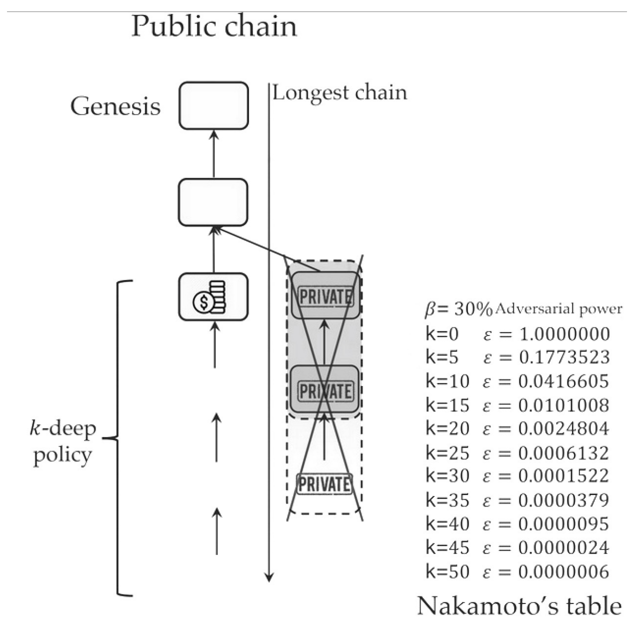
| **ECE 595: Foundations of Blockchain Systems** | **November 3, 2020** |
|---|---|
| Lecture 10 | |
| *Lecturer: Sreeram Kannan* | *Scribe: Milad Fotouhi* |

**Outline:** So far we have checked the security of longest chain protocols and as an example we checked the one that has been deployed by bitcoin. We also talked about safety and lightness of the longest chain under a general network latency modeling. The throughput and latency of bitcoin also has been discussed. In this lecture we will revisit throughput and latency to check for the area and scopes of improvement. We try to solve throughput and latency problem on longest chain.
We will also explain Prism [2], as an approach which takes the longest chain and converts it into something much better performing but still retaining the security properties.

## 10.1 Bitcoin Performance



| | |
|---|---|
| k=0 | $\varepsilon$ = 1.0000000 |
| k=5 | $\varepsilon$ = 0.1773523 |
| k=10 | $\varepsilon$ = 0.0416605 |
| k=15 | $\varepsilon$ = 0.0101008 |
| k=20 | $\varepsilon$ = 0.0024804 |
| k=25 | $\varepsilon$ = 0.0006132 |
| k=30 | $\varepsilon$ = 0.0001522 |
| k=35 | $\varepsilon$ = 0.0000379 |
| k=40 | $\varepsilon$ = 0.0000095 |
| k=45 | $\varepsilon$ = 0.0000024 |
| k=50 | $\varepsilon$ = 0.0000006 |

Figure 10.1: Illustration of k-deep policy.

Previously we have discussed that one of the biggest advantages of the longest chain protocol, particularly Bitcoin, is that it has been secure under an immense threat model that is under an

entire permission-less system and theoretically it is known that it is secure against $50$ percent adversary (this already has been proved in last section). But practically, this has really withstood the test of time. So there will be no attacks on Bitcoin however, there are other attributes of bitcoin, which are not as appealing, for example confirmation latency can be in the order of hours. Also, throughput (how many transactions per second can we process) is in the order of a few transactions per second. In contrast we can consider Visa or MasterCard, which can support a throughput of $10,000$ transactions per second with the latency of a few hundred milliseconds.
To understand this better lets recall that when we get a transaction that is accepted into a block, we do not immediately confirm that transaction because it's too risky. Our transaction needs to be deeply embedded into the longest chain for the transaction to be confirmed which is called the $k$-deep confirmation policy. As we discussed in section $8$ the longer the $k$ is, the better adversary protection. When we increase $K$, as long as the adversary has less than $50$ percent adversity power, the probability that the adversary can construct more than $K$ blocks faster than the honest notes can construct a block can be calculated. This is a race between two distinct random variables. Satoshi Nakamoto modeled this in the original Bitcoin paper and this probabilities has been actually calculated there.
As you can see in the figure 10.1, the table is showing that if we want very high availability, then we need to wait for $K$ to become equals to $30$ blocks. Considering the entire block time in Bitcoin being $10$ minutes then the overall latency here will be $300$ minutes. This is the main cost of latency in bitcoin. This latency is mainly due to two things. One is $k$ which is the confirmation of depth that the other is intro block arrival which is $10$ minutes. Reducing $K$ will reduce reliability, and if we reduce the arrival time from $10$ minutes to several seconds there will be more tries there will be more forking. Hence, we cannot increase performance without reducing the reliability or reducing the safety threshold.
As fig.10.2 illustrate here to make our entire block proposal time to be smaller than $\Delta$ we should have multiple nodes that proposed block simultaneously. Then we will have forking and it leads to slow growth of the longest chain because even though nine blocks having produced in this figure, the length has only grown by two.And this is a reduction in the security because now an adversary who does not even have $50$ percent adversarial power can make four blocks during that time, but they're all coordinated, which means they're in the longest chain. So as you can see there is a reduction in the security threshold as you increase the mining rate.

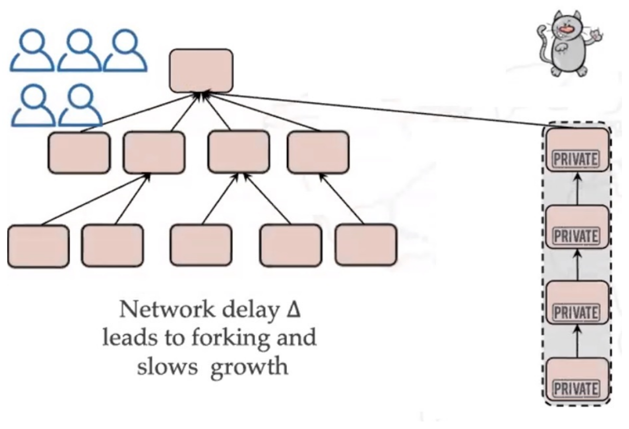
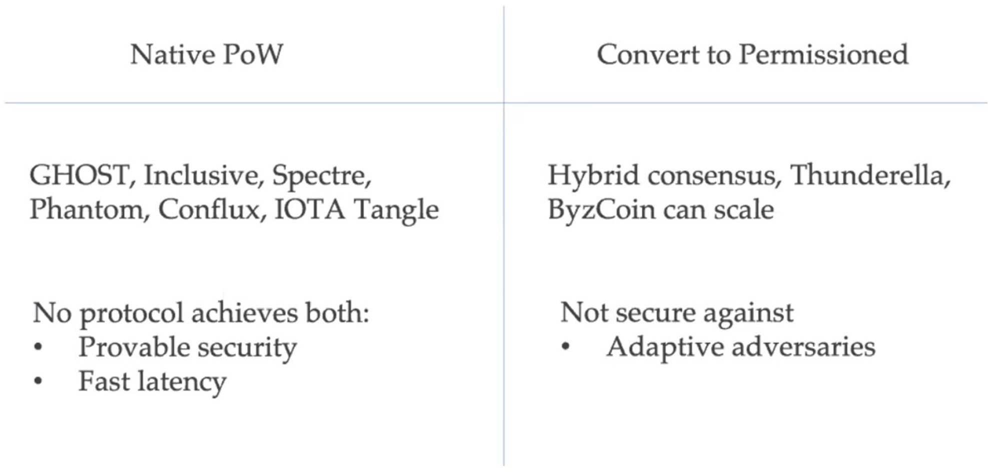


Figure 10.2: Bitcoin performance and security trade-off.

## 10.2 Existing Scalability Approaches



| Native PoW | Convert to Permissioned |
|---|---|
| GHOST, Inclusive, Spectre, Phantom, Conflux, IOTA Tangle | Hybrid consensus, Thunderella, ByzCoin can scale |
| No protocol achieves both:<br>• Provable security<br>• Fast latency | Not secure against<br>• Adaptive adversaries |

Figure 10.3: Existing scalability approaches

There are a set of existing approaches which have been trying to improve the scalability problem, GHOST [1],Inclusive [3], Spectre [5], Phantom [6], Conflux [4], IOTA Tangle are some examples of them. However, None of these protocols achieves both provable security and fast latency. There are also some approaches that convert the problem from a permission-less protocol to permissioned problem. Hybrid consensus, Thunderella, BysCoin can scale are some examples of these approaches. The rough idea in these approaches is that you let everybody participate in approval work so they all can mine blocks. Here the miners of the previous blocks will forma committee, this committee is fixed in size and prone to any civil attack. Now we can run some protocol inside this committee and convert the permission-less into a permissioned problem. The permission will be given based on the who mind more blocks during the previous stage. So the miners who have been mining previously now get to propose and form a committee and you just run a permissioned protocol inside that committee.

### 10.2.1 Adaptive Adversary

Adaptive adversary is an adversity that knows the entire state of the work, till this point; it can go on bribe whichever nodes It wants. In a purely mathematical model, we can think of it as the node can just go and somehow corrupt and control whichever node it wants.As long as the corrupted group of nodes controls less than 50 percent of computing power, the protocol secure. This is because in the approval work system after you made a block you have no power in the future. Once you sign a block, you made a block, the block is roughly sealed by the proof of work. If you want to change any content inside the block, then it won't match up to any proof of work.So once you make a block. You have no future power. But so and adversary even an adaptive adversary cannot go and figure out who are all the miners in the last hundred blocks and bribe them and then do anything because that minor is itself powerless to change the block or do anything. The only hope of the adversity is it has to bribe or corrupt enough nodes so that it actually controls 50 percent of the compute power right now.

### 10.2.2 Permissioned Protocol Vulnerability Against Adaptive Adversary

So as we said these approaches indeed convert the much harder problem, permission-less consensus, into a simpler permissioned consensus problem, but it will make it vulnerable to the adaptive adversary. Just consider adversity who can bribe the last hundred miners who mine the blocks and have the future power in this permissioned network. And so adapter adversity can exploit this behavior because it can just go and grab these 50 nodes out of this or this hundred nodes. Just Remember, these hundred nodes were themselves selected out of maybe hundreds of thousands or millions of nodes. They were selected basically because they represented a random sub-selection. If originally 20 percent of the mining power is adversarial when you do this kind of random choice roughly 20 billion of the nodes will be adversarial but what adversarial is doing is acting after the selection has happened to do what is called an adaptive adversary. These protocols are not secure against an afterword adversary, which was a unique strength across the proof of work protocols.

## 10.3 Prism

So far we discussed  a bunch of protocols that designed specifically to solve the scaling problem,but they've disrupted the core structure of bitcoin, the longest chain protocol. What you're looking for is a native proof-of-work protocol that actually solves the latency network problem as remain secure under adaptive adversary just like bitcoin. Prism [2], is a new proof-of-work blockchain protocol, which can achieve security against up to 50 percent adversarial hashing power while can achieve optimal throughput. In order to understand Prism, let's just understand Bitcoin carefully into its Subcomponents, lets deconstruct it into its sub-components, and then maybe we can put tog etherthese components correctly to get something which is much more performant. That's what we're trying to with this protocol called Prism.

### 10.3.1 Deconstructing the Blockchain to Approach Physical Limits

We should get a core observation of bitcoin and to to that we should know what is the role of different blocks. The latency of bitcoin is coming form waiting for getting enough votes when we get enough voters we can confirm a block. An obvious way to solve this latency problem is to increase the rate of voting, if we make the voting faster then we could potentially confirm a block fast. But there is a problem, if we want to increase the rate of voting we have to increase the rate of proposing (rate of voting = rate of proposing); just imagine an election that every voter is also a candidate. This was the key observation to separate roles of block, we can have different blocks having different operations. Lets consider that we will separate the proposer block form voter block. So with this schema we can accumulate votes faster. Voter chain doesn't contain any transaction, they just contain to a particular block. Consider figure 10.4, on the left side you can see two blocks and both of them has accrued at level $2$, they are $2$ separated proposal for second ledger. In the voter chain they are voting for these two blocks. Consider total number of votes being $1000$ based on the votes we can say which block will win. Figure 10.5 is deconstructing the basic blockchain structure into its atomic functionalities. The selection of the main chain in a blockchain protocol (e.g., the longest chain in Bitcoin) can be viewed as electing a leader block among all the blocks at each level of the blocktree, where the level of a block is defined as its

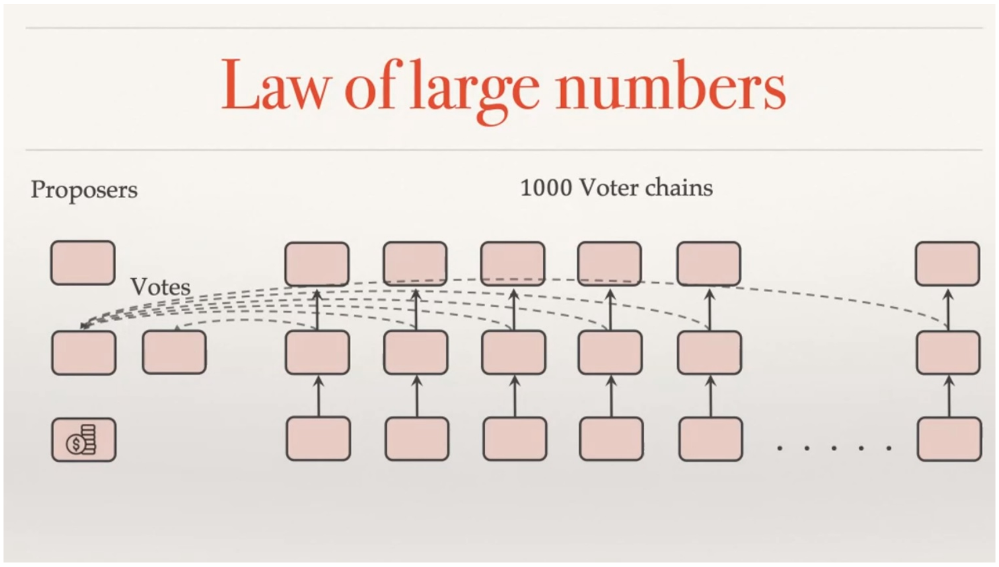


Figure 10.4: Deconstructing blockchain.

distance (in number of blocks) from the genesis block. Blocks in a blockchain then serve three purposes:they stand for election to be leaders, they add transactions to the main chain, and they vote for ancestor blocks through parent link relationships. Here we explicitly separate these three functionalities by representing the blocktree in a conceptually equivalent form Figure10.5 . In this representation, blocks are divided into three types: proposer blocks, transaction blocks and voter blocks. The voter blocks vote for transactions indirectly by voting for proposer blocks, which in turn link to transaction blocks. Proposer blocksare grouped according to their level in the original blocktree, and each voter block votes among the proposer blocks at the same level to select a leader block among them. The elected leader blocks can then bring in the transactions to form the final ledger. The valid voter blocks are the ones in the longest chain of the voter tree, and this longest chain maintains the security of the whole system.

#### 10.3.1.1 Scaling

This alternative representation of the traditional blockchain,although seemingly more complex than the original blockchain representation, provides a natural path for scaling performance to approach physical limits. To increase the transaction throughput, one can simply increase the number of transaction blocks that a proposer block points to without compromising the security of the blockchain. This number is limited only by the physical capacity of the underlying communication network. To provide fast confirmation, one can increase the number of parallel

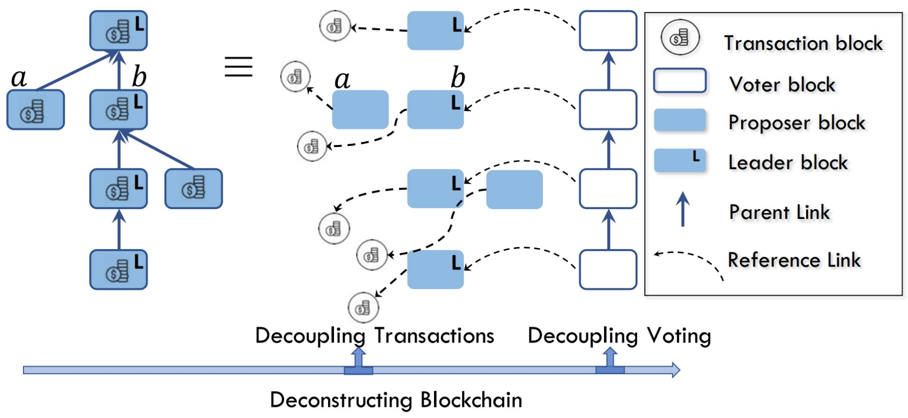


Figure 10.5: Deconstructing blockchain.

voting trees, voting on the proposal blocks in parallel to increase the voting rate, until reaching the physical limit of confirming with speed-of light latency and extremely high reliability. Note that even though the overall block generation rate has increased tremendously, the number of proposal blocks per level remains small and manageable, and the voting blocks are organized into many separate voting chains with low block mining rate per chain and hence little forking.

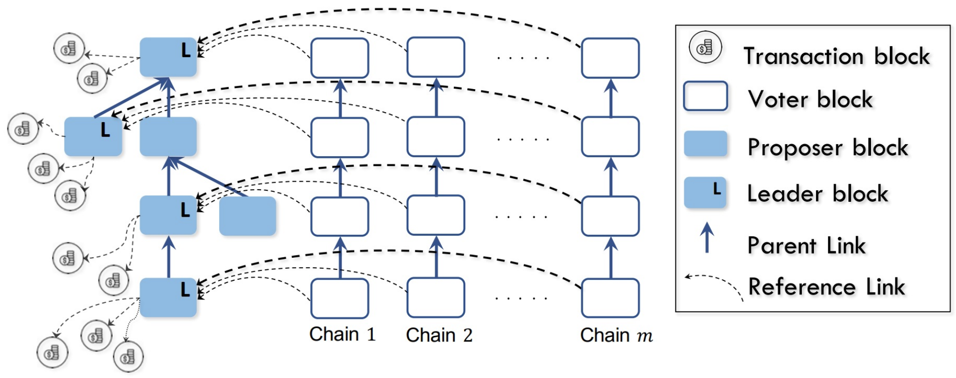


Figure 10.6: Prism

#### 10.3.1.2 Sortition

The sortition of blocks into the three types of blocks, and further into blocks of different voting trees, can be accomplished by using the random hash value when a block is successfully mined.This sortition splits the adversary power equally across the structures and does not allow it to focus its power to attack specific structures.

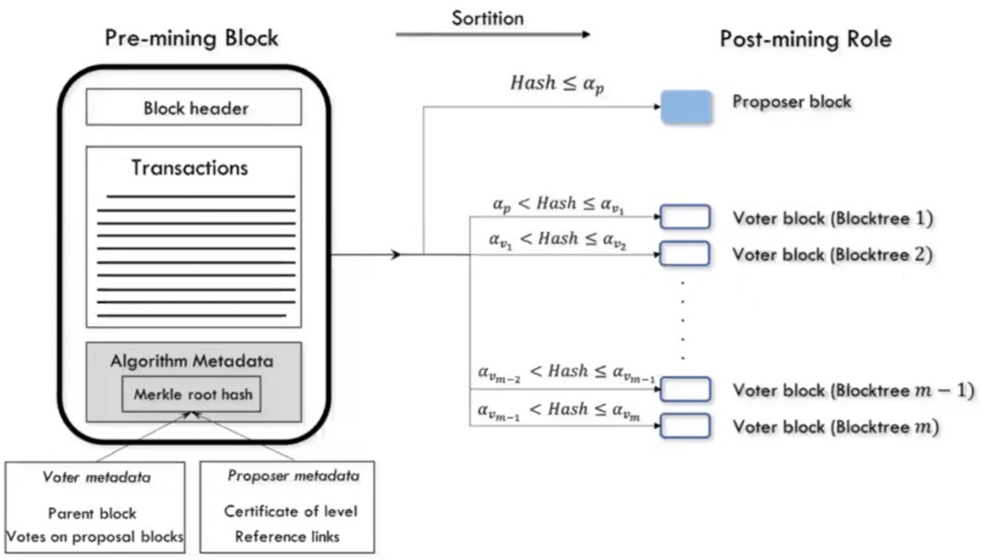

Pre-mining Block
Sortition
Post-mining Role
Block header
Transactions
Algorithm Metadata
Merkle root hash
Voter metadata
Parent block
Votes on proposal blocks
Proposer metadata
Certificate of level
Reference links
$Hash \leq \alpha_p$
Proposer block
$\alpha_p < Hash \leq \alpha_{v_1}$
Voter block (Blocktree 1)
$\alpha_{v_1} < Hash \leq \alpha_{v_2}$
Voter block (Blocktree 2)
$\alpha_{v_{m-2}} < Hash \leq \alpha_{v_{m-1}}$
Voter block (Blocktree $m-1$)
$\alpha_{v_{m-1}} < Hash \leq \alpha_{v_m}$
Voter block (Blocktree $m$)

Figure 10.7: Prism sortition

#### 10.3.1.3 How does mining happen?

When you mine a block, you do not know whether you're going to land up in a proposal chain or in a voter chain or in which voter chain.Not knowing this a priority is a very important requirement and property of this protocol. When you create a pre-mining block you put in two kinds of data, one is what is voting data (voting data if I were in voter chain) the other is who was all the blocks that I vote for (ex. If I were in voter chain 2 what are all the proposals that I would vote for).And then you have something called the proposer Metadata which says if they've got a proposal block, what would be all the transactions.Figure 10.7 Then you put in a commitment here. Let's say Merkel route hash which as a hash rate is taking the hash of those two kinds of data. But now, what you do is you take the range of the output of the hash function and then segregated into groups if it falls in the first range, then you get the proposal to block and if it falls into the second range then you get a voter block one with falls into the third range, then it's motor block to and so on.What you've done is you've taken the output range of the hash function and then segregated into groups, depending on what group you fall in you have become a voter or a proposal block for that. Now when you float this block, everybody will only look at that particular content if your hash is between $\alpha_{v1}$ and $\alpha_{v2}$ (figure 10.7 ) We know then you basically are a voter block number two which means everybody will only look at your voter metadata.

### 10.3.2 Confirmation Policy

Consider figure 10.4 that two blocks on the left have contradictory transactions. the confirmation policy is not as simple as count the number of votes right now and take a decision, we have to do something more. In this case if there are $1000$ votes and one get $100$ and the other one gets $900$ we can relatively be sure that the block with most votes will remain in the lead for future. In bitcoin lets say you get $80$ percent reliability, if one block gets a little bit more than $500$ votes, you will never confirm that block because it is too often that you get adversary. Now consider that all chains are ready to vote, and each block is stable except for $20$ percent probability, then if the a block is legit then out of $1000$ vote we expect it gets $800$ or more. So here what is happening is that instead of waiting for law of average number happening over time we have law of average number happening across the space, and because of this we will have much faster confirmation for this block. With one interval block arrival at a time you have actually confirmed a proposal block at very high reliability, so now we don't have to wait for a lot's of time to actually aggregate the voters. So we are essentially using weak protections but many chains in parallel and aggregating them and using the independence to say that we have gotten our self a strong net protections. In the longest-chain protocol, for fixed block size and network,the maximum tolerable adversarial hash power $\beta$ is governed by the block production rate; the faster one produces blocks, the smaller the tolerable $\beta$. In Prism, we need to be able to tolerate $\beta$ adversarial hash power in each of the voter trees and the proposer tree. Hence, following the observations of each of these trees individually must operate at the same rate as a single longest-chain blocktree in Bitcoin in order to be secure.The security of Prism is provided by the voter trees; a proposer block is confirmed by votes which are on the longest chains of these voter trees. Consider a conservative confirmation policy for Prism, where we wait for each vote on each voter tree to reach a confirmation reliability $1 - \epsilon$ before counting it. This would requires to wait for each vote to reach a depth of $k(\epsilon)$ in its respective tree,where $k(\epsilon)$ denotes the confirmation depth for reliability $1 - \epsilon$. This conservative confirmation rule immediately implies that Prism has the same security guarantee as that of each of the voter tree, i.e. that of Bitcoin.

#### 10.3.2.1 Least Confirmation

There are various property for Prism, mainly low latency confirmation but there are scenarios that we can not obtain low latency confirmation. If we have two blocks that both split roughly equally then we can not be sure that which one should remain in the ledger. So to be sure that we chose the right one we might need to vote until the last votes. We can't say which one will remain in the ledger but we know at least one of them will remain winner. As the blocks get dipper and dipper we will eventually be able to choose the winner.

#### 10.3.2.2 Decoupled validity

A key aspect of Prism is that it has decoupled validating. When you propose a block you do not know which block is the possible ancestor. This is very different in bitcoin; when you propose a block in bitcoin it is already inside the chain and you know under which history this block is going to be passed. So we can not guaranty that all transactions will remain valid after the block got in. So in Prism we don't require that all transactions needs to be valid for the block to be valid. There is question about the schema of the blocks here, when we build a block if we want to float the block which is only going to be proposal block do we need to contain all the voter metadata? We can say that there is a subtlety here. The data structure that we use is Merkel tree and what we use for that Metadata is Merkel root and that allows you to reveal selected subset of data which comes from and belongs to particular root-hash, we can assert that without showing other data.

## References

[1] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. Solida: A blockchain protocol based on reconfigurable byzantine consensus. *arXiv preprint arXiv:1612.02916*, 2016.

[2] Vivek Bagaria, Sreeram Kannan, David Tse, Giulia Fanti, and Pramod Viswanath. Prism: Deconstructing the blockchain to approach physical limits. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 585–602, 2019.

[3] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security*, pages 528–547. Springer, 2015.

[4] Chenxing Li, Peilun Li, Dong Zhou, Wei Xu, Fan Long, and Andrew Yao. Scaling nakamoto consensus to thousands of transactions per second. *arXiv preprint arXiv:1805.03870*, 2018.

[5] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. Spectre: A fast and scalable cryptocurrency protocol. *IACR Cryptol. ePrint Arch.*, 2016:1159, 2016.

[6] Yonatan Sompolinsky and Aviv Zohar. Phantom: A scalable blockdag protocol. *IACR Cryptol. ePrint Arch.*, 2018:104, 2018.