Playing with Fire: Adjusting Bitcoin's Block Subsidy

Anthony Towns

Scaling Bitcoin, 2018

Apologies

- First an apology: this was a terrible title
- Twitter feedback:
  - "I just want to remind everyone that @ScalingBitcoin has become a complete ****ing joke."
  - `https://twitter.com/brian_trollz/status/1030934979885322241`
- Rusty's Civil War thesis:
  - "The Third Era Will Start With Civil War – The mathematics of this situation seem inevitable: The miners and businesses with large transaction volume will both decide to (re)introduce inflation."
  - `https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a`

Apologies

- First an apology: this was a terrible title
- Twitter feedback:
  - “I just want to remind everyone that @ScalingBitcoin has become a complete ****ing joke.”
  - https://twitter.com/brian_trollz/status/1030934979885322241
- Rusty’s Civil War thesis:
  - “The Third Era Will Start With Civil War – The mathematics of this situation seem inevitable: The miners and businesses with large transaction volume will both decide to (re)introduce inflation.”
  - https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a

Apologies

- First an apology: this was a terrible title
- Twitter feedback:
    - "I just want to remind everyone that @ScalingBitcoin has become a complete ****ing joke."
    - https://twitter.com/brian_trollz/status/1030934979885322241
- Rusty's Civil War thesis:
    - "The Third Era Will Start With Civil War – The mathematics of this situation seem inevitable: The miners and businesses with large transaction volume will both decide to (re)introduce inflation."
    - https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a

Apologies

- First an apology: this was a terrible title
- Twitter feedback:
  - "I just want to remind everyone that @ScalingBitcoin has become a complete ****ing joke."
  - `https://twitter.com/brian_trollz/status/1030934979885322241`
- Rusty's Civil War thesis:
  - "The Third Era Will Start With Civil War – The mathematics of this situation seem inevitable: The miners and businesses with large transaction volume will both decide to (re)introduce inflation."
  - `https://medium.com/@rusty_lightning/the-three-economic-eras-of-bitcoin-d43bf0cf058a`

Not a pro-inflation talk

- This is not a pro-inflation talk.
- Other disclaimers:
  - This is not endorsed by Xapo
  - This is not endorsed by Bitcoin Core
  - This is not even necessarily endorsed by me

Not a pro-inflation talk

- This is not a pro-inflation talk.
- Other disclaimers:
  - This is not endorsed by Xapo
  - This is not endorsed by Bitcoin Core
  - This is not even necessarily endorsed by me

Not a pro-inflation talk

- This is not a pro-inflation talk.
- Other disclaimers:
  - This is not endorsed by Xapo
  - This is not endorsed by Bitcoin Core
  - This is not even necessarily endorsed by me

Not a pro-inflation talk

- This is not a pro-inflation talk.
- Other disclaimers:
  - This is not endorsed by Xapo
  - This is not endorsed by Bitcoin Core
  - This is not even necessarily endorsed by me

Not a pro-inflation talk

- This is not a pro-inflation talk.
- Other disclaimers:
  - This is not endorsed by Xapo
  - This is not endorsed by Bitcoin Core
  - This is not even necessarily endorsed by me

What is this talk?

- My intent:
    - I've seen a potential problem
    - I've seen a potential fix
    - We should discuss whether it's a real problem, a real fix, and consider it.
- In decentralised development, review is critical:
    - Both to avoid letting bad things get in
    - But also to avoid forgetting about good things
    - This doesn't just apply to code!

What is this talk?

- My intent:
  - I've seen a potential problem
  - I've seen a potential fix
  - We should discuss whether it's a real problem, a real fix, and consider it.
- In decentralised development, review is critical:
  - Both to avoid letting bad things get in
  - But also to avoid forgetting about good things
  - This doesn't just apply to code!

Does Bitcoin use too much energy?

- Jumping from one fiasco to another...
  - At least it's the *right* fiasco...
- Subsidising blocks with brand new money has two benefits:
  - a decentralised initial distribution of the currency (vs a pre-mine or auction)
  - subsidising payment for proof-of-work security (vs transaction fees)
- To be clear: saying Bitcoin *uses too much energy* is saying it should be *less secure*.

Does Bitcoin use too much energy?

- Jumping from one fiasco to another...
  - At least it's the *right* fiasco...
- Subsidising blocks with brand new money has two benefits:
  - a decentralised initial distribution of the currency (vs a pre-mine or auction)
  - subsidising payment for proof-of-work security (vs transaction fees)
- To be clear: saying Bitcoin *uses too much energy* is saying it should be *less secure*.

Does Bitcoin use too much energy?

- Jumping from one fiasco to another...
  - At least it's the *right* fiasco...
- Subsidising blocks with brand new money has two benefits:
  - a decentralised initial distribution of the currency (vs a pre-mine or auction)
  - subsidising payment for proof-of-work security (vs transaction fees)
- To be clear: saying Bitcoin *uses too much energy* is saying it should be *less secure*.

Does Bitcoin use too much energy?

- Jumping from one fiasco to another...
  - At least it's the *right* fiasco...
- Subsidising blocks with brand new money has two benefits:
  - a decentralised initial distribution of the currency (vs a pre-mine or auction)
  - subsidising payment for proof-of-work security (vs transaction fees)
- To be clear: saying Bitcoin *uses too much energy* is saying it should be *less secure*.

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a “bear” market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a “bear” market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a “bear” market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a "bear" market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a “bear” market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

Anecdata

- Why might you even think Bitcoin uses too much energy?
  - Mainstream news paying attention to the problem?
  - Industry profits centred around mining rather than other value adds?
  - 7x increase in PoW during a “bear” market?
  - Coins with less PoW not getting attacked?
  - No concern from paranoid users about lack of security?

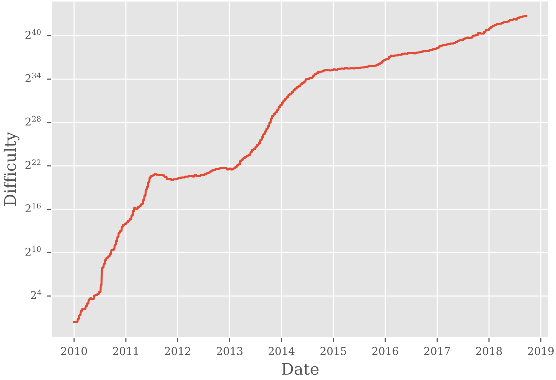
Maths

- Can we analyse this in some objective way?
- Obviously yes:
  - Hashrate: TH/s or difficulty
  - Electricity: kWh/year or GW
  - Value: Money (USD)

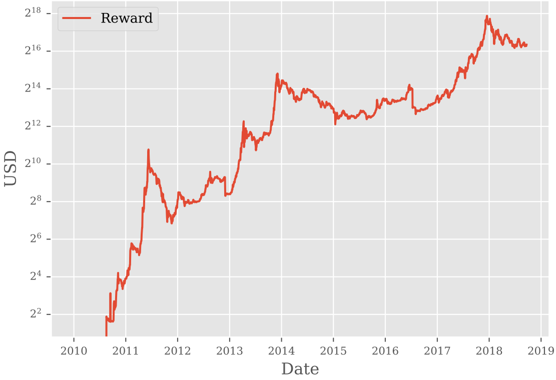
Maths

- Can we analyse this in some objective way?
- Obviously yes:
  - Hashrate: TH/s or difficulty
  - Electricity: kWh/year or GW
  - Value: Money (USD)

Hashrate/Difficulty

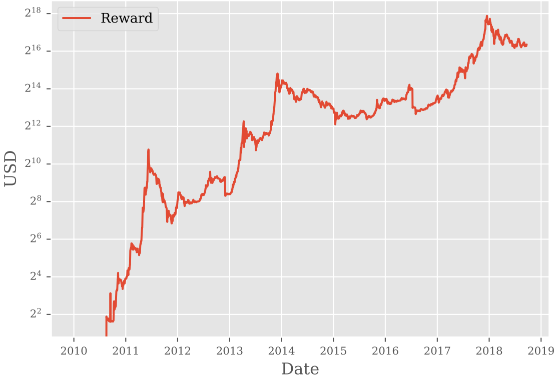


Value/USD



- Problem: tells you what you pay for, not what you get.

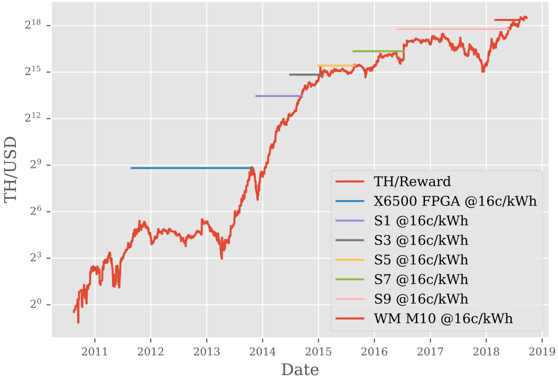
Value/USD



- Problem: tells you what you pay for, not what you get.

Hashrate vs Value

- Combine the two measures of security: TH/USD



Hashrate vs Value

- TH/USD:
  - Goes up and to the right as technology improves
  - TH/Reward measures how hard you have to work to earn revenue
  - Miner values measure how much work you get at a given electricity price
  - Not subjective!
- Gives insight into market reaction:
  - Reward halvening makes TH/Reward double
  - Price increases makes TH/Reward drop
  - Can see TH/Reward increases as new hardware comes to market

Hashrate vs Value

- TH/USD:
    - Goes up and to the right as technology improves
    - TH/Reward measures how hard you have to work to earn revenue
    - Miner values measure how much work you get at a given electricity price
    - Not subjective!
- Gives insight into market reaction:
    - Reward halvening makes TH/Reward double
    - Price increases makes TH/Reward drop
    - Can see TH/Reward increases as new hardware comes to market

Hashrate vs Value

- Aside: 16c/kWh – that seems expensive!
- Why:
    - Includes other Opex costs (cooling, staffing, etc)
    - Includes Capex not just Opex
    - Includes expected profits
    - Needs to cover risk that difficulty will rise faster than expected
    - Mining isn't a completely efficient market
- My guess:
    - 4c/kWh electricity
    - 1c/kWh misc opex
    - 6c/kWh depreciation of capex
    - 5c/kWh profit and risk premium

Hashrate vs Value

- Aside: 16c/kWh – that seems expensive!
- Why:
  - Includes other Opex costs (cooling, staffing, etc)
  - Includes Capex not just Opex
  - Includes expected profits
  - Needs to cover risk that difficulty will rise faster than expected
  - Mining isn't a completely efficient market
- My guess:
  - 4c/kWh electricity
  - 1c/kWh misc opex
  - 6c/kWh depreciation of capex
  - 5c/kWh profit and risk premium

Hashrate vs Value

- Aside: 16c/kWh – that seems expensive!
- Why:
    - Includes other Opex costs (cooling, staffing, etc)
    - Includes Capex not just Opex
    - Includes expected profits
    - Needs to cover risk that difficulty will rise faster than expected
    - Mining isn't a completely efficient market
- My guess:
    - 4c/kWh electricity
    - 1c/kWh misc opex
    - 6c/kWh depreciation of capex
    - 5c/kWh profit and risk premium

Predictions

- Can we make any predictions based on this?
- Yes, but we need to make some assumptions:
    - Where will the price go?
    - How much more efficient will miners get?
    - Will "electricity" get cheaper?

Predictions

- Can we make any predictions based on this?
- Yes, but we need to make some assumptions:
  - Where will the price go?
  - How much more efficient will miners get?
  - Will "electricity" get cheaper?

Predictions

- Can we make any predictions based on this?
- Yes, but we need to make some assumptions:
  - Where will the price go?
  - How much more efficient will miners get?
  - Will "electricity" get cheaper?

Predictions

- Can we make any predictions based on this?
- Yes, but we need to make some assumptions:
  - Where will the price go?
  - How much more efficient will miners get?
  - Will “electricity” get cheaper?

Predictions

- Can we make any predictions based on this?
- Yes, but we need to make some assumptions:
  - Where will the price go?
  - How much more efficient will miners get?
  - Will "electricity" get cheaper?

Assumptions - Price

- Price model:
  - Assume Bitcoin succeeds (if it fails, energy use won't be an issue)
  - But try to be conservative
  - Log-log curve fit, scaled down to act as a lower support
  - Sub-exponential, but still gives huge price rises over time
    - Over \$10k by 2022, over \$20k by mid-2023
    - Over \$100k in 2028, over \$500k in 2034
    - Over \$1M in 2037, over \$2M in 2041
    - Almost \$8M by 2050
  - Too conservative? “Support” as at 2018-10-06 is at \$1980 USD
    - (Multiply by 2.91 to get back to actual fitted curve)

Assumptions - Price

- Price model:
  - Assume Bitcoin succeeds (if it fails, energy use won't be an issue)
  - But try to be conservative
  - Log-log curve fit, scaled down to act as a lower support
  - Sub-exponential, but still gives huge price rises over time
    - Over $10k by 2022, over $20k by mid-2023
    - Over $100k in 2028, over $500k in 2034
    - Over $1M in 2037, over $2M in 2041
    - Almost $8M by 2050
  - Too conservative? "Support" as at 2018-10-06 is at $1980 USD
    - (Multiply by 2.91 to get back to actual fitted curve)

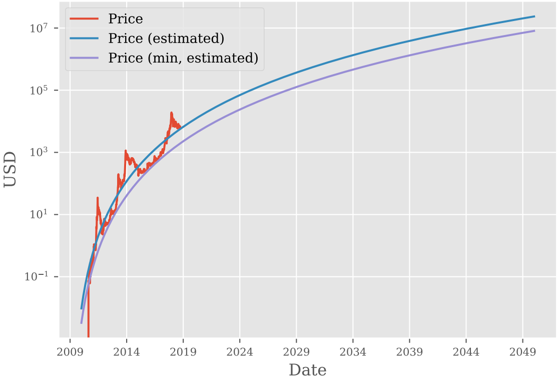
Assumptions - Price

- Price model:
    - Assume Bitcoin succeeds (if it fails, energy use won't be an issue)
    - But try to be conservative
    - Log-log curve fit, scaled down to act as a lower support
    - Sub-exponential, but still gives huge price rises over time
        - Over $10k by 2022, over $20k by mid-2023
        - Over $100k in 2028, over $500k in 2034
        - Over $1M in 2037, over $2M in 2041
        - Almost $8M by 2050
    - Too conservative? "Support" as at 2018-10-06 is at $1980 USD
        - (Multiply by 2.91 to get back to actual fitted curve)

Assumptions - Price

- Price model:
  - Assume Bitcoin succeeds (if it fails, energy use won't be an issue)
  - But try to be conservative
  - Log-log curve fit, scaled down to act as a lower support
  - Sub-exponential, but still gives huge price rises over time
    - Over \$10k by 2022, over \$20k by mid-2023
    - Over \$100k in 2028, over \$500k in 2034
    - Over \$1M in 2037, over \$2M in 2041
    - Almost \$8M by 2050
  - Too conservative? "Support" as at 2018-10-06 is at \$1980 USD
    - (Multiply by 2.91 to get back to actual fitted curve)

Assumptions - Price



Assumptions - Miner efficiency / Energy costs

- Rough fit of TH/USD
- Split into miner efficiency improvements, and decreasing "electricity" costs
  - More efficient miners from better fabs / process improvements
  - Cheaper "electricity" directly, or due to less manufacturer profits, or due to use of miners as heating elements, eg
- These are not good estimates.

Assumptions - Miner efficiency / Energy costs

- Rough fit of TH/USD
- Split into miner efficiency improvements, and decreasing "electricity" costs
  - More efficient miners from better fabs / process improvements
  - Cheaper "electricity" directly, or due to less manufacturer profits, or due to use of miners as heating elements, eg
- These are not good estimates.

Assumptions - Miner efficiency / Energy costs

- Rough fit of TH/USD
- Split into miner efficiency improvements, and decreasing "electricity" costs
    - More efficient miners from better fabs / process improvements
    - Cheaper "electricity" directly, or due to less manufacturer profits, or due to use of miners as heating elements, eg
- These are not good estimates.

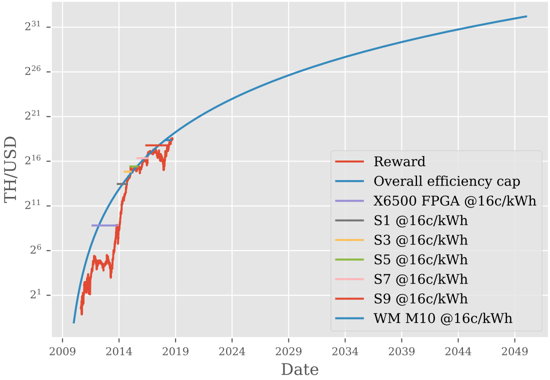
Assumptions - Miner efficiency / Energy costs

- Rough fit of TH/USD
- Split into miner efficiency improvements, and decreasing "electricity" costs
  - More efficient miners from better fabs / process improvements
  - Cheaper "electricity" directly, or due to less manufacturer profits, or due to use of miners as heating elements, eg
- These are not good estimates.

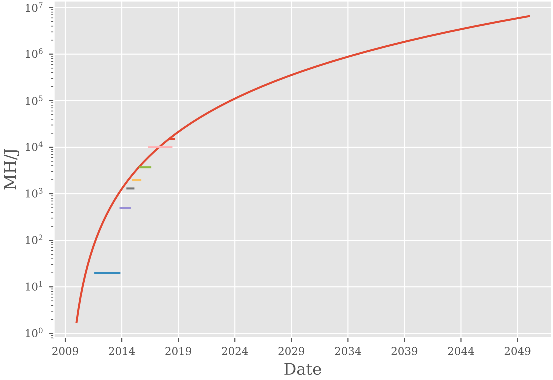
Assumptions - Miner efficiency / Energy costs

- Rough fit of TH/USD
- Split into miner efficiency improvements, and decreasing "electricity" costs
  - More efficient miners from better fabs / process improvements
  - Cheaper "electricity" directly, or due to less manufacturer profits, or due to use of miners as heating elements, eg
- These are not good estimates.

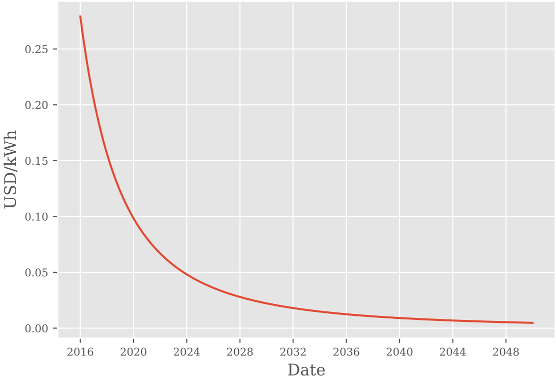
Assumptions - TH/USD



Assumptions - Miner efficiency



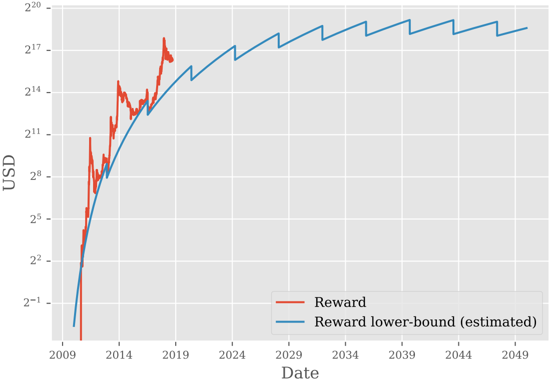
Assumptions - Energy costs



Predictions

- So we have some assumptions. What can we predict from them?

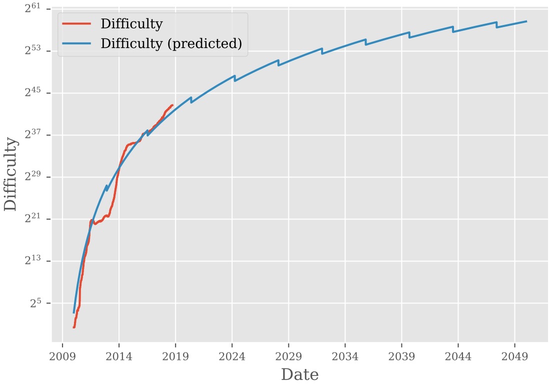
Predictions - Reward in USD



Predictions - Reward in USD

- Things to note:
  - Only relies on the price assumption
  - Even over a 30 year timeline (2019-2049), decreasing reward in BTC is mostly compensated for by growth in BTC price
  - This is a simple result of the price doubling faster than the block reward halves
  - Those little shocks at halvenings look a lot worse when you don't use a log scale

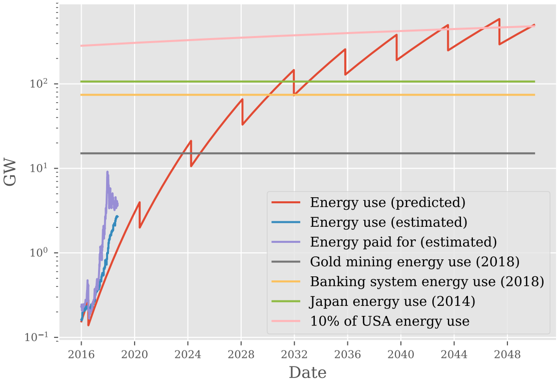
Predictions - Difficulty



Predictions - Difficulty

- Relies on assumptions about price and TH/USD
- Assumes that difficulty immediately responds to price/technology changes
  - (Not economically unreasonable, given they're assumed to be perfectly predictable)
  - (Technically unreasonable, given difficulty only adjusts every two weeks though
- Assumes the mining market is efficient and there's no profit/rents
  - (Beyond what's implicit in the "electricity" price)

Predictions - Electricity Usage



Predictions - Electricity Usage

- Relies on all the assumptions: price, efficiency, and energy cost.
- Electricity usage increases even though reward in USD does not – because we assumed “electricity” prices decrease

Predictions - Summary

- Garbage in / Garbage out
- We started from shakey assumptions, so should not have huge confidence in the predictions
- We don't get to "Bitcoin Mining on Track to Consume All of the World's Energy by 2020"
    - http://www.newsweek.com/bitcoin-mining-track-consume-worlds-energy-2020-744036
- But we do get to levels that seem high enough to justify thinking about reducing them.

Reducing Energy Usage

- The talk title is an obvious give away about how to go about reducing energy usage:
- When the price of BTC goes up, lower the reward to compensate.
- Because the overall reward in real terms does not go up as much, there's less incentive to deploy lots of new mining hardware.
- Slower deployment of new mining hardware means less growth in electricity usage.

Reducing Energy Usage

- The talk title is an obvious give away about how to go about reducing energy usage:
- When the price of BTC goes up, lower the reward to compensate.
- Because the overall reward in real terms does not go up as much, there's less incentive to deploy lots of new mining hardware.
- Slower deployment of new mining hardware means less growth in electricity usage.

Reducing Energy Usage

- The talk title is an obvious give away about how to go about reducing energy usage:
- When the price of BTC goes up, lower the reward to compensate.
- Because the overall reward in real terms does not go up as much, there's less incentive to deploy lots of new mining hardware.
- Slower deployment of new mining hardware means less growth in electricity usage.

Reducing Energy Usage

- The talk title is an obvious give away about how to go about reducing energy usage:
- When the price of BTC goes up, lower the reward to compensate.
- Because the overall reward in real terms does not go up as much, there's less incentive to deploy lots of new mining hardware.
- Slower deployment of new mining hardware means less growth in electricity usage.

Reducing Energy Usage

- But! The block reward is decided by software which doesn't know the BTC price
- But! It can detect rises in price indirectly, because people deploy more hardware and the difficulty rises.
- There is no "recursion" problem here, provided:
  - miners can predict the drop in reward that will result from higher difficulty
  - we don't try to cut the reward by exactly as much as the price increases

Reducing Energy Usage

- But! The block reward is decided by software which doesn't know the BTC price
- But! It can detect rises in price indirectly, because people deploy more hardware and the difficulty rises.
- There is no "recursion" problem here, provided:
  - miners can predict the drop in reward that will result from higher difficulty
  - we don't try to cut the reward by exactly as much as the price increases

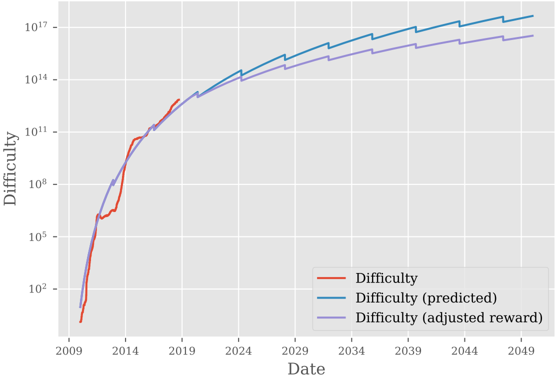
Reducing Energy Usage

- But! The block reward is decided by software which doesn't know the BTC price
- But! It can detect rises in price indirectly, because people deploy more hardware and the difficulty rises.
- There is no "recursion" problem here, provided:
  - miners can predict the drop in reward that will result from higher difficulty
  - we don't try to cut the reward by exactly as much as the price increases

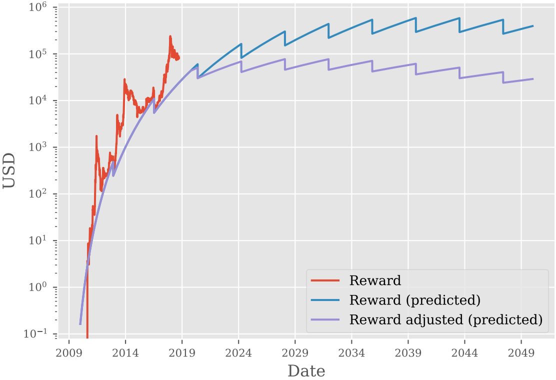
Reducing Energy Usage

- A concrete example: Cut the reward by 20% everytime difficulty doubles
  - Easy to calculate reward given block height and difficulty
  - Consistent behaviour no matter when the rule gets put in place
  - Exponential formula makes the math work out fairly nicely
  - Only applies once difficulty is above 10e12

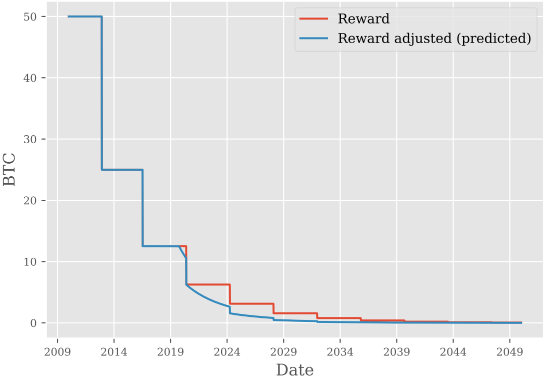
Reducing Energy Usage - Comparison



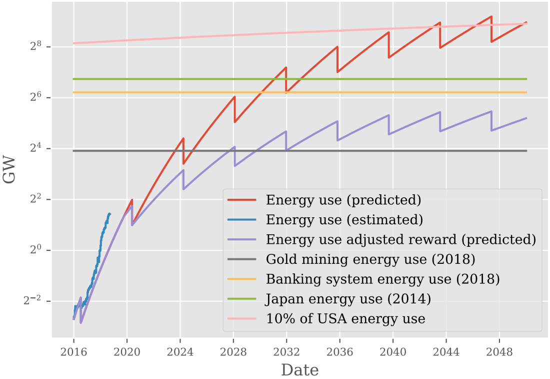
Reducing Energy Usage - Comparison



Reducing Energy Usage - Comparison



Reducing Energy Usage - Comparison



Implementation

- Reducing block reward is a soft-fork:
  - Limit what miners can claim based on the difficulty
  - Require them to burn the rest to an OP_RETURN address
- Can we keep the reward?
  - Seems wasteful not to
  - Would allow increased inflation later in Bitcoin's life when price growth slows
  - Might defer the "civil war" even further

Implementation

- Reducing block reward is a soft-fork:
  - Limit what miners can claim based on the difficulty
  - Require them to burn the rest to an OP_RETURN address
- Can we keep the reward?
  - Seems wasteful not to
  - Would allow increased inflation later in Bitcoin's life when price growth slows
  - Might defer the "civil war" even further

Implementation - Pay It Forward

- Approach: have a "miner's savings trust" UTXO
- "Burned" rewards from coinbase pay into it
- Someday, take fees from it to supplement the coinbase reward
- Consensus rules specify the amounts that each block can "withdraw" and must "deposit"

Implementation - Pay It Forward

- Approach: have a “miner’s savings trust” UTXO
- “Burned” rewards from coinbase pay into it
- Someday, take fees from it to supplement the coinbase reward
- Consensus rules specify the amounts that each block can “withdraw” and must “deposit”

Implementation - Pay It Forward

- Approach: have a "miner's savings trust" UTXO
- "Burned" rewards from coinbase pay into it
- Someday, take fees from it to supplement the coinbase reward
- Consensus rules specify the amounts that each block can "withdraw" and must "deposit"

Implementation - Pay It Forward

- Approach: have a “miner’s savings trust” UTXO
- “Burned” rewards from coinbase pay into it
- Someday, take fees from it to supplement the coinbase reward
- Consensus rules specify the amounts that each block can “withdraw” and must “deposit”

Implementation - Rules

- Each coinbase spends burned rewards to a scriptPubkey "100 OP_CSV"
- Each block contains a "savings" transaction:
  - Single output: "1 OP_CSV"
  - Inputs are (1) previous block's savings tx's output, (2) coinbase burn output from 100 blocks ago
- Consensus rules validate:
  - Coinbase burn is (at least) some appropriate value (soft-forkable up)
  - Savings fees are (no more than) some appropriate value (soft-forkable down)
- Nodes validating these rules need to only track an additional 100 UTXOs (one for each coinbase burn for the past 100 blocks) at any given point in time.

Implementation - Rules

- Each coinbase spends burned rewards to a scriptPubkey “100 OP_CSV”
- Each block contains a “savings” transaction:
  - Single output: “1 OP_CSV”
  - Inputs are (1) previous block's savings tx's output, (2) coinbase burn output from 100 blocks ago
- Consensus rules validate:
  - Coinbase burn is (at least) some appropriate value (soft-forkable up)
  - Savings fees are (no more than) some appropriate value (soft-forkable down)
- Nodes validating these rules need to only track an additional 100 UTXOs (one for each coinbase burn for the past 100 blocks) at any given point in time.

Implementation - Rules

- Each coinbase spends burned rewards to a scriptPubkey “100 OP_CSV”
- Each block contains a “savings” transaction:
  - Single output: “1 OP_CSV”
  - Inputs are (1) previous block's savings tx's output, (2) coinbase burn output from 100 blocks ago
- Consensus rules validate:
  - Coinbase burn is (at least) some appropriate value (soft-forkable up)
  - Savings fees are (no more than) some appropriate value (soft-forkable down)
- Nodes validating these rules need to only track an additional 100 UTXOs (one for each coinbase burn for the past 100 blocks) at any given point in time.

Implementation - Rules

- Each coinbase spends burned rewards to a scriptPubkey "100 OP_CSV"
- Each block contains a "savings" transaction:
  - Single output: "1 OP_CSV"
  - Inputs are (1) previous block's savings tx's output, (2) coinbase burn output from 100 blocks ago
- Consensus rules validate:
  - Coinbase burn is (at least) some appropriate value (soft-forkable up)
  - Savings fees are (no more than) some appropriate value (soft-forkable down)
- Nodes validating these rules need to only track an additional 100 UTXOs (one for each coinbase burn for the past 100 blocks) at any given point in time.

Pay It Forward - Other Uses

- This approach has a variety of potential uses:
  - Smothing the halvening schedule
  - Smoothing fee income when a fee market eventuates
  - As a cost mechanism for allowing temporary increases in the block weight limit

Pay It Forward - Other Uses

- This approach has a variety of potential uses:
  - Smothing the halvening schedule
  - Smoothing fee income when a fee market eventuates
  - As a cost mechanism for allowing temporary increases in the block weight limit

Pay It Forward - Other Uses

- This approach has a variety of potential uses:
  - Smothing the halvening schedule
  - Smoothing fee income when a fee market eventuates
  - As a cost mechanism for allowing temporary increases in the block weight limit

Other approaches

- Even if these are real problems, there are other approaches to dealing with (some of) them.
- For instance, perhaps the invisible hand of the market will already solve all these problems naturally:
  - Lower rewards will increase the price, perhaps enough to compensate?
  - Perhaps mining manufactures will make the most profit by delaying new hardware until the halvening when everyone needs to upgrade?
  - Maybe electricity will get more expensive
  - Maybe 10% of US eletricity usage just means all mining is done by hot water systems and there is no problem
- Alternatively, if there is a crisis due to too much investment, that can be undone by changing the PoW algorithm, rendering historical investment void.

Other approaches

- Even if these are real problems, there are other approaches to dealing with (some of) them.
- For instance, perhaps the invisible hand of the market will already solve all these problems naturally:
  - Lower rewards will increase the price, perhaps enough to compensate?
  - Perhaps mining manufactures will make the most profit by delaying new hardware until the halvening when everyone needs to upgrade?
  - Maybe electricity will get more expensive
  - Maybe 10% of US eletricity usage just means all mining is done by hot water systems and there is no problem
- Alternatively, if there is a crisis due to too much investment, that can be undone by changing the PoW algorithm, rendering historical investment void.

Other approaches

- Even if these are real problems, there are other approaches to dealing with (some of) them.
- For instance, perhaps the invisible hand of the market will already solve all these problems naturally:
  - Lower rewards will increase the price, perhaps enough to compensate?
  - Perhaps mining manufactures will make the most profit by delaying new hardware until the halvening when everyone needs to upgrade?
  - Maybe electricity will get more expensive
  - Maybe 10% of US eletricity usage just means all mining is done by hot water systems and there is no problem
- Alternatively, if there is a crisis due to too much investment, that can be undone by changing the PoW algorithm, rendering historical investment void.

Other Benefits

- Some people claim that halving the reward will force the price to double, as a result of supply/demand
- Even if it doesn't exactly double, less supply with the same demand seems like it would force the price to rise.
- Perhaps that is a reason for Bitcoin hodl'ers to want to reduce inflation sooner rather than later, independent of concerns about energy usage or sustainability.
- (If the price really will double everytime the reward halves; I vote we halve the reward every day for the next two weeks!)

Other Benefits

- Some people claim that halving the reward will force the price to double, as a result of supply/demand
- Even if it doesn't exactly double, less supply with the same demand seems like it would force the price to rise.
- Perhaps that is a reason for Bitcoin hodl'ers to want to reduce inflation sooner rather than later, independent of concerns about energy usage or sustainability.
- (If the price really will double everytime the reward halves; I vote we halve the reward every day for the next two weeks!)

Other Benefits

- Some people claim that halving the reward will force the price to double, as a result of supply/demand
- Even if it doesn't exactly double, less supply with the same demand seems like it would force the price to rise.
- Perhaps that is a reason for Bitcoin hodl'ers to want to reduce inflation sooner rather than later, independent of concerns about energy usage or sustainability.
- (If the price really will double everytime the reward halves; I vote we halve the reward every day for the next two weeks!)

Other Benefits

- Some people claim that halving the reward will force the price to double, as a result of supply/demand
- Even if it doesn't exactly double, less supply with the same demand seems like it would force the price to rise.
- Perhaps that is a reason for Bitcoin hodl'ers to want to reduce inflation sooner rather than later, independent of concerns about energy usage or sustainability.
- (If the price really will double everytime the reward halves; I vote we halve the reward every day for the next two weeks!)

Other Costs

- This is probably not a win-win-win scenario.
- Some people will lose out:
    - Less energy use by miners means less mining hardware means less growth opportunities for miner manufacturers
    - Lowering rewards as difficulty increases means equilibrium will be hit faster, reducing excess profits for miners
- Maybe those losses are compensated by reducing the risk of black swan catastrophes such as:
    - Bitcoin economy deciding to switch to a different PoW
    - Governments legislating against mining in order to reduce energy usage

Conclusion

- Open questions:
  - Are there reasonable ways of making better assumptions than the ones I made?
  - How robust are the predictions with different assumptions?
  - What is the likely impact on parts of the industry in real terms?
  - Is there a reasonable way to define the "burn" and "fee" formulas for pay-it-forward savings, that remains simple with future soft-forks?
  - Is an implementation actually feasible?
- Thanks for your time!
  - Slides and ipynb data sources will be up at `https://github.com/ajtowns/sc-btc-2018`

Conclusion

- Open questions:
  - Are there reasonable ways of making better assumptions than the ones I made?
  - How robust are the predictions with different assumptions?
  - What is the likely impact on parts of the industry in real terms?
  - Is there a reasonable way to define the "burn" and "fee" formulas for pay-it-forward savings, that remains simple with future soft-forks?
  - Is an implementation actually feasible?
- Thanks for your time!
  - Slides and ipynb data sources will be up at `https://github.com/ajtowns/sc-btc-2018`