linear", as implied by Theorem 3. Based on this result, we further leverage the techniques from random walk to prove that, for every block, after a delay of $O(s \log s)$ units of time, all blocks will be its descendant (Theorem 4), consequently, if we set $\ell = \Theta(s \log s)$ in our design, every block will be verified by all users, and security follows.

As we mentioned before, each new block will refer to two leaves in $L_t$. As every block offers the same total amount of verification reward, every leaf appears the same to the miners (unless they are in conflict with previous blocks and then miners will be biased based on the LWD rule). Therefore, a new block will randomly select two leaves to refer to. Assuming leaves are not conflicting with previous blocks, we show that $|L_t|$ will be $O(s)$ in the long run with an extremely high probability. First, it is easy to see that if $|L_t| \leq s$, then $L_{t+1} \geq s$ as the $s$ new blocks will be leaves at $t+1$. The following lemma shows that if $|L_t|$ is sufficiently large, then with very high probability it will reduce to $O(s)$ after enough time.

Lemma 5. *Let $\epsilon$ be an arbitary small constant. If $|L_t| \geq 1/\epsilon^3$ and $|L_t| \geq 4s$, then with sufficiently high probability (at least $1 - O(\epsilon)$), $|L_{t+1}| = |L_t| - X + s \leq |L_t| - \frac{(1-3\epsilon)s}{2}$, i.e., $L_t$ decreases by at least $\Omega(s)$.*

See Chen et al. [6] for the full proof of Lemma 5.

The above lemma shows that if $|L_t|$ is large, then with high probability $|L_t|$ shall decrease, however, what we are interested in is the probability that $|L_t| \leq O(s)$ for all $t \geq 0$. Towards this, we need to cast the problem as a *random walk*. Lemma 5 shows that with the probability of $(1 - O(\epsilon))^3 = 1 - O(\epsilon)$, $|L_t|$ can decrease by $\frac{3(1-3\epsilon)s}{2} \geq s$, while with probability of at most $O(\epsilon)$, $|L_t|$ can increase by at most $s$. This can be interpreted as a random walk which walks right (increase) by $s$ steps with the probability of $1 - O(\epsilon)$, and walks left (decrease) by $s$ steps with the probability of $O(\epsilon)$. The following lemma is proved for a general random walk.

Lemma 6 ([8], pp.272). *Consider a random walk starting at $RW_0 = 0$, $\Pr(RW_{i+1} - RW_i = s) = p$, $\Pr(RW_{i+1} - RW_i = -s) = q$ where $p + q = 1$ and $s \in \mathbb{Z}_{>0}$. If $p > q$, then*

$$\lim_{n\to\infty} \Pr(RW_i \geq 0, \forall 1 \leq i \leq n) = \frac{p-q}{p}.$$

*If $p < q$, the above limit is 0.*

Now we are ready to prove the following theorem.

Theorem 3. *Let $\epsilon$ be a small constant such that $s > 1/\epsilon^3$. With very high probability (at least $1 - O(\epsilon)$), $|L_t| \leq 5s$ for all $t \geq 0$.*

Proof. Recall that $|L_0| = 0$. Let $t^*$ be the smallest time where $|L_{t^*}| \geq 4s$, then $|L_{t^*}| \leq 5s$. Now we take $t^*$ as a starting time, $|L_{t^*}|$ as a starting point and take the random walk interpretation. Using Lemma 6, we have that

$$\begin{aligned}\lim_{n\to\infty} \Pr(|L_t| \leq |L_{t^*}|, \forall 1 \leq t \leq n) &\leq \frac{1 - O(\epsilon) - O(\epsilon)}{1 - O(\epsilon)} \\ &= 1 - O(\epsilon).\end{aligned}$$

Therefore, the probability that $|L_t|$ is bounded by $5s$ for all $t \geq 0$ is at least $1 - O(\epsilon)$. □

Lemma 7. *Let $\epsilon$ be a small constant such that $s > 1/\epsilon^3$. For any transaction at $t$ that is not in conflict with prior transactions, with sufficiently high probability (at least $1 - O(\epsilon)$) every block appended at or after $t + O(s \log s)$ will be its descendant.*

Proof. According to Theorem 3, we focus on the event that $|L_t| \leq 5s$ for all $t \geq 0$, which happens with $1 - O(\epsilon)$ probability.

For $h \geq t$, let $\Psi_h$ be the subset of blocks in $L_h$ which has a directed path from some fixed block $\tau_0 \in L_t$, which is a random subset. Let $\psi_h = \mathbb{E}(|\Psi_h|)$. Consider $L_{h+1}$. For any block $\tau_i \in L_{h+1}$, let $X_i$ be a binary random variable indicating whether $\tau_i$ refers to some block in $\Psi_h$, and hence admits a directed path from $\tau_0$. Then we know

$$\begin{aligned}\Pr(X_i = 1) &= \frac{\binom{|\Psi_h|}{2} + |\Psi_h|(|L_h| - |\Psi_h|)}{\binom{|L_h|}{2}} \\ &= \frac{|\Psi_h|(2|L_h| - |\Psi_h| - 1)}{|L_h|(|L_h| - 1)}.\end{aligned}$$

We consider $|\Psi_{h+1}|$. It is obvious that if $|\Psi_h| = |L_h|$, then every block in $L_{h+1}$ refers to some block in $\Psi_h$ and thus admits a directed path from $\tau_0$, hence, $|L_{h+1}| = |\Psi_{h+1}|$, and similarly we have $|L_{h+j}| = |\Psi_{h+j}|$ for all $j \geq 1$. Otherwise, we assume $1 \leq |\Psi_h| \leq |L_h| - 1$. Then $2|L_h| - |\Psi_h| - 1 \geq |L_h|$, and we have

$$\mathbb{E}(X_i) = \mathbb{E}\left(\frac{|\Psi_h|(2|L_h| - |\Psi_h| - 1)}{|L_h|(|L_h| - 1)}\right) \geq \frac{\psi_h}{|L_h| - 1}.$$

Note that $|\Psi_{h+1}| = \sum_i X_i$. It is easy to calculate that

$$\psi_{h+1} = \mathbb{E}(|\Psi_{h+1}|) \geq \psi_h \left(1 + \frac{1}{|L_h| - 1}\right).$$

This means, starting from $\psi_t = 1$, for each $\psi_h$ where $h \geq t$, either $\psi_h = |L_h|$ and thus $\psi_{h'} = |L_{h'}|$ for all $h' \geq h$, or $\psi_{h+1} \geq \left(1 + \frac{1}{|L_h|-1}\right)\psi_h$. Since $|L_h| \leq 5s$, $\psi_h$ increases sufficiently close to $|L_h| \leq 5s$ when $h \geq t + O(s \log s)$, and the theorem is proved. □

Given the above lemma, if we set $\ell$, the verification depth to be $\ell \geq O(s \log s)$, then any transaction at $t$ will be verified by all the users after $O(s \log s)$ units of time with high probability. The following theorem is thus true.

Theorem 4. *If $s > 1/\epsilon^3$ and $\ell \geq O(s \log s)$, then with probability of at least $1 - O(\epsilon)$, any transaction at $t$ will be verified by all the users after $O(s \log s)$ units of time.*

**Remark.** Recall that the scalability of the system increases as $\Delta$ increases, while $s = \min\{c_1 m/\Delta, c_2 n\}$, and hence the finality-duration $O(s \log s)$ decreases as $\Delta$ increases. Theorem 4 shows trade-off between the scalability and finality-duration.

## 6 CONCLUSION

We provide the first systematic analysis on blockchain systems with respect to three major parameters, verification, scalability, and finality-duration. We establish an impossibility result showing no blockchain system can simultaneously achieve the three properties. We complement the existing blockchain systems by establishing the first NLB that achieves both full verification and scalability. We also reveal, for the first time, the trade-off between scalability and finality-duration in NLB. It is not clear whether a better trade-off exists or not.

# REFERENCES

[1] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. 2019. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys Tutorials* 21, 2 (2019), 1676–1717.

[2] Sarah Azouvi, Patrick McCorry, and Sarah Meiklejohn. 2018. Betting on Blockchain Consensus with Fantomette. *CoRR* abs/1805.06786 (2018). arXiv:1805.06786 http://arxiv.org/abs/1805.06786

[3] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. 2019. SoK: Consensus in the Age of Blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019*. ACM, Zurich, 183–198.

[4] Xavier Boyen, Christopher Carr, and Thomas Haines. 2017. Blockchain-Free Cryptocurrencies. (2017).

[5] David Chaum. 1982. Blind Signatures for Untraceable Payments. In *Advances in Cryptology: Proceedings of CRYPTO '82*. California, 199–203.

[6] Lin Chen, Lei Xu, Zhimin Gao, Ahmed Imtiaz Sunny, Keshav Kasichainula, and Weidong Shi. 2020. Nonlinear Blockchain Scalability: a Game-Theoretic Perspective. *CoRR* abs/2001.08231 (2020). arXiv:2001.08231 https://arxiv.org/abs/2001.08231

[7] Mauro Conti, Sandeep Kumar E, Chhagan Lal, and Sushmita Ruj. 2018. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys Tutorials* 20, 4 (2018), 3416–3452.

[8] William Feller. 1968. *An introduction to probability theory and its applications: volume I* (3rd ed.). Vol. 3. John Wiley & Sons, New York.

[9] BF França. 2015. Homomorphic mini-blockchain scheme.

[10] Juan A. Garay and Aggelos Kiayias. 2020. SoK: A Consensus Taxonomy in the Blockchain Era. In *Topics in Cryptology - CT-RSA 2020 - The Cryptographers' Track at the RSA Conference 2020, Proceedings (Lecture Notes in Computer Science, Vol. 12006)*. Springer, San Francisco, 284–318.

[11] Merve Can Kus Khalilov and Albert Levi. 2018. A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. *IEEE Communications Surveys Tutorials* 20, 3 (2018), 2543–2585.

[12] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A Survey on Applications of Game Theory in Blockchain. *CoRR* abs/1902.10865 (2019). http://arxiv.org/abs/1902.10865

[13] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. 2013. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy, SP 2013*. IEEE Computer Society, California, 397–411.

[14] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system.

[15] John Nash. 1951. Non-cooperative games. *Annals of mathematics* (1951), 286–295.

[16] Serguei Popov. 2016. The Tangle. *cit. on* (2016), 131.

[17] Serguei Popov, Olivia Saa, and Paulo Finardi. 2019. Equilibria in the Tangle. *Computers & Industrial Engineering* 136 (2019), 160–172.

[18] Team Rocket. 2018. Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies. (2018).

[19] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. 2019. Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys Tutorials* 21, 1 (2019), 858–880.

[20] Tomas Sander and Amnon Ta-Shma. 1999. Auditable, Anonymous Electronic Cash Extended Abstract. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Proceedings (Lecture Notes in Computer Science, Vol. 1666)*. Springer, California, 555–572.

[21] Eli Ben- Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Symposium on Security and Privacy, SP 2014*. IEEE, California, 459–474.

[22] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. 2016. SPECTRE: A Fast and Scalable Cryptocurrency Protocol. *IACR Cryptology ePrint Archive* 2016 (2016), 1159. http://eprint.iacr.org/2016/1159

[23] Yonatan Sompolinsky and Aviv Zohar. 2015. Secure High-Rate Transaction Processing in Bitcoin. In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, , Revised Selected Papers (Lecture Notes in Computer Science, Vol. 8975)*. Springer, Puerto Rico, 507–527.

[24] Yonatan Sompolinsky and Aviv Zohar. 2020. Phantom, Ghostdag.

[25] The Ethereum Team. 2019. On sharding blockchains.

[26] The Harmony Team. 2018. Harmony - technical whitepaper.

[27] The Zilliqa Team. 2017. The zilliqa technical whitepaper.

[28] Nikolaos Petros Triantafyllidis and TNO Oskar van Deventer. 2016. Developing an Ethereum blockchain application. (2016).

[29] Florian Tschorsch and Björn Scheuermann. 2016. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials* 18, 3 (2016), 2084–2123.

[30] Marko Vukolic. 2015. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec 2015, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 9591)*. Springer, Zurich, 112–125.

[31] Lei Xu, Lin Chen, Zhimin Gao, Shouhuai Xu, and Weidong Shi. 2017. EPBC: Efficient Public Blockchain Client for lightweight users. In *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, SERIAL@Middleware 2017*. ACM, Nevada, 1:1–1:6.

[32] Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang. 2019. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Communions Surveys & Tutorials* 21, 2 (2019), 1508–1532.