the everyman can mine once again. (This is about your power.)

As we shift away from centralized money to decentralized money, our goal is to use Bitcoin to also shift us away from centralized energy production toward decentralized energy production. These regimes are tied up with each other: the linchpin of the contemporary fiat system is PetroDollar hegemony. Today If you want to draw from the spigot of centralized energy production you have to use dollars. Tomorrow, if our plan works we will see that we are all fonts of the power that's inside.

Decentralized power production and storage are taking off with more and more people choosing to become energy sovereign by using a solution like solar panels to produce their own energy. With the advancement of battery technology more and more power density is being stored by individuals at the edges of the network. Contrast this with the top-down centralized energy infrastructure that we have today.

By enabling people to monetize their power production investments in a peer-to-peer, disintermediated, trustless way we enable them to more quickly realize a return on their power production investments rewarding those who have made these investment, incentivizing more investments, and shifting us all toward a decentralized power production future more quickly.

We are not merely consumers at the edges drawing power down from the centralized grid. We can produce our own power as peers. We have always had this capacity to produce our own power and act as peers to the rest of the network. But we have lacked a way to exchange this power as peers with other people without an intermediating third party.

A purely peer-to-peer electric cash system would allow power to be sent from one party to another without the need for a trusted third party.

And here we are again having come full circle this isn't about Satoshi's Power, or Bitcoin's Power. This is about your power. It's always been about your power— the power you have inside.

++

There will be a fixed amount of tokens representing all of the energy necessary to create Bitcoin.
That is the energy going into mining new coin. Not the energy necessary to move coin that’s already been mined.

This is proportionate to the portion of of the block reward coming from the coinbase rather than transaction fees.

It is clear this is a finite amount of energy as no more energy will be expended to mine new bitcoin after the last bitcoin is mined somewhere a hundred or so years in the future.

The energy necessary to MOVE Bitcoin is proportionate to the portion of the block reward coming from transaction fees. It is the energy of mining going into processing transactions, contracts.

There will be ~210*10^6 total XRN corresponding to the energy necessary to mine each satoshi. (Satoshi's are the smallest unit of Bitcoin 10^-8.)

XRN is pronounced ‘ssssss’.
As in, "wow that contract cost 8 ssss per op. wtf?"

In each step of the MOAT Sale fewer XRN are available.

Bitcoin mining has already been consuming a significant portion of the world’s energy.

This activity already is recorded on chain (we have an immutable cryptographic record of a significant portion of the worlds energy consumption going back years but it’s not structured in a useful way.)

In this way we'll unlock the energy from the past that's has gone into creating Bitcoin up until this point in time by using it to make this valuable data store usable in the future.

"If our plan works a chain will unwind."

The Sale

Tokens will be allocated thus:
10% Will go to the CryptoCastle which will serve as the Shephard institution for the MOAT mining protocol
20% Will go to the founding team of engineers.
10% Will go toward community grants
60% Will be available in the crowdsale
• the amount of XRN available in the token allocation and sale will depend on the block in which the sale contract is deployed.
• The amount of XRN correspond directly to the amount energy used to mine the amount of bitcoin mined up until that block inclusive.

• 30% of sale tokens will be available in the presale round
• 25% in round one
• 20% in round two
• 15% in round three
• 10% in round four

The price of XRN in each round will depend on the amount of BSV contributed to buy XRN.

The remaining XRN will be mined over time and rewarded to bitcoin miners, other power use attestants, and oracle participants.

++
Mining is the outpoint for all the energy that goes into Bitcoin and of course it's also how transactions are processed. So it's the outpoint that cointains all the other outpoints. If we are tracking the energetics of mining on chain we are also tracking the energetics of transactions, smart contracts, computation. As Bitcoin becomes global infrastructure we have presented yet another stack of use-cases: over time this data gives us a picture of the energetics of everything happening in the economy, creating an energy oracle, the foundation for a new set of power protocols.

In order for our plan to work we need, as with the pipe network, we need to measure in-points as well as out-points to do power flow analysis.
Mining as it consumes such a significant, diverse, dispersed portion of world power production is a sufficient outpoint. We need an in-point.
The CryptoCastle will be the initiatory physical anchor and "in-point" of the MOAT network. Cuz every castle needs a moat.

Our plan is to work from this single physical place, the CryptoCastle in San Francisco outward into San Francisco hottest neighborhood: the CryptoHood. The CryptoHood is the neighborhood around the CryptoCastle where work with denizens and community partners on our p2p microgrid has already begun.

But this is personal. It isn't about Satoshi's Power, or Bitcoin's Power. And this isn't about your neighbors' power. This is about your power.

In order to achieve the granularity we need to build the energy oracle and the impact we want to have on the world we want you to give your own power attestations and we'll give you personal power accounting software that will help you see your own power. We think that once you see your own power (consumption and use patterns), you'll wake up and realize: it's you who has the power.

Our ultimate vision is for you to be able to transfer power, real electricity person-to-person wirelessly using witricity.

We are not merely consumers at the edges drawing power down from the centralized grid. Most of us never go anywhere without our personal power pack in our pocket. We're like walking packs of power. But we have lacked a way to exchange this power as peers with other people without an intermediating third party.

A purely peer-to-peer electric cash system would allow power to be sent from one person to another without the need for a third party.

Miners changed the world by using Bitcoin to show people that together we have the power to change the meaning of money.

"People act as if money actually does make the world go ‘round — as if it is a part of nature, not a human invention. Life and death decisions are made on this basis. But the prisons we live in are the work of our own hands: they are human inventions [like the locks on Bitcoin]. They cannot exist without us. We can only liberate ourselves by realizing we are our own jailers. We create and sustain these systems by participating in them and believing in them. Remembering this is the key to freeing ourselves: what restricts us, ultimately, is not lack of a tool, a language, or a medium of exchange, but a way of thinking. These prisons are prisons of the mind. In order to free ourselves we

need to free our minds. Money is the largest check on human self-efficacy. Removing this check is the key to unlocking human potential. In this sense, this movement is about breaking money not making money. By demonstrating that money can be reinvented, Bitcoin and its movement rewaken people to their essential capacity to create and transmit value."

Ultimately this is about achieving a shift in consciousness.

So much of our work has focused on empowering people. On bringing the power to the people. On bringing the power of Bitcoin to you. But this is a turning point. We wanna flip the switch. This isn't about Satoshi's Power, or Bitcoin's Power. This is about your power. Now, we wanna bring the power FROM the people. Because the power is in you. We want to reawaken you to your own power. We hope that once you realize that it's you who's had the power, and that you can wield Bitcoin full-power, that we will be able to solve a lot more problems together. We're excited to set out on this adventure, and strike the spark of this era. The fact that you're reading this now means we think you're one of the people who will help us turn this spark into a fire. We hope one day soon you'll give an attestation of your own power on the chain and show the world that this is the power each of us has inside ... it's going to be a wild ride!

==========

Thank you to Jaeson Booker, Eli Sakov, Clarke Hughes, Alex May, and Chris Calderon for talking through the ideas in this paper with me.