PROPOSING A MASTER KEYCHAIN FOR OFFCHAINS JUST BELOW PARENT BITCOIN

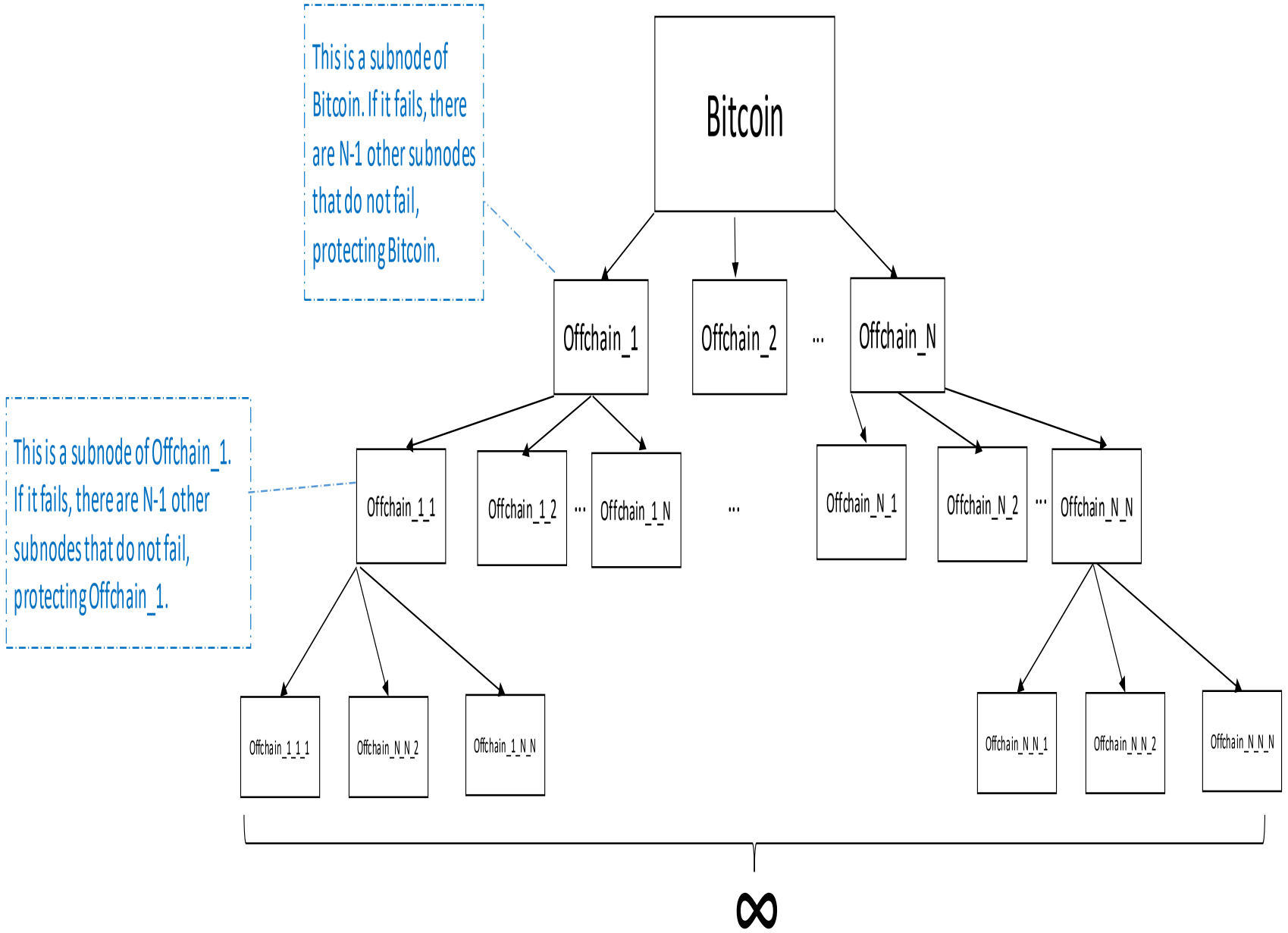
What is the "issue" and is it even an issue?

Bitcoin has a block size limit of 1MB along with a fixed block time of 10 minutes (Bitcoin software back solves based on total hash computing power to fix the block time at 10 minutes – i.e. if hash processing capacity increases, they lower the odds of getting the right hash; if processing capacity decreases, they increase the odds of getting the right hash, pegging the block time to 10 minutes).

This means that if there is an increase in transactions, the price (fee) of that transaction will rise until there is demand destruction for the transactions as supply cannot adjust. This is because the fixed block time, in concert with a block size limit, means that only 1MB of transaction data can be processed every 10 minutes. With the average transaction containing 250 bytes, this puts the max transactional processing capacity of the system at 7 transactions/second (=1,000,000/250/10/60). Since there is no mechanism for the supply to increase processing capacity, demand destruction is required to lower the transaction fee from elevated levels. In other words, in the example of Uber and Lyft, when there is a surge in demand, the price rises, incentivizes drivers to come out (thereby increasing supply), and both demand and supply are able to equilibrate. Since Bitcoin, by deliberate design, fixes supply, this means that only demand can adjust, with the largest transactions (or most important) paying the clearing price.

Is this an issue? No. It leads to an inevitable solution (conclusion):

Many saw the collapse in the bitcoin price that resulted from this strain on the system and elevated transaction fees leading to demand destruction as a sign of a fatal flaw in the system (bitcoin increases in popularity, has no supply response mechanism, falls victim to its own success and collapses). Debates emerged, centering on block size limit, with some going as far as to propose hard forks from Bitcoin to enact a block size limit increase. We think this argument and proposed solutions miss the very point of Bitcoin. We believe that Satoshi intended the restriction to generate a series of off-chains that would operate as intermediaries that lower transaction costs within each off-chain. In other words, suppose you have $10,000 of BTC. There are a flood of transactions that have increased the price of processing a Bitcoin transaction to $100. You want to buy a cup of coffee for $5. It obviously makes no sense to pay that transaction fee. Instead, you should periodically have the equivalent of a checking account held off-chain, where the operator of the off-chain is a "trusted" third-party that holds your bitcoins. When you place an order for your coffee, the off-chain operator can move the relevant amount of bitcoins (satoshis, or small sub-units of bitcoins, in this case) to the account of the merchant who sold you the coffee. The transaction would take place electronically without involving a solved blockchain, much like a traditional credit card network. Does this defeat the point of a decentralized network and disintermediating the third parties? No, it's actually the point of the block size limit. By imposing a block size limit, Bitcoin inevitably either increases the cost (and average processing time) of all transactions, or incentives the splintering into off-chains. Clearly, the former (an unsuccessful currency) is not the goal, whereas the latter is actually an elegant protection mechanism for Bitcoin, which sits up top on the chain. This is because suppose there are multiple off-chains sprouting off from Bitcoin, should one "trusted" third-party prove untrustworthy, its ultimate failure (and fraud) will be isolated to that particular node, not disrupting the parent Bitcoin. In fact, an infinite amount of nodes and subnodes can be added isolating the fraud risk to micro nodes and not disrupting the system. Let's illustrate:


This is a subnode of Bitcoin. If it fails, there are N-1 other subnodes that do not fail, protecting Bitcoin.
This is a subnode of Offchain_1. If it fails, there are N-1 other subnodes that do not fail, protecting Offchain_1.
Bitcoin
Offchain_1
Offchain_2
...
Offchain_N
Offchain_1_1
Offchain_1_2
...
Offchain_1_N
...
Offchain_N_1
Offchain_N_2
...
Offchain_N_N
Offchain_1_1_1
Offchain_N_N_2
Offchain_1_N_N
Offchain_N_N_1
Offchain_N_N_2
Offchain_N_N_N
∞

In theory, we should all have wallets that we periodically fund to off-chains, where the transactions are processed within the off-chain at low cost, and the off-chains can agglomerate funds to run a transaction on Bitcoin parent where needed. Applications are endless (e.g. payroll to an offchain as discussed below).

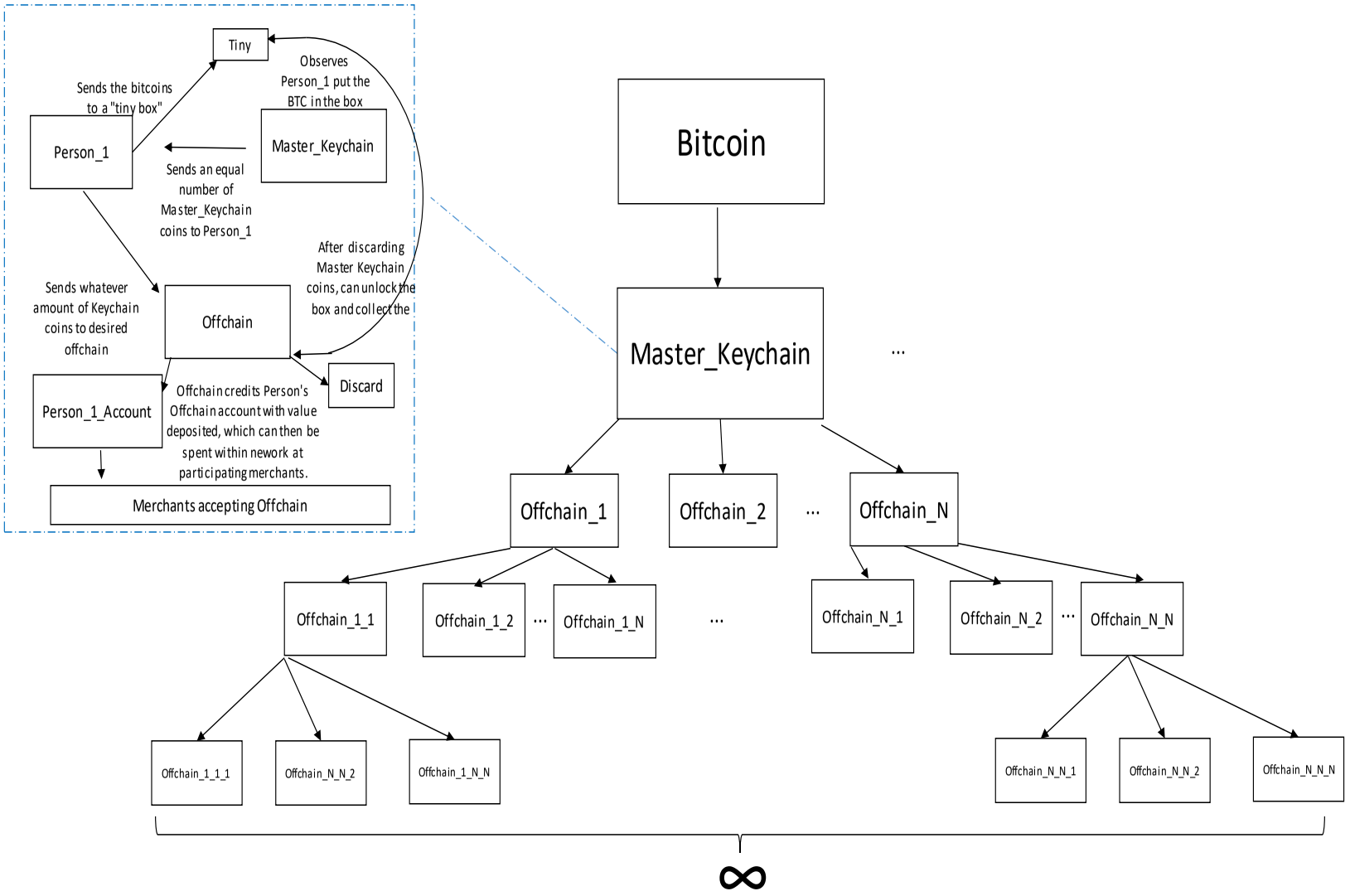
Why hasn't this occurred?
We believe this is the inevitable "vision" of Bitcoin. It cements its place as the permanent main cryptocurrency, upon which any other cryptocurrency webs out. It's a matter of time before this practical solution, which Satoshi seems to allude to in his paper and in posts, becomes reality.[1]

How can this be facilitated/jumpstarted?
Attached to the central Bitcoin node, and sitting right below it, we propose a Master Keychain, which functions as a sidechain, feeding other off-chains. Concretely, a person would send their bitcoin to a tiny box, the Master Keychain would send them Master tokens that are each equal to the bitcoins put into the tiny box. Then, the person is free to use these Master tokens with downstream offchains. When the person sends a Master token to an offchain, the offchain destroys it, and the tiny box is unlocked. In exchange, they provide the person with their own tokens. In essence, one can put all their bitcoins into this Master Offchain using sidechain methodology (so the Master Keychain is virtually as secure as Bitcoin itself), then take the resulting Master Keychain tokens and use them in other offchains, or if they want their bitcoin back, they have the option to burn the Master Keychain tokens themselves and collect back their bitcoin (or they could use a broker to sell Master coin for bitcoin, which should be at an equivalent or close to equivalent value). The utility of this design is that it creates a virtual Master Keychain/Wallet (or Safe Deposit Box) for each person that houses their bitcoins in a tiny box. And if they want to use dozens of offchains, they don't need to pay the Bitcoin transaction fee itself, which will be quite high. All the while, if any offchain or offchain of an offchain is fraudulent, the damage is isolated to that node in the complex web, not working its way across or upwards (but potentially orphaning further downstream nodes).

Now, if this takes off, how do people actually fund the Master Keychain since that initial transaction using Bitcoin will be quite expensive?
Essentially, no one would ever really use the Bitcoin transaction (except perhaps for large banks or government entities). Instead, a web-world of offchains is created. For example, your employer could pay you in ADP_Coin (ADP is a large company that processes payroll) where ADP is the "trusted entity" safeguarding that ADP offchain. You could then move these coins to other off-chains (horizontally) that accept ADP_Coins, or work your way up the offchain ladder, to your bank's offchain Node (e.g. JPM_Coin), or all the way up to the Master Offchain that sits right below Bitcoin parent. So you can fund your Master Wallet by transferring cash into the JPM_Coin offchain (at an exchange rate) or receiving auto-pay deposits to your ADP_Coin offchain. Cash eventually is displaced by bitcoin entirely, which is in fixed supply, and from which everything is a derivative. An illustration:

[1] Satoshi's white paper states: "Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification." His posts state: "[W]hatever size micropayments you need will eventually be practical. I think in 5 or 10 years, the bandwidth and storage will seem trivial…[microtransactions on the blockchain] can become more practical…if I implement client-only mode and the number of network nodes consolidated into a smaller number of professional server farms."

Sidechain illustration:



Note on practicality:
All these offchains would simply reference bitcoin equivalents, so from an end user's perspective, they do not have to get into the complex web of details of how Bitcoin and offchains and sidechains work; they will simply be using their Visa_Coin account or JPM_Account much like in the real world with a common Bitcoin Equivalent unit (BTCEU), and could be USDBitcoins for example inside a US Federation. In theory, the electricity drain currently imposed by bitcoin will work its way down to nothing when mining is exhausted (and well before then given the function generating the coins has most running out well before).

What makes this Master Keychain exclusive?
Nothing. In time, other Master Keychains, or Federations will likely emerge. They could be formed by governments (e.g. US_Keychain) that safeguard and attempt to police and monitor nodes beneath them, but at the end, it is a peer-to-peer system and it's opt-in to any specific keychain or offchain. Should a bad party emerge at any node, the damage does not work its way upstream (just downstream and possibly horizontally if there are horizontal linkages).

Positive Implications for Bitcoin:
The price of bitcoin rose dramatically as the volume of transactions started to rise substantially; however, the inability of supply to respond to the increase (by design described above) meant transaction fees spiked to the point of demand destruction, which led to less demand for bitcoin and a sudden drop. In theory, actual transactions on the Parent Bitcoin would be minimal in this described system and isolated to large institutions; in short, bitcoin price could be more stable and less vulnerable to this issue that has been its undoing in the past.

What are the implications of the success of Bitcoin on monetary policy and the world?
The web of nodes described above emanating from the Bitcoin node makes it only the nerve center of a digital world. Offchain Federations would emerge that are policed with governance just as the world currently works. In fact, everything is basically unchanged – this just recreates the global economy in a digital world. In fact, one could argue that within an offchain federation, it is actually easier to track where money flows. That will become a huge source of debate as to whether bitcoin actually just made things easier to track or created a true peer-to-peer network. However, the system would still enable moving to a different Federation or to an offchain with blockchain. In short, those aspects of Bitcoin as it currently exists remain, but the vast majority of the economy would be traditional as we know it. Effectively, Bitcoin recreates the world as we know it.

Unresolved:
- If there are too many offchains are they prone to hacking and the 51% attack?
- The idea here is to make it simple transfer your bitcoins one time to one keychain, instead of to various offchains and paying multiple transaction fees that will get more expensive; and the block time can be lower on the keychain and offchains, with lower transaction costs. But what will encourage adoption? In theory offchains would be keen to plug into the keychain since it's secure (it's a sidechain), and perhaps once there exists a master keychain that has participation from major offchains beneath it, people will convert their bitcoins to the keychain, and then start to transact more frequently?

Definition of offchain: Simply an offshoot of a chain above it. Basically, it's a child chain sitting below a parent chain, and by providing the offchain third party with coin in the parent chain units, they in turn create an account for you at their offchain. You are trusting them with this because you are giving them your bitcoin (your money). The advantage of their offchain is that they can just facilitate transactions electronically without complex blockchain mining and verification. They are basically operating as a third-party intermediary like a credit card processor. In fact, it's likely there would be one to emerge like a Visa_Offchain. Should they engage in fraudulent behavior, society would either seek recourse possibly preserving this node, or it would die off, but again, upstream is protected. There could be offchains that use blockchain to avoid trust issues.

Definition of sidechain: Operates as follows – person A sends their bitcoin to a secret box; the sidechain entity is able to confirm the bitcoin has been locked in the box. They provide the person with an equivalent number of coins on the sidechain (where the value of each coin is equal to the value of bitcoin). Then, when the person seeks to use the sidechain coins at an offchain, they send them to the offchain, the offchain kills the coins by sending them to a terminal address (this can all be verified by the sidechain and person), the box unlocks, and the offchain has the bitcoins. This is the sole area of counterparty risk. From here, the offchain could take the BTC and run, but that's where society still plays a role in making sure a JPM doesn't take the money and run. If they do, the value of that offchain collapses, and any offchains beneath it collapse (and possibly any horizontal ones that had an interchange agreement unless it's broken), but it does not work its way upstream (unless a parent offchain like Visa suffered from too much downstream fraud), protecting Bitcoin Parent.

Definition of hash: Function that converts an input of letters and numbers into an encrypted output of fixed length. "In the abstract, a hash function is a mathematical process that takes input data of any size, performs an operation on it, and returns output data of a fixed size. In a more concrete example, this can be used to take a sequence of letters of any length as input – what we call a *string* – and return a sequence of letters of a fixed length. Whether the input string is a single letter, a word, a sentence, or an entire novel, the output – called the *digest* – will always be the same length. A common use of this kind of hash function is to store passwords. When you create a user account with any web service which requires a password, the password is run through a hash function, and the hash digest of the message is stored. When you type in your password to log in, the same hash function is run on the word you've entered, and the server checks whether the result matches the stored digest. This means that if a hacker is able to access the database containing the stored hashes, they will not be able to immediately compromise all user accounts because there is no easy way to find the password which produced any given hash."

Definition of satoshis: Smallest unit of bitcoin currency recorded on the block chain. It is one hundred millionth of a single bitcoin.