An analysis into the scalability of Bitcoin and Ethereum.

Richard Dennis[1] and Jules Pagna Disso[2]

[1] University of Portsmouth, Portsmouth, United Kingdom
[2] Nettitude labs, Leamington Spa, United Kingdom
Richard.dennis@port.ac.uk

Abstract. With cryptocurrencies and blockchain based networks being increasingly used for more and more applications, a fundamental issue is now being notice; scalability. In this paper we conduct what we believe the first long term assessment of the two largest blockchain based networks; Bitcoin and Ethereum. Using historic data, we model how their growth could be over the next three years and propose a model, a temporal blockchain, to reduce the network size and increase scalability.

Keywords: Bitcoin, Ethereum, Scalability, Peer-to-peer.

1 First Section

Currency is a first-to-file application, where the order of transactions critical, for a cryptocurrency to be successful a solution to a decentralized consensus without a requirement of a centralized repository system or administrator was needed to be found.

The foundations of cryptocurrencies were published by Wei Dai, proposing d-money in 1998, with the key contribution of being rewarded with a token through solving a computationally expensive puzzle. This would later form the foundation of proof of work, however due to poor implementation details this idea was never deployed.

Hal Finney expanded on d-money in 2005, implementing a concept of reusable proof-of-work (PoW) in addition to Hashcash puzzles to create arguably the first cryptocurrency. However, since the decentralized consensus problem was still not solved, this model relied on a trusted computing back end so was not widely adopted.

Taking the previous research in the field of cryptocurrencies, Bitcoin was invented by an unknown programmer, or a group of programmers, under the name Satoshi Nakamoto, published in a white paper in 2008, before being released as open-source software in 2009.

The key invention made by Nakamoto was the blockchain is a novel peer-to-peer approach which links a sequence of transactions or events together in a way that makes them immutable, without the requirement of a centralized authority, solving the decentralized consensus problem.

The blockchain is a public ledger of all transactions that have ever been completed since the first “genesis” block.

Each transaction from the Bitcoin protocol is broadcast to all nodes in the network which are maintaining the blockchain. This means the blockchain is constantly growing, as no data is ever deleted from the blockchain.

The blockchain has since become the foundations of 1394 cryptocurrencies currently being traded (09.01.2018) with a market cap of $739,163,041,418.

Bitcoin is the most successful blockchain-based network; it has a market cap of over USD 8.5 billion and sees an average of 214,000 transactions being conducted on its network every day.

Bitcoin is not the only successful currency of Blockchain technology. Ethereum, considered as blockchain 2.0, is a cryptocurrency which in addition to storing the transfer of assets, in the case of Bitcoin, also allows contracts to be stored and run on the network, known as smart contracts.

Ethereum was created in 2013 by Vitalik Buterin, and was deployed on 30 July 2015, as is currently the second most valuable cryptocurrency.

Ethereum collects batches all data into blocks, like Bitcoin's implementation of the blockchain, however the block generation time is reduced from 10 minutes to an average of 15 seconds. Another major difference in Ethereum implementation of the blockchain, is rather than store transactions the current "state" of accounts, contracts and storage are stored.

Again, as with Bitcoin, all nodes which participate in the network are required to store a complete blockchain, and this blockchain increases in size every 15 seconds.

Blockchain-based networks have not properly addressed the issue of scalability; this causes the original decentralized nature of the blockchain to become increasingly centralized, as only the highest-resourced users are able participate in the network.

This is because each node on the network is required to store the entire blockchain, which stores every transaction since its deployment and consequently low-resourced users; such as mobile users – are excluded from the network.

There has been several other peer-to-peer (P2P) and decentralized networks such as Bittorent which have face similar scalability issues, overcame some of these issues with the use of a Hybrid architecture model, combining both the client-server model and P2P architecture.

This paper looks at the current growth of Bitcoin and Ethereum, a predicts future network growth based on past history, conducting analysis on the resources this level of growth requires.

This is the first known time in literature such an analysis based on prehistoric data of both networks has occurred.

Using this data as a base we compare blockchain models, and examine how a temporal blockchain can reduce network resources following the collected and predicted data.

The paper is laid out in the following. First, we conduct a thorough review of literature on both networks, conducting analysis on predicted network growth based on historic, live data, and demonstrating the cost in resources if the networks was to follow previous observed growth rates.

We then compare these models, to the temporal blockchain, examining how, by removing the requirement to store all data on the blockchain can reduce the network resources and aid in growth, before concluding the research and recommending future work.

2 Previous research

The blockchain was first described in a self-published research paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" written under the pseudonym of Satoshi Nakamoto.

The blockchain is the underlying gossip protocol of all cryptocurrencies and is a novel peer-to-peer method of linking a sequence of transactions or events together in a way that makes them immutable [9]. McConaghy et al. accurately describe the main characteristics of the blockchain as decentralized control, immutability, and creation & movement of digital assets [8], and Pilkington credits the success of Bitcoin solely to the blockchain [10].

Drainville correctly describes how the blockchain is a collection of every transaction to have ever occurred on the Bitcoin network [2].

On creating a transaction, a user broadcasts this to all peers in the network. Kroll et al. expand on this by explaining how a select group of peers, called miners, collect broadcast transactions and attempt to gather them in a block that satisfies a cryptographic hash function [6]. The block must contain a cryptographic hash of the previous block; this is the method used to cryptographically link every block in the blockchain to its previous block, all the way back to the first or "genesis" block. Producing a block is both computationally intensive and probabilistic. Given a proposed block, each miner has a fixed and independent probability of successfully producing a block which satisfies the hash function for each unit of
computation time. Whilst it is difficult to produce a block, it is not difficult to verify a correct block.

Kroll et al. [6] explain that the mining process requires vast computing power as only a "brute force, trial and error" method can be used to calculate the SHA-256 hash. Every two weeks, the complexity of the challenge is adjusted to ensure that, on average, a block is mined every 10 minutes. The financial incentive of 25 bitcoins (USD 14,419.50 [1]) is offered to the first miner to successfully calculate the hash. Barber et al. [2] argue that it is this financial reward that ensures the majority of the miners on the network act honestly and obey the network protocol.

Poon and Dryja summarize the scalability problem facing all blockchain-based networks as not being a single problem, but rather the combination of multiple issues that ultimately affect the possible scalability of the blockchain [11].

Poon and Dryja [11] reinforce their scalability argument by demonstrating how the maximum theoretical number of transactions per second that Bitcoin's blockchain is able to process is 7, whereas VISA can process 20,000. McConaghy et al. [8] agree with Poon and Dryja and demonstrate that the Bitcoin's blockchain is currently 50GB – having grown by 24GB in 2015 – and also prove that in order to achieve the transaction rate of VISA by only increasing the block size, the blockchain would need to grow by 3.9 GB/day or 1.42 TB/year.

Overall, the blockchain is the most important invention of the original Bitcoin whitepaper.

While it has seen impressive growth and now handles an average of 239,138 transactions per day [1], it is not a faultless system. Having been shown to be vulnerable to attacks, such as the 51% attack, and faced with scalability issues which impact on the potential growth, there is plenty of room for further research to solve these issues.
Poon and Dryja [6] describe the Blockchain Scalability Problem as not being a single problem, but rather the combination of multiple issues that ultimately affect the possible scalability of the blockchain.

On average, VISA handles around 2,000 transactions per second (tps), with a recorded daily peak rate of 4,000 tps. It has a peak capacity of around 56,000 transactions per second [13]. By comparison, the maximum number of transactions per second that Bitcoin can currently theoretically achieve with the 1MB block size limit is 7 [4]. Poon and Dryja [6] describe how, whilst it is possible to achieve the tps VISA is capable of on Bitcoin, this would result in 8GB blocks, and a blockchain that would increase in size by over 400 terabytes a year.

Ethereum has been described by Buterin as the first Turing-complete blockchain based network, which allows for any computation to be run on all nodes, if an algorithm can be created for it.

While the first use case of blockchain was used for payment transactions as shown in Bitcoin, Ethereum use of the blockchain is designed to allow the development and deployment of truly distributed applications.

The smart contracts that can be run on the Ethereum network is writing in a programming language, Solidity based on JavaScript. This language is then converted to Ethereum Virtual Machine bytecode using the Solidity complier, and it is this bytecode which is stored in the blockchain.

Due to the decentralized nature of blockchain networks, and Ethereum, each node in the network must run computations stored on the blockchain. However, all nodes (a Turing machine) has one problem: the halting problem.
The halting problem can be described as the problem of determining from an input and description of a program if the program will complete or run forever. This problem still exists today, with the only reliable method for knowing if a program will run forever is to run the code.

If a program was allowed to run without being stopped, all nodes on the network would get caught up in an infinite loop (since all nodes are computation all transactions on the blockchain at the same time).

Nodes do not know how long each contract will run for before being executed is a potential security risk, as it would be possible to generate a contract which never ends, thus potentially conducting a DOS (denial-of-service) attack.

X details the growth of Ethereum over a period of 6 months, demonstrating how the network has increased from 300,000 to 875,000 transactions per day and compares this to the limited number of Bitcoin transaction per day at 400,000. Buterin theorizes the increase in the transactions is down to the increase use of the network for smart contracts, since each contract is treated as transaction.

Since all data, such as balances are being stored, the increase in users, as well as the increase in transactions causes the blockchain to grow. The blockchain grows (in Ethereum) every 10 – 12 seconds.

One method developers are talking about is increasing the number of transactions that can be stored in a single block, an increase on this hard-coded limit would allow for more transactions to be conducted, but with this approach, the scalability of the network suffers, as the resources required (bandwidth, storage, CPU) will mean only industries will be able to participate, centralizing a decentralized network.

In other words, decentralization and scalability are currently at odds, and is a current open research question on how to solve this.

A solution has been suggested - Sharding draws its inspiration from the scaling technique called “database sharding”. This is a popular mechanism for enabling scalability of databases, which breaks a single database into multiple pieces and spread across multiple servers. This now reduces the load on each server, as they are no longer required to store the whole database, instead just a portion of it.

The aim of the sharding protocol is to no longer require a single node to store the full state of the network and every transaction that occurs, instead just storing a subset of this data.

With this model, each node would be responsible for a particular subset of the blockchain, and would only respond to transactions which effect the data the node has. If a node needs to know about transactions or blocks that it doesn’t store, then it finds another node with the information it needs.

However, this model is not trust less, as now a node and user must rely on other nodes in order to confirm a transaction and could be an easy mechanism for an adversary to prevent a user from confirming a transaction or by lying a transaction took place or never happened.

3 Our research

We attempted to run full nodes on Both networks, using various clients. First, we measured the download time to obtain the full blockchain.

All nodes were the same specification VPS, with the same resources in terms of bandwidth, CPU, Ram, and none of the VPS's suffered any downtime during the experiments.

3.1 Blockchain download

We first conducted analysis of the download time for each blockchain. We observed as of the 29th November 2017, the full Ethereum blockchain size is 385GB, and on the same day, the Bitcoin blockchain was 139 GB. These figures are for the “full” blockchain, without any reduction in size mechanisms applied to them.

The almost triple in size of Ethereum’s blockchain compared to Bitcoin’s was a surprise, as Ethereum was first deployed on July 30th 2015, compared to Bitcoin being deployed on the 31st October 2008, which shows despite the nearly 7 years of growth on the blockchain, the uptake on Ethereum has been greater, and the use of smart contracts and coding on the blockchain has meant far larger transactions being added to the blockchain, this combined with no block size limits compared to Bitcoin has allowed the blockchain of Ethereum to swell in size to 385 GB

Using a modified Parity Ethereum client, we conducted analysis to examine how various blockchain size reduction methods have impacted on the size of the blockchain a user needs to download. It should be noted that the pruning function of the client requires first to download all the data and then conduct the relevant deletion of data.

Apart from the light client, which only downloaded the headers, all other models would have downloaded the entire blockchain and then conducted deletion.

The table below shows various configurations using Parity on downloading both the blockchain and state chain of Ethereum. The top 6 entries in this table are considered full nodes on Ethereum.

For a node to be considered a full node it must satisfy the following

- Has a full blockchain since the genesis block
- Able to confirm and replay all transactions and execute all contracts
- Able to compute the state for each block
- All historical data to be stored locally
- Most recent states to be stored locally

A full node in summary is able to fully participate in the network, the mining process and the confirmation of new transactions without requiring any data from external sources such as other nodes. These are the same requirements a Bitcoin full node must meet as well.

Table 1. Table showing the blockchain size and various configurations used

3.1 Pruning mode	**Database Config**	**Block verification**	**Available blocks**	**Available states**	**Blockchain size**	**Parity flags**
Archive	+Fat +Trace	Full	All	All	385 GB	pruning archive --tracing on --fat-db on
Archive	+Trace	Full	All	All	334 GB	prun-

						ing archive --tracing on
Archive		Full	All	All	326 GB	pruning archive
Fast	+Fat +Trace	Full	All	Recent	37 GB	tracing on --fat-db on
Fast	+Trace	Full	All	Recent	34 GB	tracing on
Fast		Full	All	Recent	26 GB	no-warp
Fast	+Warp	Ancient – PoW only	All	Recent	25 GB	
Fast	+Warp -Ancient	No-Ancient	Recent	Recent	5.3 GB	no-ancient-blocks
Light		Headers-only	None	None	0.005 GB	light

This table shows the full blockchain size of 385 GB. Ethereum was designed to be a P2P (peer-to-peer) network, which was decentralized application with no need for any centralized components.

Due to the lower guarantees offered by non-full nodes, to download the blockchain a home user would need to contribute over a month of continuous up time, nearly 400gb of hard drive capacity and also 525 GB of bandwidth on a 10MB connection. This is realistically out the reach of most home users without dedicated equipment.

To compare the results, four additional Ethereum clients was modified and attempted to download the blockchain using different options for reducing blockchain size. As can been seen in table 2 none of the clients was able to download a complete blockchain within two weeks.

The hardware used for this was a dedicated VPS (Virtual private server) of specification: 100MB internet connection, 100% up time, quad core CPU and 16GB of RAM. All experiments were started at the same time and once again was repeated 6 times over the period of 6 months. This specification was chosen as this mimic a high end, commercially available personal computer.

This experiment was different to the first experiment as we set a limited period of 14 days in order to download the blockchain, whereas the first experiment had no such limits.

Table 2 shows, no client was able to download the full blockchain within the timeframe.

Table 2. Table showing different clients and time taken to download the full blockchain

Client	Mode	Blockchain size	Able to complete within timeframe
Geth			
	Light	0.175 GB	Yes
	Fast	20.367 GB	Yes
	Full	N/A	No
EthereumJ			
	Pruning enables	13.299 GB	Yes
	Pruning disabled	N/A	No
Eth (No pruning available)			
	Default	N/A	No
PyEthApp (No pruning available)			
	Default	N/A	No

This experiment was aimed to model the average home user wishing to participate in the network, and the results show it is not possible to download a full copy of the blockchain within 14 days, with 100% uptime.

This is forcing anyone wishing to contribute to the Ethereum network to use commercial hardware, thus centralizing the network further, in addition it is unlikely any new nodes joining the network will be true full nodes, with complete blockchain and state history. This is leading to a network that is self-trusting, and even with current limitations in the number of transactions that can be incorporated into a block, the true blockchain size will continue to grow. This could then be leveraged and abused in the system by a malicious adversary.

We then examined the blockchain data retrieved from Ethereum network. To do this we developed a unique application which parsed the retrieved blockchain to allow us to extract more data from it. We were able to determine on the 19th December 2017, the Ethereum network completed the most transactions in a single day: 1,092,234.

In table X, we have shown the average transaction conducted on the Ethereum network per day for a set month. We then compare these results for the average number of transactions per day of the previous month and calculate the average change, in addition we also calculate the total growth rate on average TX per day since we first started analyzing the data from September 2015 to December 2017.

Table 3. Table showing parsed data from the blockchain – average number of TX per day.

Yea	Month	Average TX per day	Growth change compared to previous month	Total transaction growth since September 2015	Average transactions conducted over the past year	Percentage increase year on year
2015	September	5793.5				
2015	October	6614.354839	14.17%	14.17%		
2015	November	7824.433333	18.29%	35.06%		
2015	December	11196.51613	43.10%	93.26%		
2016	January	13219.4333	18.07%	128.18%		
2016	February	17932.41379	35.65%	209.53%		
2016	March	29586.09677	64.99%	410.68%		
2016	April	34103.2	15.27%	488.65%		
2016	May	43444.967	27.39%	649.89%		
2016	June	45051.2	3.70%	677.62%		
2016	July	43771.19	-2.84%	655.52%		
2016	August	45346.54839	3.60%	682.71%		
2016	September	46247.06667	1.99%	698.26%		
2016	October	42898.29032	-7.24%	640.46%		
2016	November	43386.2	1.14%	648.88%		
2016	December	42455.8371	-2.14%	632.82%	13609707.83	
2017	January	45473.03226	7.11%	684.90%		
2017	February	50358.85714	10.74%	769.23%		
2017	March	78273.25806	55.43%	1251.05%		

2017	April	84665.53333	8.17%	1361.39%		
2017	May	136952.129	61.76%	2263.89%		
2017	June	241488.5667	76.33%	4068.27%		
2017	July	252770.1613	4.67%	4263.00%		
2017	August	339457.3548	34.29%	5759.28%		
2017	September	355974.7333	4.87%	6044.38%		
2017	October	406518.1613	14.20%	6916.80%		
2017	November	509742.3	25.39%	8698.52%		
2017	December	876495.5714	71.95%	15028.95%	102752660.5	655.00%

Analysis of table 3 shows some surprising trends, over 28 months, there was only three months in which the average number of transactions per day in a set month did not increase on the previous month. In addition, some months the number of transactions per day increased between 50 – 70%.

The data contained within the blockchain leaves little data on the transactions, for example what they were for. However, by examining recent ICO (Initial coin offerings), with nearly 98% of these using the Ethereum network and the ERC20 token standard, the increasing number of transactions directly correlate to the launch of other cryptocurrencies which are based on Ethereum.

The network has been shown an increase of over 650% from 2016 to 2017. This shows the growth of the network has not stopped, with 7.6 times increase in the average daily transactions year on year.

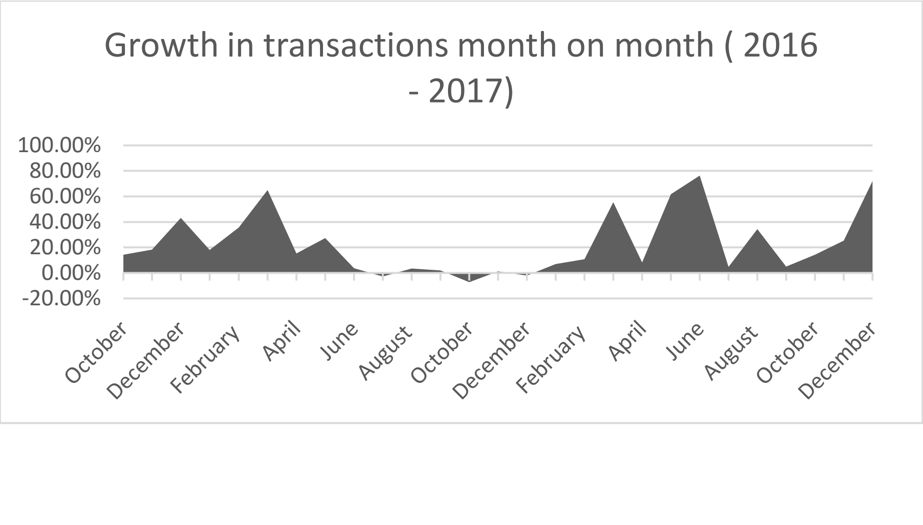

Fig. 1. A graph showing the growth on the number of transactions (month on month) on the Ethereum network over a period of 2 years.

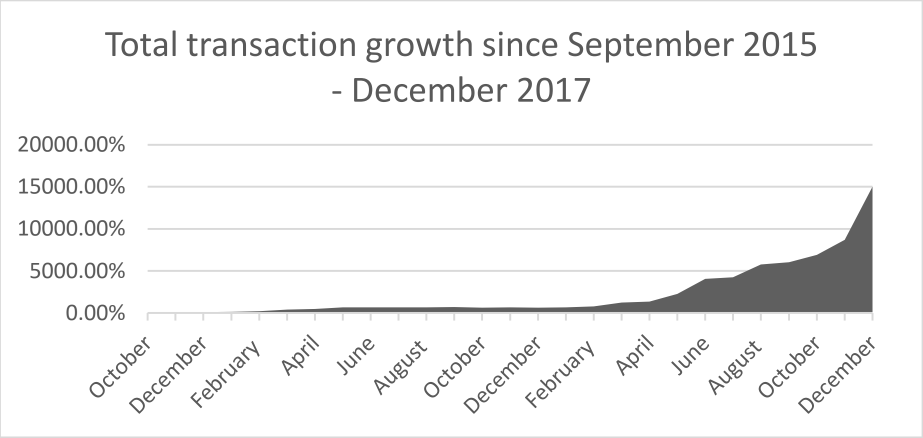

Fig. 2. A graph showing the grow in the number of transactions (daily) on the Ethereum network over a period of two years.

Graph 1 demonstrate the increase in transaction month on month between 2016 and 2017, while graph 2 shows the dramatic increase in the average number of transactions per day from September 2015 to current day. With a nearly 16000 % increase in transactions per day in December 2017 compared to an average day in September 2015.

Bitcoin

These experiments were then conducted on the Bitcoin blockchain. The current blockchain size of Bitcoin is 139GB. Only one major client was available, and using the same process as used in the Ethereum test, a download of a full Bitcoin Blockchain took on average 6.5 days.

Table 4. Table showing the parsed data from the Bitcoin blockchain – average number of TX per day

Year	**Month**	**Average TX per Day (Bitcoin)**	**Network growth month on month**
2016	January	187618.9091	
	February	213899.5862	14.01%
	March	184915.8621	-13.55%
	April	210071.852	13.60%
	May	212645.1953	1.22%
	June	224069.1407	5.37%

	July	216841.5255	-3.23%
	August	217291.97	0.21%
	September	211396.2072	-2.71%
	October	236498.2978	11.87%
	November	258377.0366	9.25%
	December	265397.6858	2.72%
2017	January	252937.8909	-4.69%
	February	281949.9418	11.47%
	March	277315.4918	-1.64%
	April	271617.3624	-2.05%
	May	300098.6282	10.49%
	June	260655.1755	-13.14%
	July	213865.6226	-17.95%
	August	258481.7011	20.86%
	September	219804.763	-14.96%
	October	271232.3764	23.40%
	November	307990.7499	13.55%
	December	322040.6784	4.56%

With the downloaded blockchain we were able to parse the data contained as shown in table X, the network, while growing has kept a steady number of transactions per day over the course of the year.

The reason we may be saying a more constant number of transactions per day, and not the rapid growth as found in Ethereum, that despite Bitcoin being the larger currency, the transactions tend to be smaller due to the lack of code for a smart contract, and also there is a hard-coded limit of 1MB per block, which gives a theoretical limit of 7TPS.

A comparison has been conducted between the average number of transactions per day between both networks from 2016 to the start of 2018. In graph 3 it is clear to see the number of transactions per day for Bitcoin is very stable, and has not increased over the observed two-year period, however Ethereum is a different case, a 16000 % increase in transactions per day. This growth looks set to continue, and while the hard-coded limit on Bitcoin blocks is certainly harming the growth of the network compared to the younger but un restricted Ethereum blockchain.

The theory the hard-coded block size is harming network growth can be confirmed by graph X. This shows data from the downloaded blockchain, which shows for near a six-month period from 1/6/2017 the majority of the blocks was over 90% capacity.

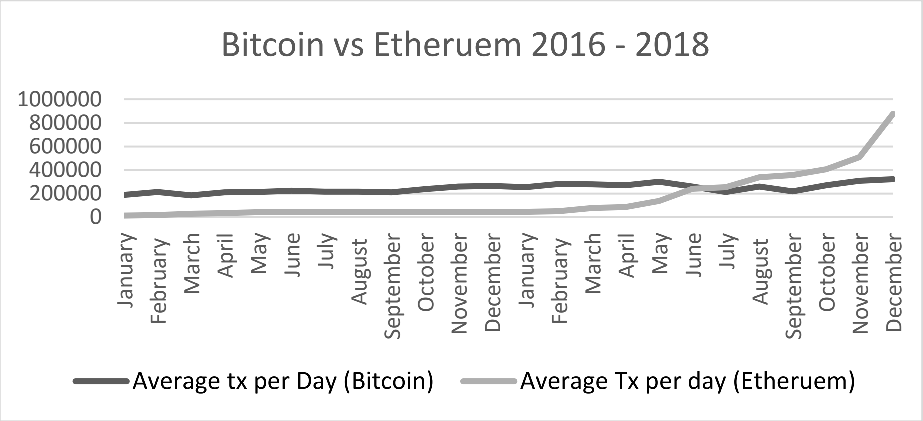

Fig. 3. A graph comparing the number of transactions per day (average) on the Ethereum and Bitcoin network over a period of two years

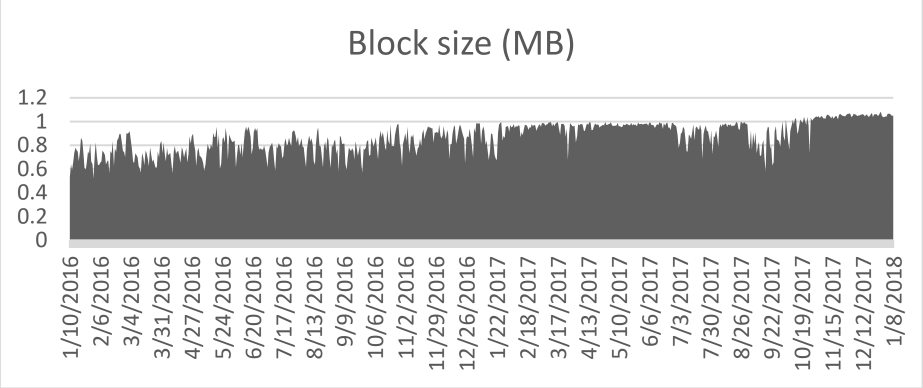

Fig. 4. A graph showing the average size of blocks on the Bitcoin network.

4 Predicting the future

Predicted growth on the Bitcoin blockchain is relatively easy to model. The assumption the hardcoded 1MB limit of blocks is enforced is likely to hold true the blockchain would grow at a rate of 62GB.

However, this growth in the Bitcoin blockchain is artificial of the networks true capacity. As show in graph X, the majority of the blocks over the past 6 months has been at capacity, this shows there is a need for network growth, and the current solution to reduce resources on the network and users by capping and limiting the growth of the blockchain is also limiting the growth and adoption of the network.

Ethereum

Ethereum limitless transactions per block, and almost month on month growth however makes an interesting look at what potentially the future could hold for the network should the historic data be repeated.

Using existing data on the number of transactions per month to occur on the Ethereum network, if the current trend from 2015-2017 was to carry on, we would see 500% increase in transactions month on month in 2021 as adoption of the Ethereum network continued to grow and more applications was built on top of this technology.

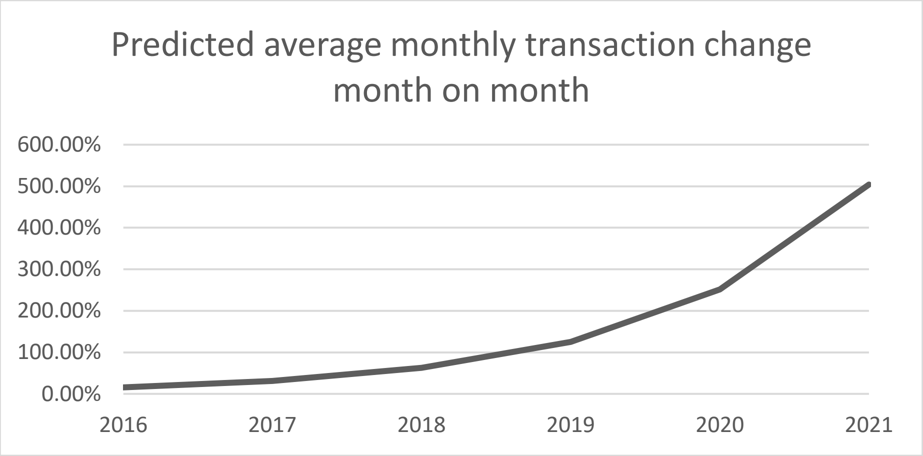

Fig. 5. A graph showing the increase in the number on transaction, month on month on the Ethereum network.

This rapid growth as have been observed from 2015 – 2017 and predicted growth to 2021, shows why scalability of a blockchain based network is so important. Should these growth trends continue (we are making the assumption the limit on number of transactions is removed in order for the network to be used and not backlogged) the blockchain size would increase at a rate of 4.09 TB every 12 seconds in 2021.

Table 5. Table showing predicted TX growth on the Ethereum blockchain

Year	Predicted average monthly transaction change month on month	Predicted Transactions per month average	Predicted Transactions per year
2016	15.59%	1148901.632	13786819.59
2017	31.24%	11993741.78	143924901.4
2018	62.61%	2628382808	31540593694
2019	125.49%	3.15085E+13	3.78102E+14
2020	251.49%	8.71607E+19	1.04593E+21

2021	504.03%	1.76281E+29	2.11537E+30

The mean transaction size over a period of two months (01.06.2017 – 01.08.2017) was 508 bytes. This was calculated by dividing the size of each block by the number of transactions occurred in the block.

This transaction size could increase if the complexity of smart contracts increased, but we are assuming for calculations this is the current average size of an average transaction.

Following the past growth patterns for the Ethereum network, if this was carried forward and repeated, the blockchain would swell 1.074608e+21 TB in 2021.

This obviously cannot be realistically achieved, which shows that growth patterns which was observed during 2016 and 2017 cannot carry on.

By using this limited history of the growth of the network we have come up with the above figures, however, since these are not realistic, and no more historic data is available to us in order to better predict the growth of the network, we cannot accurately model the growth on the network.

This does however show the current network growth cannot carry on and scalability solutions are required to be found.

Taking a conservative view, on network growth, with a 15% increase month on month (as seen in 2016) is possible and likely.

Table 6. Table showing increased in TX based on a 15% month on month increase.

Year	Predicted average monthly transaction change month on month	Predicted Transactions per month average	Predicted Transactions per year
2016	15.59%	1148901.632	13786819.59
2017	31.24%	11993741.78	143924901.4
2018	15%	73082019.91	889164575.6
2019	15%	391007084.8	4757252865
2020	15%	2091985696	25452492640
2021	15%	11192646693	1.36177E+11

Even with this conservative estimate of 15% increasing month on month, in 2021, the network would be adding 4,318 transactions per second to the blockchain which with current infrastructure is not possible.

The reason for the rapid growth in the Ethereum blockchain, as unlike Bitcoin, there are no hardcoded limits on block size. This lack of limit has allowed the network to grow to the current size, but cannot carry on, as have been shown in the earlier section of this paper, the average home user is now unable to participate Ethereum by running a full node.

5 Solution - The temporal blockchain.

The constant growth of the networks shows storing historic, and potential irreverent data is not possible in the long term, due to ever increasing resources, and network growth out pacing Moore's law.

One solution is the temporal blockchain. This is a blockchain based network, which has a finite blockchain size. The size of the blockchain is the number of blocks required to be stored by the network.

This network has been shown to be no more vulnerable to attacks than Bitcoin, with the 51% attack being the most likely attack against the network.

However, by requiring only the past 30 days (a use case in reputation data) to be stored, this can dramatically reduce the amount of resources (storage space + bandwidth used to join the network). This would be a far more scalable option than current generation Bitcoin blockchain, as shown in graph 6.

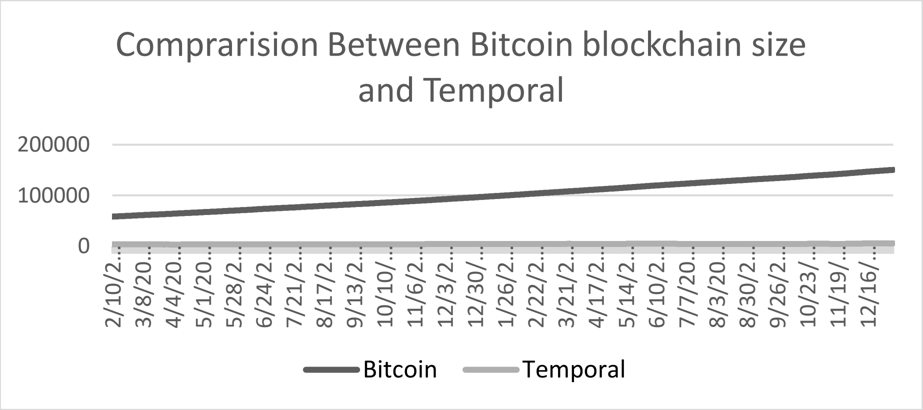

Fig. 6 A compassion showing the blockchain size using the current bitcoin implementation vs the size if Bitcoin was implemented on the temporal blockchain.

The temporal blockchain would require on average 6.4% of the resources compared to the Bitcoin blockchain.

However even with this significant 93.6% reduction in resources, it is clear the current networks are not realistically able to scale at the same rate as have been observed over the past two years.

The sheer amount of data required to be stored and processed and the resources required to do this task are unrealistic. It shows the current concept of being able to create and deploy any application upon the Ethereum blockchain for example cannot continue. Instead it is more realistic to expect a single application run on its own bespoke blockchain, to reduce the resources required, however here also becomes an issue. The security of blockchain is in the miners. These provide the hashing power on a network to prevent double spend attacks, however with many different blockchains, a miner would have to decide which blockchain to support

6 Conclusion

This research has shown Bitcoin's blockchain while is growing at a constant rate, is artificial, and is limiting the potential growth of Bitcoin. With 95% of blocks being at capacity, it is clear the limiting of block size is not a method which can be used to help the scalability of the network. In addition, it is clear for the Ethereum model, of limitless transactions per second, while clearly aids in the adoption of the network, it cannot scale.

A comparison against the temporal blockchain has been made and have shown a 96% reduction in blockchain size, whilst also maintaining the growth in number of transactions per day.

7 Future work

This work has shown blockchain has serious scalability limitation and some networks have already reached the limits of their growth. A proposed solution of the temporal blockchain has been discussed here and follows on from previous work on the temporal blockchain, but a further analysis of how the temporal blockchain can handle the large predicted number of transactions is required and would be beneficial for the community.

References

1. CoinDesk, http://www.coindesk.com/data/bitcoin-daily-transactions/
2. Drainville, D.: An Analysis of the Bitcoin Electronic Cash System, https://uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/drainville_danielle.pdf
3. Dumas, J., Sygnet, P., Xuereb, V.: Bitcoin a Peer-to-Peer Payment Solution, https://www.semanticscholar.org/paper/Bitcoin-a-Peer-to-peer-Payment-Solution-security-Dumas-Joseph/7a1e2a9e0fa3b9e64d09c0587ce302dfe7a32ee3/pdf
4. Hashing It. (2014). 7 Transactions Per Second? Really?[Online]. Available: http://hashingit.com/analysis/33-7-transactions-per-second
5. I. Eyal, A. Gencer, E. Sirer and R. van Renesse. (2015). Bitcoin-NG: A Scalable Blockchain Protocol[Online]. Available: http://arxiv.org/abs/1510.02037
6. J. Poon and T. Dryja. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [Online]. Available: https://lightning.network/lightning-network-paper.pdf
7. Kroll, J., Davey, I., Felten, E.: The Economics of Bitcoin Mining or Bitcoin in the Presence of Adversaries, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.364.5595&rep=rep1&type=pdf
8. McConaghy, T., Marques, R., Müller, A., De Jonghe, D., McConaghy, T., McMullen, G., Henderson, R., Bellemare, S., Granzotto, A.: Bigchain DB: A Scalable Blockchain Database, https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf
9. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

10. Pilkington, M.: Blockchain Technology: Principles and Applications, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660
11. Poon, J., Dryja, T.: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, https://lightning.network/lightning-network-paper.pdf
12. Sompolinsky, Y., Zohar, A.: Secure High-Rate Transaction Processing in Bitcoin, http://fc15.ifca.ai/preproceedings/paper_30.pdf
13. Visa. (2015). Visa Inc. at a Glance [Online]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf