@ProjectBabbage's Latest Attack on Bitcoin

Savings, validation and another dose of my way

Opinion | 1 November 2026 | @BitcoinSvGuide | https://bitcoinsv.guide/wp-content/uploads/2026/11/ProjectBabbage_Latest_Attack_on_Bitcoin.pdf

Bitcoin should not make saving money a disadvantage. Nor should its future depend on miners assuming somebody else has checked the work. Yet that is the dangerous direction I see in Ty Everett's latest public pitch.



In his Halloween video, @ProjectBabbage describes a miner arriving without checking the historical blockchain, building a limited record from newly accepted transactions, and mining spends from the outputs it knows. He predicts indexers will disappear and suggests people who object are frightened of scalable Bitcoin. [1]

I consider this an attack on Bitcoin's purpose. Not a deployed attack that has already stranded savings, but public encouragement of a direction that could weaken validation and make long-held money less convenient to use. We do not have to wait for the damage before challenging it.

1 Who does the work while you collect the reward

Think of the familiar "Empty Block Miner," but with a different shortcut. Instead of leaving out all ordinary transactions, this miner includes only spends from outputs it has observed since joining, leaving older, unknown outputs to other miners. I call this **"NewTxOnly mining."** "New" refers to the miner's records—not newly issued coins.

The common concern is collecting block rewards while leaving part of the work to others.

The mining puzzle does not become easier. The potential shortcut is in the infrastructure and checking behind it. A miner could avoid some historical setup work, rely on transactions accepted by others, and still compete for the block subsidy and selected transaction fees.

That creates an obvious question: **what happens if leaving that work to others becomes the more profitable approach?**

Whether those savings outweigh the fees forgone has not been established by the video. But the question does not disappear because a smaller miner might initially process fewer payments. If the approach becomes attractive and spreads, who keeps paying for the work everybody else assumes will be done?

2 Somebody else checked is not a security argument

The whitepaper says nodes accept a block only when its transactions are valid and not already spent. Its simplified verification method is described separately and relies on honest nodes. [2]

Skipping a replay from genesis is not, by itself, proof of unsafe mining. The unanswered question is how Ty's miner checks other miners' blocks when those blocks spend coins missing from its own records. He does not show how it detects bad blocks or recovers when the others get it wrong.

If miners can earn most fees without checking older spends, what preserves the incentive to do that checking? A miner missing the necessary records cannot independently distinguish a legitimate old spend from a fabricated or already-spent output merely by watching others accept it. If enough miners blindly follow, they could extend an invalid branch.

In BSV's own model, the nodes responsible for enforcing these rules are miners. If most mining power follows blocks without fully checking them, **which miners are still enforcing the rules, and how much mining power stands behind them?** The remaining fully validating miners would reject an invalid branch; greater hashpower would not make it valid. But those miners could find themselves outpaced by a majority building on blocks it cannot independently verify. **That is a potential network split—not a validation problem solved by pointing to somebody else.**

Peter Todd raised the underlying incentive danger in 2015: miners relying on others' validation could become more attractive when they could also collect transaction fees. He warned that validation failures could spread through miners building on an invalid chain. That was a warning about a different design, not proof that Ty's proposal is identical to SegWit. **The relevant question is the same: what happens when too many miners depend on somebody else doing the checking?** [3]

Wasn't this what overlays were supposed to address?

BSVA's own documentation explains that overlays let users retrieve transaction data ***"without having to index all block data."*** Applications can use specialized services instead of each searching the entire blockchain. That is already an approach to dividing the work. [8]

But choosing which transactions an application needs is different from determining whether another miner's block is valid. **An overlay can focus on its own business. That does not explain how a miner checks a block containing coins absent from its records.**

Ty's argument slides between these different responsibilities. Avoiding universal application indexing does not establish that miners can safely follow blocks they cannot fully check. **What additional problem does his proposal solve—and where is the demonstration that it preserves independent block validation?**

3 Your savings are not obsolete transactions

Imagine saving BSV for ten years. You keep the keys secure. You leave the coins untouched. Then you need the money.

A miner following Ty's limited-record approach might not process your spend because the old output is outside its records. Another miner can still confirm it. Your coins do not become invalid merely because one miner does not know them.

But that reassurance depends on miners willing and able to serve you remaining available. If a substantial share of mining adopts selective coverage, your savings could have fewer confirmation opportunities. If broader service becomes scarce, extra fees or separate arrangements could follow. That is a foreseeable risk, not an existing Bitcoin surcharge.

"They would lose the fees" does not settle the savings question. In a just-in-time payment economy, enormous volumes could circulate through recently created outputs. If those rapidly moving coins generate most transaction fees, missing the occasional spend from older savings might barely dent a partial miner's income. Serving those savings would still carry costs. Whether the extra fees justify those costs—and keep enough miners willing to serve savers—requires evidence. **That is a question to demonstrate, not wave away.**

Teranode's own UTXO Store documentation explicitly recognizes outputs that remain unspent for decades. Its wording is clear:

"…or it may remain unspent for decades, meaning that the unspent outputs must persist for as long as they remain unspent." [7]

Your savings are current ownership records. Their age does not make them obsolete. This does not require every miner to keep every record locally. It does require an answer about how those records remain available and trustworthy when you need your money.

Ty has not proposed an explicit fee for saving. The concern is the economic result if the infrastructure he promotes makes dormant coins less welcome. A saver should not have to keep moving money merely to keep it convenient for service providers.

This is the danger of infrastructure optimized around whatever is moving now: stored wealth becomes somebody else's problem until its owner needs it. Calling that efficient does not answer whether it is good money.

4 A treasury asset must work while it sits in the treasury

Craig Wright's 2018 essay encouraged people to *"move their savings into Bitcoin"* and *"hold their surplus funds in Bitcoin,"* alongside spending and replacing. Saving was part of the argument for use, not an offence against it. [4]

Our strategic-reserve and hybrid-asset articles make the same essential distinction. BSV can serve people transacting continuously and people deliberately holding reserves. Businesses need working balances. Families need savings. Treasury managers need confidence that money held today remains usable when required. [5]

Holding demand could support BSV's value alongside demand for transaction services. Undermining confidence in long-term access risks weakening that demand. This is not a prediction that Ty's proposal will crash the price. It is a warning against damaging one reason people might choose to own BSV at all.

Why promote BSV as infrastructure worth holding, then normalize a direction in which holding it still could make you a second-class customer?

5 More my way before the evidence

We challenged the claims about competing wallets in *Show Us the Scale*. We challenged BRC234's proposed retreat from free indexing coverage in *Let the Builders Compete*. The same question keeps returning: where is the evidence that justifies the pressure? [6]

Now Ty offers another direction without showing a tested implementation in the recording. Then, around 3:40, he says anticipated objections come from people who "don't like scalable Bitcoin" and are "terrified", while framing his own vision as "courageous". Later, support for adaptation becomes something everyone can embrace "if we're here for the right reasons." [1]

Disagreeing with Ty Everett is not opposition to Bitcoin. Wanting savings protected is not fear of scale. These are legitimate questions about the money people own and the validation protecting it. Turning them into a test of courage or loyalty is divisive marketing.

We do not have to wait for the damage

A dangerous direction deserves opposition before it becomes entrenched. Once businesses have reorganized around an incentive, and customers discover the consequences, reversing course becomes harder.

In my view, promoting dependence on others' validation, selective service for older coins and contempt for anticipated critics is a threat to the Bitcoin BSV should be building: money people can use, save and trust to remain usable.

Ty is entitled to develop a different mining architecture. He is not entitled to have its unanswered questions dismissed as other people's fear. His video closes by looking forward to the first miner demonstrating the approach. The sales pitch is already ahead of the demonstration. [1]

Build it. Show how it fails safely. Explain who carries its costs—and what happens to the saver who has not moved a coin in ten years.

Until then, stop treating public confidence in your preferred direction as a substitute for proof.

Bitcoin needs scale that serves its owners. Savers are owners too.

Sources

[1] Ty Everett, Halloween mining video, 31 October 2026. Audio and publisher-verified transcript supplied by the publisher. Transcript below begins at 0:27, omitting the opening 26 seconds. Approximate times: proposal through 2:42; indexers 2:53–3:05; rhetoric 3:40–4:25; closing 4:31–4:54.

[2] Satoshi Nakamoto, Bitcoin whitepaper, sections 5, 7 and 8. Distinguishes block acceptance, storage pruning and simplified payment verification.

[3] Peter Todd, Segregated witnesses and validationless mining, 23 December 2015 UTC. Historical incentive and failure analysis, not a test of Ty's proposal or a verdict on present-day SegWit.

[4] Craig Wright, Hoarding and Bitcoin, 24 September 2018.

[5] BitcoinSvGuide, When Infrastructure Becomes an Asset and Bitcoin's Hybrid Asset Thesis. Economic arguments, not guarantees of price appreciation.

[6] BitcoinSvGuide, Show Us the Scale report collection and Let the Builders Compete.

[7] Teranode, UTXO Store documentation, section 1, Description. Accessed 1 November 2026. The quotation reproduces the end of the sentence verbatim; the opening words are omitted.

[8] BSV Association, Overlay Services, "Overlays at a Glance" and "Infrastructure Dependencies."

Video transcript

https://x.com/ProjectBabbage/status/2116657780883079312/video/1

SPEAKER: Ty Everett

(0:27 – 1:31) <skipped the first 26 seconds – no relevance> I thought maybe we should talk about Bitcoin, because I love Bitcoin and you know, this is the anniversary of the white paper after all. So let's talk about mining. And there's this common claim in Bitcoin mining that the miners have to keep the whole UTXO set around, and that it can be pruned, and that new miners have to go through this process of validation for all blocks. But I actually disagree with that. I think a new miner can come into the system with nothing, with no previous blocks, start listening to new spends, and as they do, they learn, well, you know, if the rest of the network is going to accept this spend, then that makes a new UTXO. And if that UTXO gets included in the new block, then from nothing other than just listening to the current fire hose of transactions over time, they start to build up maybe not a very big subset of the UTXO set for themselves, but they start to build up a little bit. And as long as the rest of the network continues to accept these blocks over time and build on top of them, this miner can actually get pretty confident that, you know, those UTXOs are actually current and valid, the ones that got included into new blocks. And so those UTXOs, when they become spent in new transactions, that miner can actually start to include some of those new transactions into some of their own blocks. And notably, they didn't need to go through a historical process to validate all of them.

(1:32 – 2:42) So, suppose in the future, you know, there's this aggregate of all the miners, and they have all these, you know, UTXOs, and some of them, you know, have more data than others, right? You don't really know how much each person has, but as long as you know that, you know, the UTXOs that you've witnessed to be created and accepted by the rest of the network have now become valid, and as long as you know that you see a new transaction, and it actually spends one of those newly valid UTXOs that you do know about, without any historical knowledge of the blockchain, you can verify that all of this data that you're going to include in your new block, maybe your block can't be quite as expansive as everyone else's, but you can start to build up this authority over time. As more and more new transactions get broadcast, the longer you stick around, the more fee revenue that you earn, even if it's small at the beginning for your new blocks. You can actually start to use that to, you know, to expand, and you can start to include more and more transactions, even if you never went through the process of initially validating the whole blockchain.

(2:43 – 3:16) So, that's my scary controversial take for today on Halloween, and I just wanted to share it with you. So, check out Bitcoin SV, the most scalable blockchain on earth, where not even the miners have to keep everything from the past, and where indexers will ultimately become, in my opinion, a thing of the past as well. You know, because Bitcoin is really, really, really powerful, and lots of people are going to use it, and they're going to create a scary number of transactions over time.

(3:17 – 3:46) So large a number, in fact, that it's going to be, if you want to keep a database of all of them, it's going to be like trying to keep a database of every single IP packet ever sent, and that way, you know, you go back and look through all of them to see, no, no, no, that's just not how it's going to work. We're going to have so many transactions, guys, that no one's going to be able to keep track of all of them, and that's going to make some people mad. But that's because those people don't like scalable Bitcoin, and they're terrified.

(3:47 – 4:03) But you know what? You should be terrified if you don't want a scalable Bitcoin. You should be terrified about what this technology is capable of disrupting. You should be terrified that the things that you may have built your business on, you know, they may not last forever.

(4:04 – 4:25) But courageous people can recognize that's actually a good thing. It means that we have to be adaptable. We have to be willing to change, and we have to be able to do what's necessary to scale Bitcoin for the entire world, and that's something I think we can all get behind if we're here for the right reasons.

(4:26 – 4:57) So, have a happy Halloween, everybody, and happy White Paper Day, and I look forward to seeing the first Bitcoin miner join the BSV network without having to verify every single transaction from the past, because it's possible, and one day it's going to happen, and one day you're not going to be able to get every single one of your previous transactions for free from an indexing service. So, cheers everybody! Okay.