The Zilliqa Project:
A Secure, Scalable Blockchain Platform

[Non-Binding until Formal Document is Offered. Content Subject to Change]

The Zilliqa Team
Version 0.5
November 2017

[DISCLAIMER]

This paper is for information purposes only and does not constitute and is not intended to be an offer of securities or any other financial or investment instrument in any jurisdiction.

Anquan Capital and Zilliqa Research disclaim any and all responsibility and liability to any person for any loss or damage whatsoever arising directly or indirectly from (1) reliance on any information contained in this paper, (2) any error, omission or inaccuracy in any such information, or (3) any action resulting therefrom.

A. Executive Summary

Blockchain platforms are bringing to life the concept of a consensus computer --- a distributed network of computers carrying out useful tasks. One of the most pressing problems facing these platforms is their lack of *scalability,* i.e., the ability to handle a larger number of transactions per second as the network grows. A number of works have noted how existing blockchains are handicapped in their ambition to scale the next generation of Internet-style applications. An oft cited example is the 3-7 TX/s available in Bitcoin and Ethereum today, and the demands of payment processing in centralized operators (e.g., VISA, MasterCard) for supporting thousands of TX/s.

Zilliqa is a new blockchain platform that is designed to securely scale in an open, permissionless distributed network. The core feature that makes Zilliqa scalable is *sharding* --- the division of the network into several smaller component networks capable of processing transactions in parallel. As a result, the transaction rate in Zilliqa increases as the mining network expands. Zilliqa aims to rival traditional centralized payment methods such as VISA and MasterCard. In fact, with a network size of 10,000 nodes, Zilliqa will enable a throughput which matches the average transaction rate of VISA and MasterCard with the advantage of much lower fees for the merchants.

Zilliqa leverages proof-of-work (PoW) to establish identities and perform sharding. However, unlike several existing blockchain platforms (such as Ethereum and Bitcoin), Zilliqa does not employ PoW to achieve consensus.

This provides several advantages:
1. PoW can be performed after, say every few hundred blocks. As a result, the high energy cost often associated with PoW will not apply in Zilliqa. In fact, we estimate that the cost of running a Zilliqa node will be about 1/10 of running an Ethereum node today.
2. Since miners reach consensus on several blocks with a single PoW, Zilliqa ensures a much more stable payout with low variance.

Furthermore, the unprecedented throughput of Zilliqa implies that the processing fee per transaction can be very low. In many of today's popular blockchains, users have to compete for the few transactions processed per second. As a result, transactions with low or insufficient fees experience delays in processing. Such issues will be significantly alleviated

in Zilliqa as the number of transactions processed per second becomes several hundred times more and beyond.

Zilliqa will support a smart contract platform with a novel scripting language that is sharding-friendly, i.e., it will allow users to compute programs in parallel, harnessing the full computational capacity of the mining network. For instance, the Zilliqa platform will allow users to build distributed advertising networks, conduct parallel auctions, deploy MapReduce-style trading algorithms, run a shared economy, etc.

Zilliqa aims to support high-throughput data-intensive applications via a *dataflow-style programming* language interface. The underlying sharding architecture allows Zilliqa to support high throughput, both in terms of transactions processed as well as smart contracts executed per block epoch.

The Zilliqa team consists of computer scientists with PhDs from some of the world's best universities and research institutions including Princeton, Berkeley, Inria and NUS. The team also consists of developers with many years of secure software systems-building expertise. The advisors to the project include established academics in cybersecurity, technology entrepreneurs, bankers and leading experts in the cryptography community. The Zilliqa team proposed the theory of sharding in an academic paper in 2015, and since then the protocol has been under research, refinement and active development (through Anquan Capital Pte Ltd, a Singapore-based deep technology company). Zilliqa's infrastructure has been trialed in the financial services sector, for example enabling transparency and efficiency that were hitherto not possible in the Over-The-Counter (OTC) securities markets.

We are now at the stage of developing a public testnet prototype of Zilliqa's protocol, so that users can see its operational capabilities. However, there are many more innovations and development milestones ahead of us that will enable further scalability and add many significant features to Zilliqa. As outlined in the section of Roadmap, we will release a testnet of Zilliqa's initial implementation in December 2017. The source code of the testnet as well as future development will be made freely available to the public.

We believe that the public release of the Zilliqa protocol will enable development of scalable blockchain applications that will return enormous benefits to the users of Zilliqa and the applications built on it.

Table of Contents

B. Why Zilliqa?

Blockchain scalability is a pressing issue that has attracted much attention, as seen in recent plans to scale Bitcoin and Ethereum in the future.

However, it is unclear whether such proposals can scale up to the ever increasing network size without discarding legacy transactions. In the wake of the recent Bitcoin split, it is further evident that a truly scalable solution would require a clean-slate design that is built with scalability in mind.

Zilliqa is exactly that design - we have chosen to develop a clean-slate design and have built a new blockchain that develops and deploys our innovations around a scalable and secure protocol.

In order to illustrate the growing need for a scalable blockchain, we outline a particular industry use case in digital advertising. This is just one example of a large scale market opportunity that can be enabled by the Zilliqa blockchain.

Illustrating Example: Building A Blockchain-based Digital Advertising Supply Chain

The most basic advertising supply chain involves the following three entities:
1) Marketers who wish to promote their product through ads,
2) Publishers who show ads, and,
3) The target audience for the advertisements.

Marketers pay publishers to show the ads to the target audience. However, in reality, there exist several other entities in the digital advertising ecosystem such as ad agencies, ad exchanges and networks, various forms of middlemen who buy and sell ad impressions, etc. These entities form a digital marketplace where publishers can sell (or auction) advertising space and marketers can buy them.

The digital ad ecosystem as it exists today is plagued with issues, which adversely affect many players in the ecosystem. For instance, due to the presence of several layers of middlemen, the cost of digital advertising goes up while marginalising the revenue of publishers. Moreover, in recent years marketers have faced serious fraud attacks, where attackers using Internet bots present fake publishers and users to siphon off millions of dollars from victim marketers. Beyond monetary loss, such attacks also leave marketers with a completely spurious belief on where their advertisements have been delivered. This may further lead to poor judgement in evaluating the effectiveness of their marketing campaign. Users too get affected as they often receive uninteresting, offensive or unsafe advertisements. This drives many to use ad blockers, which unsettles the entire advertising-based web economy.

With the blockchain technology, we envision that a simplified supply chain can be implemented in the form of smart contracts. For instance, marketers who wish to deliver advertisements can submit smart contracts to specify general and specific requirements for ad impressions they need, including target audience profiles, geographic restrictions, time

constraints in ads delivery, etc. Publishers or ad networks, can also submit smart contracts to sell ad spaces in bulk with different properties in terms of publisher page context, as well as audience user profiles. Once submitted to the blockchain, the smart contracts from marketers and those from the publishers can automatically match against one another to instruct ad content delivery. The smart contracts can also record evidence of claimed impressions, and settling the payment as per agreed upon between different parties.

Such a blockchain-based advertising supply chain will solve many of the existing issues by enabling a fair marketplace with transparency and accountability. For instance, with such a digital marketing platform, those middlemen who merely buy and sell ad impressions may no longer be relevant. This will further reduce the cost of the marketing campaign, and drive the entire ecosystem into more efficient and effectiveness execution. Moreover, if all transactions regarding ads delivery, impression and payment are backed by a blockchain, then the marketers can obtain details on each ad impression, who saw the ad and where the traffic ends up. It can further provide an audit trail of every stage of the advertising process and would give a way to correctly measure the success of a marketing campaign. Equipped with the right data, marketers can take future decisions with much greater confidence. Several ongoing efforts such as BAT, adChain, AdEx, among others have plans to run digital ad supply chain on blockchains.

However, there are fundamental limitations of the existing blockchain protocols to support such a digital supply chain as it gains popularity. We list some of them below, and then discuss how Zilliqa addresses these challenges with a new scalable blockchain backed by several technical advancements.

1. **High Volume:** Since digital advertising is run programmatically, it entails high volume both in terms of the number of ads served and the number of ad impressions collected. If on-chain digital advertising ever becomes popular, it should be able to handle billions of ads and ad impressions per day. None of the existing blockchain platforms are capable of processing transactions at this rate even if they dedicate the entire network to process only ad related transactions and nothing else. For instance, Ethereum as of today can process a maximum of around a million transactions per day, while Bitcoin around 50,000 transactions per day.

2. **Real-time Parallel Bidding:** The sale of advertising space is often done via a real-time auction. Clearly, the auctioning is expected to be an efficient process. First of all, bidders should not have to wait for long before being able to successfully bid for tokens. This should be the case even under high volume and volatility. Moreover, bidders should be able to bid for multiple advertisement spaces for sale in parallel without sacrificing efficiency. However, auctioning of digital tokens on existing blockchains in the recent months shows a dismal trend. During a crowdsale or auction of digital tokens, the transaction volume often gets increased by an unexpected magnitude to an extent that wallet services are forced to scale from 10% capacity to 1000% capacity in the course of less than a minute.[1] As of now, these

[1] https://qz.com/1004892/the-bancor-ico-just-raised-153-million-on-ethereum-in-three-hours/

auctions (or crowdsale) are carefully timed in a way that two big events do not end up running in parallel. However, this is unrealistic in the case of real-time bidding as multiple ad spaces are routinely auctioned in parallel.

3. **Correctness:** The rightful winner should get the advertising space at the expected bidding price, which is paid to the seller. In existing smart contract platforms, the correctness is hard to be guaranteed. Bidders have to trust the seller. In fact, even if the bidder is honest, the contract code may have vulnerabilities that may lead to an incorrect outcome of the auction. Moreover, existing contract codes are hard to reason about for correctness.

4. **Fairness:** None of the buyers/sellers gets disadvantaged in the auctioning process. For reasons similar to the previous property, it is not clear how to argue about fairness in existing smart contract codes.

These challenges are by no means exhaustive, but they are typical for the large-scale distributed dApps that Zilliqa aims to support. We now discuss how these challenges are addressed by Zilliqa.

It is evident that efficiency is key to the success of such an application. As for any blockchain platform, it should be able to process the ensuing high-volume transactions. Failure to do so would mean heavy congestion and transaction queuing. Moreover, the underlying blockchain protocol needs lots of message exchanges to reach any agreement. Such message exchanges are required for security against malicious nodes, yet constituting severe gridlocks for performance and scalability.

To resolve such gridlocks, Zilliqa leverages an orchestrated secure *network sharding* scheme that can automatically divide, say, bidding requests into a subgroup of nodes. All subgroups can simultaneously process different ad space auctions. They also lock the deposit from different bidders before the final bidding results are obtained. This significantly improves the throughput of such an application.

Moreover, Zilliqa supports the computation of highly sophisticated optimization algorithms to conduct and participate in auctions via *computational sharding*. In this respect, the auction application can instruct Zilliqa to form many small groups of nodes to compute. Each group is tasked to compute a portion of the algorithm, such as many groups for multiplication of different matrices, some other groups for sorting, and finally groups for aggregation. Nodes inside each group independently compute the task and cross-check against one another. Zilliqa allows different levels of security to be enforced as requested by the application on a needs basis.

The correctness of the result is guaranteed at two levels: consensus level and the contract level. At the consensus level, almost all honest nodes agree on the final auction allocation results. This is typical to any distributed system where, if just a few nodes make the final decision, the system would lose all the desirable properties of decentralization. Zilliqa innovates on several new techniques to develop a protocol that enables almost all honest nodes to quickly and unambiguously reach a conclusion for sale requests and bids

processed across the entire network. For instance, Zilliqa develops an *efficient collective signature* scheme to make it secure even in a highly hostile environment. This signature scheme is then used to significantly reduce the convergence time needed for reaching the auction allocation results across the network.

At the contract level, Zilliqa uses a *data-flow style programming* language that allows us to reason the correctness of the contracts in an easy manner. The data-flow language approach is also useful to prove several other properties such as fairness. Moreover, a data-flow program provides the potential for massive parallel execution. Roughly speaking, a data-flow program can be interpreted as a graph where a vertex represents a computational unit that can start processing the moment its inputs become available. To continue with our advertising supply chain example, some vertices of the graph can handle the placing of bids for advertising space, another set of vertices may process the bids to find the winners, while a set of dedicated vertices may handle the settlement of payments. The first set of nodes can independently process bids for several advertisement spaces in parallel. Once a bid for advertisement spaces are placed, the next set of vertices can run the auctioning algorithm in parallel to find the winner for each advertisement space (again in parallel) and the last set of vertices can transfer funds. Zilliqa's smart contracts have built-in support for dependency, atomicity and consistency between such different sets of operations.

The advertising supply chain is just one example of many high-throughput dApps which Zilliqa can enable. We will discuss other applications in the section entitled Sample Applications Enabled By Zilliqa.

C. Key Features of Zilliqa

Zilliqa is built to scale from many aspects. It leverages a *network-level sharding* mechanism to divide the nodes in the network to process transactions in parallel, and an atomic *transaction sharding* protocol to ensure transactions are accepted as if there is no sharding. Zilliqa also proposes a novel *computational sharding* framework to allow computation-intensive applications to be executed efficiently over the network. To facilitate a high-level understanding of them, we describe some of the key ideas below.

1. Network Sharding

Zilliqa dynamically splits the network of blockchain nodes into different subgroups, called *shards*, with each shard formed to process and reach consensus on a subset of transactions. This way, disjoint subsets of transactions can be processed in parallel, and significantly boost the transaction throughput by orders of magnitude. Eventually, such transactions are merged into a new block that is committed to the blockchain.

The primary challenge in realizing such network sharding is how to ensure the security of the protocol. The naive approach would suffer from much higher susceptibility to compromised blocks as the size of the consensus groups is smaller under network sharding. To address security implications from it, we invent a new protocol that achieves scalability with strong

security guarantees, inspired by our innovative research outcome [1] and other state-of-the-art research literature [2] [3].

The gist of our network sharding protocol is to leverage a proof-of-work (PoW) puzzle to elect and update a *directory service committee* in a decentralized and democratic manner. The directory committee is tasked to coordinate the sharding process, as well as validate the blocks of transactions proposed by each shard and verify if they have received approval from a sufficiently large quorum within the shard.

Unlike several existing blockchain platforms (such as Ethereum and Bitcoin), Zilliqa does not employ PoW to achieve consensus. In fact, PoW is used only to prevent sybil attacks and perform sharding. As a result, it can potentially be replaced by any other sybil resistance mechanism such as proof-of-stake (PoS). Our choice of PoW is motivated by the fact that its security guarantees have been well studied in the literature unlike PoS which is still under active research.

2. Secure & Efficient Consensus Algorithm

Within the directory service committee and each shard that processes and accepts transactions, we run a secure and efficient consensus protocol. The protocol enables each shard to reach an agreement on the blocks to propose. Our consensus protocol is based on the idea of *byzantine fault tolerance* (BFT) [4] with heavy optimizations. We choose BFT to design our consensus protocol to ensure that the resulting blocks are definitive, without the need of long confirmation times as required in the popular “longest-chain” rule in existing cryptocurrencies. However, existing BFT protocols entail a large communication bandwidth and hence time elapsed to converge. As a result, they do not scale well to a large network of nodes.

We specifically identify a recently proposed scalable signature scheme CoSi [5] that has the potential to make BFT protocols much more scalable. The challenges we faced here was that CoSi was proposed to work in a much less hostile environment than that of a public blockchain. With several significant enhancements we develop for the CoSi scheme. In particular, we add extra steps and message rounds to the CoSi protocol both on the leader's side and on the signer's side to prevent malicious leaders and signers in the protocol. The added steps and checks ensure that malicious behaviors get detected as early as possible. As a result, we derive a secure scheme and apply it to develop a scalable BFT protocol for consensus in Zilliqa.

3. Transaction Sharding

Zilliqa employs account-based design. The account-based design allows transactions to be sharded according to the sending accounts. This ensures that attacks akin to double spending or replay can be thwarted by the same shard of nodes. For better scalability, Zilliqa makes two conscious choices in the design of transaction sharding: 1) Zilliqa provides atomic transaction commits without involving cross-shard communication that is often costly and complex. 2) Zilliqa allows transactions to be processed asynchronously with the

consensus processes of the blockchain. Zilliqa adopts a “reject-and-retry” mechanism to asynchronously process transactions as and when the majority of nodes become up-to-date.

4. Computational Sharding & Data-flow Smart Contract Language

Smart contracts allow applications to be built on top of the distributed ledger provided by the blockchain storage and consensus. However, today’s mainstream public blockchains are not suitable for running computation-intensive tasks, as any of the computation tasks would have to be repeated at all full nodes for validation. Albeit being secure, such a fully redundant programming model is prohibitively expensive for running large-scale computations.

With scalability as the main goal of Zilliqa, we propose a new smart contract language that scales much better for a multitude of applications that range from automated auctions, shared economy to financial modelling.

The smart contract language in Zilliqa follows a *dataflow programming paradigm*. In the dataflow programming model, a smart contract is represented by a directed graph. Nodes in the graph are primitive instructions or operations. Directed arcs between two nodes represent the data dependencies between the operations, i.e., output of the first and the input to the second. A node gets activated (or operational) as soon as all of its inputs are available. This stands in contrast to the classical execution model (as employed in Ethereum), in which an instruction is only executed when the program counter reaches it, regardless of whether or not it can be executed earlier.

The key advantage of employing a dataflow approach is that more than one instruction can be executed at once. Thus, if several nodes in the graph become activated at the same time, they can be executed in parallel. This simple principle provides the potential for massive scalable execution. To see this, consider the simple example of naive matrix multiplication of two square matrices A and B. Let the resulting matrix be C. Then, each entry of C can be independently computed by considering a row of A and a column of B. Since each of these operations are independent, they can in fact be performed in parallel. When run on the Zilliqa’s sharded network, each node in the dataflow program can be eventually attributed to a single shard or even a small subset of nodes within a shard.

More specifically, this smart contract language has the following features:

- Data sharing between smart contracts via virtual memory space.
- 2-phase commit for atomic execution.
- First-order abstraction for computing MapReduce tasks.
- Flexible security budgeting via computational sharding.

The last feature is enabled by sharding the computational resources in the blockchain network via an overlay above the consensus process. Computational sharding allows users of Zilliqa and applications running on Zilliqa to specify the sizes of consensus groups to compute for each of the subtasks. Each consensus group will then be tasked to compute the same subtask, and produce the results. The user specifies the condition on acceptance of

the results, e.g., all in the consensus group must produce the same results, or ¾ of them must produce the same results, etc.

We apply gas fees to bound the computation required for smart contract execution and prevent abuse of computational resources available on the blockchain. A user of the application running on Zilliqa can budget how much he or she wants to spend on computing and security, respectively. In particular, a user running a particular application may spend more gas fee on running different subtasks than letting too many nodes repeating the same computation. In this case, he or she can specify a smaller consensus group for running each neural network computation. On the other hand, a sophisticated modeling algorithm that requires greater precision may task consensus groups of larger number of nodes to compute the critical portions of the algorithm to be more resilient against potential tampering and manipulation of the results.

Finally, equally important to the efficiency of smart contract execution is its friendliness to programmers. Although dataflow programming is very good for efficiency and easy to be automatically verified for its security and correctness, it may not be the programming language and model that most programmers today are familiar with. To address this challenge, Zilliqa will provide a front-end higher level language to programmers, whose syntax will be similar to Solidity. We will develop compilers to automatically convert such Solidity-like smart contracts into the underlying dataflow programming language. We believe such syntax-level compatibility with Solidity will ease the migration cost of some existing smart contracts to Zilliqa for much higher-throughput.

5. Profitable Mining

As discussed earlier, Zilliqa uses PoW only to establish identities and prevent sybil attacks. Zilliqa does not use PoW to reach consensus on blocks. This has the following two advantages:

1. once the identities are established, the nodes can reach consensus on several blocks in a row. As a result, a PoW can be performed after, say every few hundred blocks. This is in contrast with the use of PoW as in Bitcoin and Ethereum where, a new PoW solution is required to reach consensus on every new block. As a consequence, the energy cost often associated with PoW per block will on average be very low in Zilliqa.
2. since miners can reach consensus on multiple blocks during an epoch, they are guaranteed more stable rewards with low variance.

The unprecedented throughput of Zilliqa also has an important impact on the incentives that miners draw from transaction processing, i.e., gas fees (or transaction fees). In many of today's popular blockchains, users have to compete for the small number of transactions that can be processed every second. Miners also tend to pick transactions with higher fees to compensate for their operational costs. As a result, transactions with low or insufficient transaction fees will experience delays in processing, or worse can be held indefinitely. The situation may further deteriorate as mining rewards close to zero in currencies with finite

supply such as Bitcoin. Recently in August 2017, the average transaction fee in Bitcoin rose as high as USD 9[2]. Such issues will be significantly alleviated in Zilliqa. As the number of transactions processed per second becomes 200x more or beyond, the competition in terms of transaction fees will be less intense. At the same time, the cost of processing a transaction on the miners' side is also cut by orders of magnitude. We expect that the bar for transaction fees acceptable to miners will be lowered significantly.

Note that a low fee in Zilliqa does not necessarily imply that miners are insufficiently incentivized. On the contrary, due to its high throughput, the aggregated sum of incentives from several transactions can compensate the low fee per transactions.

D. Comparison to Existing Techniques

Many proposals have surfaced to scale up the transaction throughput of existing blockchain protocols, for instance, re-parameterizing the original Bitcoin protocol (e.g., increasing block sizes), moving as much computation off-chain (e.g., micropayment channels and lightning network), creating hierarchy of blockchains (e.g., sidechains). None of these protocols directly make the blockchain protocol itself more scalable. Zilliqa targets the heart of the scalability problem --- its own blockchain. Having said that, any of these scaling mechanisms can be used on top of Zilliqa to further scale its throughput.

Zilliqa is based on ideas inspired by Bitcoin-NG [2], CoSi [5], ByzCoin [3], and the Elastico proposal [1]. The scalability goal is intrinsic throughout the different layers of Zilliqa, from network sharding, secure and efficient consensus protocol with multi-signature, to computational sharding and data-flow smart contract language. Without any legacy of blockchain design and protocols and transaction or block formats that hinder scalability, Zilliqa has a promising trajectory to hundreds and thousands of times more scalability than existing public blockchains.

E. Sample Applications Enabled By Zilliqa

It is Zilliqa's mission to support highly scalable computations such as automated auctions, financial modelling, advertising supply chain, shared economy to name just a few. Zilliqa focuses on such specific applications (dApps) with throughput and scalability requirements that cannot be met today.

1. Automated High-Volume Auctions

Zilliqa is ideal for building a token trading dApp suite. The trading app should allow digital tokens from several sellers to be auctioned among a set of potential buyers in parallel. With the growing popularity of crowdsale to fund blockchain related projects, such a dApp is clearly useful. Zilliqa provides the infrastructural support for conducting any trading application at high volume and large scale.

[2] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y

2. High-Performance Scientific Computing

Typical examples of this category of applications include large matrix operations, search in the sea of huge amount of data, simulation over a large dataset, etc. Instead of building highly available and capable data centers, Zilliqa provides such computing tasks with an inexpensive and short turnaround alternative. With Zilliqa, volunteer computing such as the search for extraterrestrial intelligence (SETI), can be significantly secured from attacks targeting the experiments themselves or the computers participating in the experiments. Moreover, with the right incentive in place with computational sharding, Zilliqa can be leveraged as a readily available and highly reliable resource for such heavy computation load.

3. Applications Requiring Highly Reliable Results

Different from the applications mentioned above, some applications, such as computations over financial models, may require very reliable results. Any minor error or mistake, benign or affected by malicious attacks, may incur heavy capital or monetary losses. Such applications can task consensus groups of larger number of nodes in Zilliqa to allow them to cross-check the computational results of each other. One key challenge in offloading the computational tasks of such financial modeling algorithms to a public platform, such as Zilliqa, is the concern of data privacy and intellectual property of the algorithms. To begin with, we envision that a certain well known portion of such computation can be placed to Zilliqa for efficient and secure computation first, while the future research and development of Zilliqa will further strengthen the protection of data privacy and intellectual property for such applications.

F. The Zilliqa Team

Zilliqa is initiated by a team of renowned entrepreneurs and scientists, as well as engineers with strong expertise in cybersecurity and systems. Most of them have a PhD in computer science or engineering.

Xinshu Dong (CEO)
PHD, NATIONAL UNIVERSITY OF SINGAPORE

Xinshu is a scientist and practitioner in building secure systems, ranging from blockchains to web browsers and applications. He was a technical lead for several national cybersecurity projects in Singapore. The outcome of his research has been published at top international conferences. More recently, he led the research and development of Anquan's proprietary scalable and secure blockchain, deployed for financial and ecommerce applications. He is currently leading the Zilliqa team for developing a new public blockchain, Zilliqa, for high-throughput applications.

Prateek Saxena (Chief Scientific Advisor)
PHD, UNIVERSITY OF CALIFORNIA, BERKELEY

Prateek Saxena is a research professor in computer science at National University of Singapore, and has a PhD in Computer Science from UC Berkeley. He works on

blockchains and computer security. His research has influenced the design of browser platforms, web standards and app stores widely used today. He has received several premier awards such as the Top 10 Innovators under 35 (MIT TR35 Asia) in 2017.

Christel Quek (Head of Marketing)
BSc SOCIAL SCIENCES, NATIONAL UNIVERSITY OF SINGAPORE

Christel has built brands and digital businesses since the advent of the digital economy. She is a Co-Founder of BOLT, a live TV & gaming service (over 3M users in Kenya, Southeast Asia, and Latin America), and the Founder of pin8cle, a strategic consultancy to turn start-ups to rev-ups. Previously, Christel founded Brandwatch's first office in Asia-Pacific (fast-growth, digital intelligence and analytics), was the Head of Content at Twitter across their International Markets, and led Social Business for Samsung Asia. Christel was selected by The Guardian as one of the top global digital strategists, Campaign Asia-Pacific as a Woman to Watch, and Business Insider as one of the 30 best executives to follow on Twitter. More recently, Christel delivered the commencement speech at the National University of Singapore in 2016, and has contributed articles to Harvard Business Review and Huffington Post.

Yaoqi Jia (Blockchain Architect)
PHD, NATIONAL UNIVERSITY OF SINGAPORE

Yaoqi is a Research Fellow at the National University of Singapore. He gained his Ph.D. in Computer Science from NUS. His research interests span web security and privacy, network security, distributed systems and applied cryptography. He has proposed solutions to addressing consensus and privacy issues in P2P systems. His work has been published in top-tier security conferences, got acknowledged by various vendors including Google and Apple and has received attention from the media including Dailydot, Gizmodo and Techspot.

Max Kantelia (Visionary)
BSC (HONS) ENGINEERING SCIENCE

Max is a financial services entrepreneur with 25 years' experience of building professional services and technology firms in Europe, the US and Asia. He is a Co-Founder of Anquan Capital in Singapore and is on the board of Aeriandi (Oxford) and untapt (New York), both fast growth deep technology companies in the areas of voice technology and artificial intelligence. Max is an engineering graduate and started his career at GEC Marconi designing airborne radar systems. He was selected by EY as one of Asia's Top 100 FinTech contributors in 2016 and is a part of the London Mayor's Internationalisation programme.

Amrit Kumar (Crypto Lead)
PHD, UNIVERSITÉ GRENOBLE-ALPES (FRANCE)

Amrit is a Research Fellow at the National University of Singapore. He holds a PhD from Université Grenoble-Alpes, France and was hosted at Inria's Grenoble center. Prior to his PhD, he obtained an Engineer's diploma from Ecole Polytechnique, France, where he

studied Computer Science and Mathematics. His research interests broadly span security, privacy and applied cryptography.

Juzar Motiwalla (Strategist)
PHD, UNIVERSITY OF WISCONSIN - MADISON

Juzar Motiwalla has investment and board-level experience with global technology startups. He was a venture capitalist responsible for investments in Asia and Silicon Valley. M&A exits with leading US and Japanese companies were secured for companies he was involved with. Prior to his venture capital journey he was the CEO of a 350-person computer science research lab in Singapore.

Antonio Nicolas Nunez (Core Dev)
BACHELOR IN PHYSICS AND COMPUTER ENGINEERING, ATENEO DE MANILA UNIVERSITY

Antonio has bachelor degrees in Physics and Computer Engineering from Ateneo de Manila University, as well as a diploma in R&D Management from University of the Philippines Open University. He has over 10 years experience as a software engineer, deploying industry-grade solutions for multiple sectors. His programming interests include efficient C++ coding as well as build and test automation.

Jun Hao Tan (Core Dev)
BACHELOR OF COMPUTER SCIENCE (HONOURS), NATIONAL UNIVERSITY OF SINGAPORE

Jun Hao is a practitioner in various areas in the Computer Science domain including blockchain, web security, trusted computing and program analysis. He was also awarded the National Infocomm Scholarship and graduated from the National University of Singapore (NUS) with a bachelor degree in computing science with specialisation in information security. At NUS, he co-founded NUS Greyhats, a cybersecurity interest group, which has won numerous cybersecurity events. He also co-founded Edgis, a non-profit special interest group provides a platform where infosec enthusiasts can meet, exchange ideas with others and contribute to community.

Siddhartha Dutta (Core Dev)
BACHELOR OF TECHNOLOGY (HONOURS), IIT BOMBAY

Siddhartha graduated from the Indian Institute of Technology Bombay with a bachelor degree in Computer Science and Engineering. His technical interests include Operating Systems, Computer Networks, Distributed Systems and NLP. He has worked at Microsoft and Adobe Research where his work led to two patent applications. He cofounded HumBee, a political social network to encourage critical thinking and enable collective action on social issues.

Advisors to Zilliqa

Aquinas Hobor
PHD, PRINCETON UNIVERSITY

Aquinas Hobor got his undergraduate degrees from the University of Chicago and his PhD in computer science from Princeton University in 2008. He does research in computer theory, including semantics, verification, machine-checked proof, logic, complexity, and algorithms. From 2008-2011 he was a Lee Kuan Yew Postdoctoral Fellow in the School of Computing, National University of Singapore. Since 2013 he has been an assistant professor with a joint appointment between Yale-NUS College and the School of Computing.

Alexander Lipton
PHD, MOSCOW STATE UNIVERSITY

Alexander Lipton is Founder and CEO of StrongHold Labs, Partner at Numeraire Financial, Co-Founder and Advisor of Distilled Analytics, Connection Science Fellow at MIT Media Lab and Visiting Professor of Financial Engineering at EPFL. He is an Advisory Board Member at UCL Centre for Blockchain Technologies, Clearmatics and Numerix. His prior experience includes Managing Director at Bank of America Merrill Lynch, leading the quant group. Earlier, he also worked for Citadel Investment Group in Chicago, Credit Suisse, Deutsche Bank and Bankers Trust.

While working full time as a banker, Alex held several prestigious academic appointments, including Oxford-Man Institute, Imperial College London and the University of Illinois. Before switching to finance, Alex was a Full Professor of Mathematics at the University of Illinois and a Consultant at Los Alamos National Laboratory. He received his undergraduate and graduate degrees in pure mathematics from Moscow State University.

In 2000 Alex was awarded the first Quant of the Year Award by Risk Magazine. Alex is the author of two books and a hundred papers on hydrodynamics, magnetohydrodynamics, astrophysics, chemical physics, and financial engineering.

Loi Luu
PHD, NATIONAL UNIVERSITY OF SINGAPORE

Loi is a researcher working on cryptocurrencies, smart contract security and distributed consensus algorithms. He is also a regular invited speaker at Bitcoin and Ethereum workshops such as DevCon2, EDCON. Loi believes in the force of the Ethereum and Blockchain technologies and much of his work revolves around this community. He developed Oyente, the first open-source security analyzer for Ethereum smart contracts. Loi also cofounded SmartPool, another open source project which embraces decentralization of mining pools in existing cryptocurrency. He continues to champion decentralisation and trustless properties of the Blockchain with KyberNetwork, taking inspiration and developing value for the community.

Stuart Prior

Stuart Prior is a Fintech veteran with 20+ in Corporate and Investment Banking. Stuart specializes in leading corporate banking initiatives for the adoption of blockchain technology and Crypto Finance. Throughout his career he has focused on the development of banking technology applications including Ultra High Frequency / Low Latency trading and the development of large scale data management platforms. Over the years he has worked with many of the largest banks in the world, including Credit Suisse and Deutsche Bank, and will bring his expertise to help guide Zilliqa's development and practical applications.

G. Roadmap

Time	**Development Milestones**
Jun 01, 2017	Project Zilliqa started
Aug 10, 2017	Whitepaper released
Sept 01, 2017	Experimental result release of internal testnet v0.1 ● Cryptographic primitives & proof of work ● Data layer ● Network sharding ● Consensus based on BFT and Schnorr signature
Oct 01, 2017	Experimental result release of internal testnet v0.5 ● Transaction sharding & processing ● Persistent storage
Nov, 2017	Releasing design documentation on ● The smart contract language framework and design
Dec, 2017	Releasing public testnet v1.0 Releasing source code of public testnet v1.0 ● Facilitating new nodes joining ● Linux-based miner software ● Wallet software ● Performance optimizations ● Feedback & bug fixes
Q1, 2018	Releasing public testnet v1.5 ● Resilience and recovery ● Support for basic features of smart contracts ● Performance optimizations ● Feedback & bug fixes
Q2, 2018	Launching the first version of Zilliqa public mainnet ● Computational sharding for smart contracts
Q3, 2018	Releasing dApps

H. Plans on Future Research & Development

The focus of Zilliqa Research is to lead the research and development of the platform from an initial implementation to a full public blockchain platform. The mission of Zilliqa will remain to further increase the scalability of the blockchain and dApps running on it to gain 100x to 1000x over today's public blockchain platforms. To achieve that, there is a long journey of innovation and development. We briefly outline some of the research ideas that we would like to explore.

State Sharding

The first release of Zilliqa achieves scalability without state sharding. In essence, state sharding will alleviate full nodes from storing and receiving all blocks and transactions. This way it can further reduce the storage and communication load for blockchain nodes, and thus constitute another scaling-up factor to the throughput. However, it is non-trivial to design a secure and efficient state sharding scheme, as cross-shard communications arising from state sharding may outweigh the performance gains. More research needs to be done to address such additional complexity.

Secure Proof-of-Stake (SPoS)

Proof of stake (PoS) schemes are a promising direction for efficient blockchain consensus protocols. However, at Zilliqa security has always been a top priority. We believe PoS schemes are still at an early stage, and the security and decentralization of such schemes are still to be further studied and analyzed. Thus, we base Zilliqa's building blocks on schemes that have been shown to be secure over time, e.g., proof-of-work and byzantine fault tolerance. However, given the significant performance gain from PoS for consensus algorithms, it is worthwhile investigating further into the PoS paradigm, in search for a secure and efficient PoS scheme for Zilliqa.

Storage Pruning

We will also explore ways to securely prune the dated blocks stored on the blockchain to reduce the storage requirements and ease the joining process for new nodes. We may consider multi-grade storage, compression of blocks and transactions as possible solutions.

Cross-Chain Support

Zilliqa has every intention to complement other public blockchains and build a healthy ecosystem to provide end users a broad spectrum of platforms of choice for their applications. To this end, Zilliqa will seek technical solutions to support gradual cross-chain communication and potentially enable cross-chain applications.

Privacy-Preserving Computation

It is desirable by financial modeling applications to have strong privacy and intellectual property protection when running on Zilliqa. We will conduct more research into leveraging efficient cryptographic schemes that can render such protection. For instance, we plan to explore solutions that re-encrypt different pieces of sensitive data with operation-specific homomorphic encryption schemes and dispatch the data to specific consensus groups for performing a single operation on it. For instance, certain consensus groups are tasked to only perform addition, while others multiplication, for greater efficiency.

I. References

[1] Elastico: A Secure Sharding Protocol For Open Blockchains, Loi Luu, Viswesh Narayanan, Kunal Baweja, Chaodong Zheng, Seth Gilbert, Prateek Saxena, ACM Conference on Computer and Communications Security (CCS 2016)

[2] Bitcoin-NG: A Scalable Blockchain Protocol, Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse, In Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation (NSDI 2016).

[3] ByzCoin: Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, Bryan Ford, In Proceedings of the
25th USENIX Security Symposium (USENIX 2016).

[4] PBFT: Practical Byzantine Fault Tolerance and Proactive Recovery, by Miguel Castro and Barbara Liskov, ACM Transactions on Computer Systems (TOCS), vol. 20, no. 4, Nov. 2002, pp. 398-461.

[5] CoSi: Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning, Ewa Syta, Iulia Tamas, Dylan Visher, and David Isaac Wolinsky and Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford, 37th IEEE Symposium on Security and Privacy (SP 2016).