Roughly ten years ago Satoshi Nakamoto, the founder of Bitcoin made a dent in the financial universe. Nakamoto had the following goal: remove the “trusted third party” so that transactions run smoothly i.e. decrease transactions costs and increase transaction size (both small and large). This objective allowed for the reversal of such transactions without the possibility of fraud [2]. Not only did such an ambition revolutionize financial transactions, it also reaffirmed the necessity for efficiency, power, and security in the hardware and software that block-chains use today.

In “Blockene: A High-throughput Blockchain Over Mobile Devices”, Satija et al. argue that the SOTA (state of the art) of Blockchain is inefficient. This is a valuable contribution since current blockchains have heavy resource usage in servers, networks, and storage. All three current Blockchain technologies— ‘proof of work’, ‘ proof of stake’, and ‘consortium’ blockchains— require significant storage and high network throughput. Bitcoin is the ubiquitous ‘proof of work’ blockchain that, according to Satija et al. has extremely inefficient computation costs [2].

Satija et al. exhibit the following SOTA principles of blockchain: a blockchain is simply a collection of such hashed values. There is a database that uses a Merkle tree data structure to store keys and values. Such values are unique because the path from the root to its leaves make the “global state” of the blockchain secure. This is the entire occasion of the paper: to increase the throughput of such transactions while keeping this chain secure for current and future users.

The greatest contribution is that blockene is decentralized *and* secure. Similar to syntactic sugar, the authors provide their audience with a metaphor of a democratic government to describe their hierarchal model. Although sometimes superfluous Satija et al. describe a democratic model of security distributed through its ‘citizens’ and ‘politicians’. All transactions (‘decisions’) are made by such citizens (cell phones). The politicians are the untrusted servers without any ‘voting rights’. They can only execute what the citizens want. The same way in which power is affirmed by the majority in a democracy, data must ‘signed’ by a ‘majority’ of citizens. This hedges the real, verifiable transactions against fraudulent transactions through the ‘majority’ (two thirds) of its ‘honest citizens'. For Saija et al., scale leads to better security [2].

Much of the paper revolves around security where in theory, the more nodes (participants) that use the technology, the more shared control there is over the technology which results in less collusion. To increase security, the authors discuss incentive so that more users adopt Blockene and therefore increase its security as a blockchain. Bitcoin on the other hand, must incentivize its users by paying them in its own currency [1].

But, rather than bribe its users, Blockene takes a different angle towards incentive: high transaction throughput (meaning better security from its model) and lighter load on ‘citizens’ or common users on their phones and larger servers. If it requires little work from a user, the more likely it is that they will use it. This will have a cascading effect where the blockchain will be more secure and produce more trust in its technology. The question then arises: if more users use the technology, how can it *stay* secure and most importantly, how can it use green technology to keep its model as efficient as possible? Can we couple Blockene efficiency with green scheduling model of Aksanli et al.'s model? For Blockene's VM's can we schedule its light workloads with wind and solar? [6]. This is one question that Blockene doesn't answer which could be a vital property to blockchain technology in the future.

Although green energy isn't mentioned in its proof of concept, Blockene core questions do have efficiency in mind: "what is the throughput and the latency on devices? How secure is it? Are the optimizations useful? And what is the load on the battery?"[2]. They answer these questions through the following simulation: Citizen nodes are written in over 10k lines of code for Android application and 11k lines of code for servers. Since the authors' goal is to reduce network and storage resources, Blockene proved that via over 2000 'Politician' nodes (8 core VM with 32GB of RAM servers) and 2000 'Citizen' nodes (1 core VMs) with 2GB of RAM over a network throughout the United States limited to 1MB/s latency, only 3% of battery usage for mobile phones was used per day . This was all achieved an efficient '1045 transactions/sec' [1].

Such efficient throughput is an important feat considering new blockchain technology. Blockchains like Algorand require users to maintain the network at *every* signed transaction leading to wasted battery usage [2]. Blockene shows that security is achieved at low costs by enabling those only with a cellphone to ‘commit blocks a few times a day, i.e. not striving for up-to-date’ throughput [2]. The blockchain is therefore secure and more popular to use since users trust their currency (every user validates and stores an ‘up to date list of public keys of other Citizens’), and need only 3% of battery usage from their smart phones per day [1]. Wide scale consensus ensures secure validation of transactions, but this requires a lot of energy. Blockene avoids this through their efficient security model with the following results in Figure 3: higher latency for malicious actors and lower latency for honest transactions [2].

This paper necessitates efficient operating systems in smart phones and virtual machines. Innovators such as Satija et al. can only innovate so much. This is why innovators like Lin et al. contribute to the promise of high energy efficiency to multi-domain SOCs. K2 for example, is an excellent compliment to the light workloads of Blockene. Because Blockene requires updates to its chain a few times a day, its light workload on mobile devices could be improved even more. Its 3% battery usage for mobile phones could very well be reduced if innovation like K2 were be applied to reduce OS workloads handling Blockene by 10x [4]. Also, the authors could have reported their results by suggesting further efficiency in virtual machines, possibly citing interactions of a Xen hypervisor with Blockene. Can we apply the Xen architecture to virtual machines that cater only to Blockchain technologies? By paravirtualizing VM design could we increase the performance of the ‘politician’ nodes that take on the heavier load of maintaining Blockene? Could we run over 100 different blockchain technologies, including Blockene, on 100 different OSs? It's clear that Xen can handle such a workload [5].

The cascading effect of efficient technology has changed the world. From open source protocols in Hypervisors in VMs to new and efficient blockchain architectures, we are on a path towards a world of immediacy and freedom. Blockene is more than just this efficiency, low latency, and security. It is a symbol for borderless financial institutions and most importantly a spirit of innovation that connects us all.

References

[1] *Utilizing Green Energy Prediction to Schedule Mixed Batch and Service Jobs in Data Centers*. Baris Aksanli, Jagannathan Venkatesh, Liuyi Zhang, Tajana Rosing.

[2] *Blockene: A High-throughput Blockchain Over Mobile Devices*. Sambhav Satija and Apurv Mehra, Microsoft Research India; Sudheesh Singanamalla, University of Washington; Karan Grover, Muthian Sivathanu, Nishanth. Chandran, Divya Gupta, and Satya Lokam, Microsoft Research India

[3] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*

[4] Felix Xiaozhu Lin, Zhen Wang, and Lin Zhong. *K2: A Mobile Operating System for Heterogenous Coherenece Domains.*

[5] Paul Barham∗, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer†, Ian Pratt, Andrew Warfield. *Xen and the Art of Virtualization*

[6] Baris Aksanli, Jagannathan Venkatesh, Liuyi Zhang, Tajana Rosing, *Utilizing Green Energy Prediction to Schedule Mixed Batch and Service Jobs in Data Centers.*

Your analysis of the paper, including:

- Do you find the work to be valuable? Why or why not?
- Can you relate any part of this work to other papers that we have read for this class?
- Do you see issues with the paper, or confusions or questions that were not answered?
- What do you think researchers (including but not limited to the paperâ€™s authors) should do next to further this line of inquiry?