Untangling Blockchain: A Data Processing View of Blockchain Systems

[1]Prerna Siddharth Ingle, [2]Prof V. A. Losarwar

[1]M. E. Student, [2]Associate Professor
Department of Computer Science & Engineering,
PES College of Engineering Aurangabad

***Abstract*: This Blockchain technology is gaining popularity in recent years. Blockchain is an accounting system that helps parties that do not trust each other to maintain a set of states around the world. The parties coincided with the existence, values and history of the state. Because technology is expanding rapidly, it is important and challenging to fully understand what central technology offers, especially about data processing capabilities. In this article, we will first explore the state of the art by focusing on the private chain. We analyze production and research systems in four dimensions: accounting, distribution, encryption, protocol, consensus and smart contracts [1].Then we will present BLOCKBENCH, a comparison framework to understand the effectiveness of private blogs and data processing workloads. We carry out a comprehensive evaluation of the three main blockchain systems using BLOCKBENCH, including Ethereum, Parity and Hyperledger Fabric. The results show many exchanges in the design area, including a large gap between the blockchain system and the system. Database based on the design principles of the database system, we will analyze several research approaches to increase the efficiency of the block chain as close as possible to the scope of the database.**

***Index Terms*: Component, formatting, style, styling, insert.**

I. INTRODUCTION (HEADING 1)

All manuscripts must be in English. Hatching with Bitcoin is a challenge. Liberation from the Great Recession cryptocurrency has been dubbed by the first representative as an outlet for the inequality and corruption of traditional financial systems. They adhere to the belief that when This parallel currency is brought out, it will compete and finally triggering the unofficial poem of Bitcoin "in coding, we are convinced". Bring new: merchant banking, third-party mediator to "trust" is not reliable[1]. These humans enter the path of other humans by cutting profits and complex transactions.

Bitcoin tries to replace the services provided by these intermediaries with encryption and code. When you use a check to pay for your mortgage, there are many agreements that occur in the background between your financial institution and others, allowing you to transfer money from your account to other people. Your bank can guarantee that your money is good because it saves where your money comes from and when. Blockchain is a record of each block instruction. There are many transactions. In the database context, the blockchain can be viewed as a solution to distributed transaction management: nodes store simulation data and agree on the order of transactions. Distributed transaction processing systems often deal with concurrency control through 2-phase assignments. However, to withstand the Byzantine behavior, the overhead of concurrency control will increase in the block chain.

Blockchain has many applications in business such as securities trading and payments, asset management and finance, banking and insurance. Currently, these applications are managed by systems created on MySQL and Oracle and by trustworthy companies / individuals, both lawyers / clerks / etc. Blockchain can block the status quo due to reduced infrastructure and costs. Human The inability to change, transparency and Blockchain's natural security reduces human error / malice and the need for self-intervention due to conflicting information. The paper said: "Goldman Sachs is a savings of about 6 billion in current capital markets and JP. Morgan estimates that power plants will begin to change their current infrastructure by 2020."

Peer-to-Peer electronic cash will allow online payments directly from one party to the other without having to go through a financial institution. Digital signatures are part of the solution. But the main benefits will be lost if reliable third parties still want to prevent redundant spending. We propose a solution to the problem of redundant spending using a peer-to-peer network. Network transactions record time by compressing those data in the hash-proof chain continuously by creating a record that cannot be changed without having to repeat the test again. The longest chain not only But acted as a sequence of events that saw But prove that it comes from the largest power source of the CPU. As long as most CPU power is controlled by nodes that do not cooperate in network attacks, they will create the longest network. The network itself requires minimal structure. The message is conveyed on the basis of the best effort and the node can leave the position and join the network as needed by accepting the chain with the longest proof to prove what happened while they disappeared[2].

Public block chain as compared to private block chain

In a public chain block, any node can join / exit the system. Therefore, the blockchain is completely decentralized, similar to peer-to-peer systems in chain blocks[3].Private blockchain enforces strict membership through access control and certification.

Bitcoin uses work evidence (PoW) for consensus: only successful diggers to solve difficult puzzles (Improper search that is appropriate for the block header) can be integrated into the blockchain. It will add two blocks simultaneously by creating separate paths in the blockchain Bitcoin. Modifying by considering only the blocks that are confirmed after that, followed by a block number. Very PoW works well in public settings because it prevents Sybil's attacks. But since it is not configurable and has high computing

costs, it is not suitable for applications such as banking and finance, which must handle a large number of transactions in a given manner.

Because node identity is known in private settings, most blockchain uses a single protocol from many literature in consensus. Hyperledger v0.6.0 uses PBFT, which is Paxos that is resistant to Byzantine, while other chains Use normal Paxos (Hyperledger v1.0.0-rc1 using the No-Byzantine consensus protocol according to Kafka). However, despite the flexibility of PBFT resizing (or XFT), those Paxos protocols cannot be scaled to tens of thousands of hundreds[4].

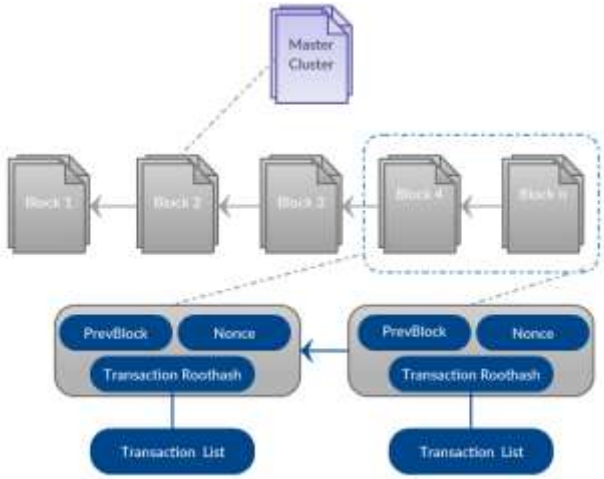

Figure 1.0 Block Chain Process

Distributed Ledger Architecture

Distributed ledger: In the block, the ledger accounts are replicated on all nodes as an annex-only data structure. The blockchain starts with some initial state and the ledger records the entire history of the update operations that occur with the state[5].

Encryption:

Used for checking the integrity of the ledger to ensure that there is no blockchain data editing. States around the world are protected by trees. The hash (Merkle) that Hagjog is kept in the block. Block history is also protected by linking blocks through the chain of cryptographic hash pointers: the content of the block number n + 1 has the hash of the block number n. In this way, any modifications in the block n will Cancel all subsequent blocks immediately[6].

Intelligent contract means a calculation that is performed when a transaction is made. At the end of the spectrum, Bitcoin nodes use a simple replica model which moves coins from one address to another. On the other hand, Ethereum smart contract can specify arbitrary calculations and come with their own virtual machines for running Ethereum bytecodes. Similarly, Hyperledger uses a Docker container to perform contracts written in any language. Many new business applications, but this makes software defects very important in attacking DAO. The attacker steals a property worth $ 50M to find a bug.

Bitcoin is a well-known example of public chain blogs in Bitcoin. The state is a digital coin. (cryptocurrencies) and transactions will move coins from one set to another Each node releases a set of transactions that need to be processed. A special node called miners collects transactions into their validation blocks and starts a consensus protocol to integrate the blocks into the Bitcoin block chain using work evidence (PoW) for consensus[7]. only the digger That succeeded in solving difficult puzzles (nonce searches that are appropriate for the block header) can be integrated into the blockchain. PoW is resistant to Byzantine's failure, but is likely to cause Possible: It is possible to append two blocks at the same time, create separate paths in the blockchain. Bitcoin corrects this by considering only those blogs that are confirmed after that, followed by a number of blocks.

Private Blockchain

Hyperledger [8] is one of the most popular personal block chain. Because the node's credentials are known in personal settings, most blogs use one protocol from many literature to vote consensus PBFT as Popular protocols currently in use Hyperledger uses PBFT1 directly, while others such as Parity ,Ripple and ErisDB develop their own parameters. PBFT is a three-phase protocol. During pre-preparation, leaders will publish values that must be delivered by other nodes. Next, in the preparation process, the node will convey the value that is about to be delivered. Finally, the confirmation process confirms the commitment value when more than two-thirds of the nodes agree in the previous phase. PBFT has limited communication but receives some safety and well-being in synchronous networks. part In addition to the established consensus, another important feature of private blocking is the support of intelligent contracts that can show very complex transactions. These qualities are especially needed in business and financial systems. Indeed, blocking the private sector caused this interest from large banks and financial institutions, some of whom even claimed that they had the potential to prevent data management practices [9].

Cryptography

A user in a blockchain is uniquely identified by her public key certificate. In public settings, the user first generates a key pair (the default option being ECDSA based on the Secp256k1 elliptic curve), then derives the identity as the hash of the public key. This hash serves as a transaction address or an account number in crypto-currencies systems. To claim ownership of the transaction output or of the account, the user signs transactions with the corresponding private key. In private settings, there is an additional access control

layer[10]. Hyperledger separates this layer from the blockchain, in the form of a membership provider service and a certificate authority service. The administrator can implement arbitrary policies with these services to control who gets access to the blockchain

II. LITERATURE SURVEY

Paper Name	Author	Algo	Dataset	Publications	advantage	Disadvantage	Features
Untangling block chain : A data Processing view of block chain system	Tion Tuon Anh oinh, Rui liu, Meihuizhang	Consensus Algo. Cryptographic (pow)	Database - Oracle (my SQL) Distributed database	IEEE	1. Improve security 2. Easter Transaction 3. Customers can receive variation in hours or min 4. elimination of duplicate data	1. Complexity 2.Easter Transaction 3. Customers can receive variation in hours or min 4. elimination of duplication data	1. Transparency 2. Low Cost 3. Decentralize system
Application of block chain in health care : current landscape & challenges	Gajendra J. Katuwal, Sandip Panday, Mark Hennessey & Bhishal Lamichhane	SHA-256 (se.hash Algo) cryptographic hash Algo	Decentralize dataset / distributed dataset.	International conference IJBRT / IIPS IEEEE	1. Process integrity 2. Traceability Problem 3. Security 4. Faster Processing	1. Process integrity 2. Traceability Problem 3. Security 4. Faster Processing	1. Supply chain mgmt. 2. Control over information 3. Better collaboration
Block chin Application in the biomedical domain : a scope in review	George Drosatos, Eleni Kardoudi	Cryptographic algo. (consensus algo) pow (hash chain)	Medical evidence database	1. Springer link 2. Science direct	1. Decentralize mgmt 2. Robustness 3. Security & Privacy	If integration with the existing system	1. Data Provenance 2. Reduce the attach 3. Trusted Transformation Scheme
Application of block chain technology beyond crypto currency	Mahdi H. Miroz Maoxuf Ali	Pow (Cry.Alg) validation & very process	Distributed dataset (digital ledger)	IEEE	1. Secure 2. Telaintain privacy 3. Decentralize mgmt	1. Power use 2. Low cost	1. Increased capacity 2. Better security 3. Efficiency
Current research on block chain technology as systematic Review	Jasse Yli-Huumo, Deokyoon ko, sujin choi, sooyong pork, kaxi smolander	consensus Algo (PBFT)	Distributed dataset	Open access journal conference / workshop journal	1. Faster Security 2. Process Integrity 3. Traceability	Uncertain reg. status power use cost	1. Better Collaboration 2. Scalability
An Overview of block chain technology : architecture, consensus & future Trends	Zibin zheng shaoon xie, Hong-hing Dai	Consensus Algo (PBFT)	Distributed dataset	Conference paper (IEEE)	1. Efficiency 2. Zero / Fraud 3. Safety	1. Storage 2. Diff. in updating	1. Regulations 2. Scalability 3. Reliable
Block chain internet of minds : a new opportunity for cyber-physical-social systems	Fei-yue wang yong yaun, Tun Zhang	Machine learning algo	Distributed dataset	IEEE	1. Easy Access to sense 2. Trustable	1. Complex System	1. Transparency 2. Better Security
Parallel block chain : An architecture for CPSS	Fei-yue Wang young yuan	1. Gredy Algo 2. Data mining Algo 3. Bayesian Algo	Distributed dataset	IEEE	1. Secured 2. Trusted Fashion 3. Reliable	1. CPSS is Complex system 2. Parallel explanation	1. Computational Experiments 2. Parallel block chain

Based smart societies							3. Block chain power smart societies in the near future

III. Table 1.0 Literature Survey Review

Before Blockchain systems use encryption techniques to ensure the integrity of the ledger. Integrity here refers to the ability to detect, modify, blockchain data. This feature is important in public settings that are not reliable in advance. For example, public confidence in encrypted digital currency, such as Bitcoin, which determines the value of that currency depends on the integrity of the ledger[11]. That is, the ledger must be able to detect spending twice. Even in a personal blog, integrity is equally important because the authenticated nodes can be dangerous. There are at least two levels of integrity protection. The first time the state around the world is protected by a hash tree (Merkle) whose hash roots are stored in the block. Any status changes will result in a new hash path. The leaves of the tree contain the internal node state, including the hash of the children. For example, Hyperledger v0.6 uses a hash map of the deposited state in which the status is grouped (by hashing) into the predefined number of tanks in turn. Ethereum used early, PatriciaMerkle Which is similar to the species and the leaves have a status as a key value Secondly, the blog history is protected, ie the blog will not change when it is integrated with the blockchain. The key technique is to link the block through the chain of cryptographic hash pointers: the contents of the block number n + 1. Contains the hash of the block number n. In this way, any modifications in the block n will cancel all blocks that follow immediately. With the Merkle tree pointer and blockchain hash, offering a safe and effective data model that tracks all historical changes that occur in states around the world. Blockchain's security model assumes the availability of public key encryption[12]. The identity, including the identity of the user and the transaction, is derived from the public key certificate. Secure key management is necessary for any block chain in other security systems. Losing a private key means losing access. But in blockchain applications such as crypto-currency Loss of keys has direct financial impact and irrevocable.

Bitcoin provides around 200 opcodes, but many are disabled in recent usage. Users can write stacked programs with the most popular Bitcoin contract opcodes associated with multiple signatures. One example is a contract that requires 2 in 3 signatures before issuing coins. The language can also use the contract for the bounty hunting scheme, such as one that publishes a medal. When found in advance of the hash value, BigchainDB [13] uses a language that has more meaning than it is called. crypto-condition Developed as part of the Interledger Protocol project [14]. Encryption conditions allow to specify complex boolean expressions through multiple types of signatures. The crypto-condition script There are conditions and practices which are considered script inputs and outputs. Conditions that include the timeout which will help the timer contract The encryption of Crypto conditions is higher than Bitcoin opcodes, making it easy to display complex logics.

EVM transactions also track intermediate and backward status changes if there is money. Not enough to pay for the operation. Hyperledger does not have his own bytecotes, but will run intelligent contracts that do not believe language in the Docker container. In any language, which will be compiled into native code and imager Docker packed into the contract are uploaded each node starts a new container with the image. Contract execution can be done through the Docker API. The contract can access the blockchain status in two ways: getState and putState. Revealed by the shim layer. One of the advantages of Hyperledger is that it supports many high-level programming languages such as Go and Java. With the blockchain require special logics applications for high-level data structure mapping into tuples. Key-values Sawtooth Lake supports intelligent contracts in the form of business. Natural Family Each family is a user-defined Python class loaded into the ledger during startup. The contract is executed in the original runtime environment as a regular Python program.

One of the results of Turing's complete contract support is the lack of pure software. But inevitably While empowering the genre, Ethereum's genius contract has been severely criticized. Security concerns have actually occurred in the DAO attack ,where the attacker has stolen property worth $ 50 million. The attack is finding flaws that occur simultaneously in the DAO smart contract, which will allow one to Repeatedly pulling more money than specified in the transaction Such errors exist in languages such as EVM that are weak or have no formal definition of their meaning. OYENTE presents three important reasons for security flaws: references, orders, transactions Reference timestamp and false exception It gives the official Ethereum semantics and offers tools for direct debugging on EVM bytes. The tool finds more than 8000 Ethereum contracts (worth more than $ 60M) with potential security flaws. As with other transactions on the blockchain, intelligent contract execution is transparent. It refers to the network input, output, and status of the Hawk contract. Zerocash expands to ensure the privacy of transactions for intelligent contracts. The main challenge compared to Zerocash is in arbitrary transaction logics, while Zerocash logics are limited by small operating sets. Another challenge is to protect the local state which is not available in Zerocash. Hawk promises to collect it with zkSNARK to maintain privacy. Input and output transactions are processed before and after Hawk to hide complex encoding details. Although protocols are costly in both time and space[15].

Even before DAO attacks, some bloggers have rejected models that allow unconditional calculations. Kadena, Tezos and Corda languages are more powerful than Bitcoin scripts, but they exchange Turing's perfection for security. The language of Kadena is a language that looks like a ripple called Pact. The Pact contract is stored in a separate account human-readable format that will Clients parsed and executed in Ocaml It is strongly typed and can be checked formally. In the same way, the Tezos stack language named Michelson comes with a strong system and complete definition. As a result, the Tezos contract can be monitored consistently for safety. In Corda, the contract is a sequence of pure functions that do not change status. Since the function is only a security limitation of the contract, it can be done as a regulation and can be checked.

Proof of Stake(POS)

The work test is a protocol whose main purpose is to deter cyberattacks, such as a distributed denial of service (DDoS) attack, which aims to exhaust the resources of a computer system by sending several false requests.
The concept of Proof of Work already existed before bitcoin, but Satoshi Nakamoto applied this technique to his / her, we still do not know who Nakamoto really is, digital currency is revolutionizing the way traditional transactions are established.
In fact, the idea of PoW was originally published by Cynthia Dwork and Moni Naor in 1993, but the term "proof of work" was coined by Markus Jakobsson and Ari Juels in a paper published in 1999.
But, to date, proof of work is perhaps the most important idea behind Nakamoto's Bitcoin document, published in 2008, because it allows for a confident and distributed consensus.
A trust and distributed consensus system means that if you want to send and / or receive money from someone who does not need to resort to third party services.you use traditional payment methods, you must rely on a third party to set up your transaction (for example, Visa, MasterCard, PayPal, banks). They keep their own private record that stores the transaction history and balances of each account.
The common example to better explain this behavior is the following: if Alice sent Bob $ 100, the trusted third party service would debit Alice's account and prove Bob's, so both of them have to trust that this third party will do the same. Right. .
With bitcoin and some other digital currencies, they all have a copy of the accounting book (blockchain), so no one has to trust third parties, because anyone can directly verify the written information.
Deepening, the work test is a requirement to define a costly computer calculation, also called mining, that must be done to create a new group of reliable transactions (the so-called block) in a distributed ledger called blockchain[16].

Mining has two purposes:

- To verify the legitimacy of a transaction, or avoid the so-called double expense;
- To create new digital currencies rewarding the miners for doing the previous task.
- Transactions are grouped into what we call a block;
- The miners verify that the transactions within each block are legitimate;
- To do so, the miners must solve a mathematical problem known as a work test problem;
- A reward is given to the first miner who solves each block problem;
- Verified transactions are stored in the public blockchain.

IV. PROPOSED SYSTEM

After To overcome scalability with PBFT, Ripple has used a method that divides the network into small groups called federates. Each federation uses local consensus protocols between members and then local agreements are propagated. Distributed to all networks through nodes located in the junction of the federation The security conditions of the Ripple are the most honest nodes in every federation and the intersection of any two states. There are at least one honest node. Ripple assumes that the federates are predetermined and their safety conditions can be enforced by the network administrator. In a distributed environment that does not recognize the identity of the node, such assumptions will not be stored. Byzcoin and Elastico offer a new two-phase protocol that includes PoW and PBFT. In the first phase, PoW will be used to establish the group. Byzcoin consensus is carried out with a window scrolling above the block chain and selecting the digger of the block within the Elastico window. Group nodes according to the identity that changes every age. In particular, node identity is a way to solve cryptographic puzzles[18].

Advantages of our system

• Hyperledger consistently works better than Ethereum and Parity in standard criteria. But it failed to expand up to 16 nodes
• Ethereum and Parity have more flexibility on node failures But there is a risk of security attacks using the blockchain
• The main bottleneck in Hyperledger and Ethereum is the corresponding protocol. But for parity, bottlenecks are caused by signing a transaction.
• Ethereum and Parity have a high cost in terms of memory and disk usage. Their execution engine is also less efficient than Hyperledger.
• Hyperledger's data model is low. But its flexibility allows it to be tailored appropriately for analytical queries

Distributed Ledger:

It is a system supporting distributed ledgers and is characterized by its target applications, by the number of ledgers, and by the ledger ownership.

Cryptography

Users in the blockchain are uniquely identified by her public key certificate. In public settings, the user creates a pair of keys for the first time. (The default option is ECDSA followed by the Secp256k1 oval curve.) Then get the identity information as a public key hash.
This hash serves as the transaction address or account number in the digital currency system. To claim ownership of the transaction results or of the user account, sign the transaction with the corresponding private key
In personal settings, there is an additional access control layer. Hyperledger separates this layer from the blockchain in the form of member providers and certification services.

Hyperledger will be checked against these services before proceeding by the next element (consensus). Multichain offers a simpler form with a certain number of world-class privileges, while the remaining systems provide small details. Of their protocols
Most blockchain is designed to protect the accuracy of the transaction. But does not consider the privacy of the transaction. The blockchain is said to have the privacy of the transaction when (1) the transaction cannot be linked from one place to another and (2) the content of the transaction is known only to entrants join In personal settings, transparency of transaction history may not be a problem [19].

Consensus

Blockchain systems use encryption techniques to ensure the integrity of the ledger. Integrity here refers to the ability to detect, modify, blockchain data. This feature is important in public settings that are not reliable in advance. For example, public confidence in encrypted digital currency, such as Bitcoin, which determines the value of that currency depends on the integrity of the ledger. That is, the ledger must be able to detect spending twice. Even in a personal blog, integrity is equally important because the authenticated nodes can be dangerous. There are at least two levels of integrity protection. The first time the state around the world is protected by a hash tree (Merkle) whose hash roots are stored in the block. Any status changes will result in a new hash path. The leaves of the tree contain the internal node state, including the hash of the children. For example, Hyperledger v0.6 uses a hash map of the deposited state in which the status is grouped (by hashing) into the predefined number of tanks in turn. Ethereum used early, PatriciaMerkle Which is similar to the species and the leaves have a status as a key value Secondly, the blog history is protected, ie the blog will not change when it is integrated with the blockchain. The key technique is to link the block through the chain of cryptographic hash pointers: the contents of the block number n + 1. Contains the hash of the block number n. In this way, any modifications in the block n will cancel all blocks that follow immediately. With the Merkle tree pointer and blockchain hash, offering a safe and effective data model that tracks all historical changes that occur in states around the world. Blockchain's security model assumes the availability of public key encryption. The identity, including the identity of the user and the transaction, is derived from the public key certificate. Secure key management is necessary for any block chain in other security systems. Losing a private key means losing access. But in blockchain applications such as crypto-currency Loss of keys has direct financial impact and irrevocable[20].

V. CONCLUSION

Blockchain has the potential to solve problems because it provides trust without having to have a middleman. Traceability is a starting feature and promises a new business model by using a new incentive structure. Because Blockchain's potential has gathered a lot of interest in the industry. In this article, we will examine the key use cases of the blockchain along with related projects. We found that most blockchain projects have limitations in the form of white documents, proof of concepts and products with a limited user base.

REFERENCES

[1] Tien Tuan Anh Dinh et. al, "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 30, NO. 7, JULY 2018
[2] Q. Lin, P. Chang, G. Chen, B. C. Ooi, K. Tan, and Z. Wang,"Towards a non-2PC transaction management in distributed database systems," in Proc. ACM Int. Conf. Manag. Data, 2016,pp. 1659–1674.
[3] A. Thomson, T. Diamond, S. Weng, K. Ren, P. Shao, and D. J.Abadi, "Calvin: Fast distributed transactions for partitioned database systems," in Proc. ACM Int. Conf. Manag. Data, 2012, pp. 1–12.
[4] P. Bailis, A. Fekete, M. J. Franklin, A. Ghodsi, J. M. Hellerstein,and I. Stoica, "Coordination avoidance in database systems," Proc.VLDB Endowment, vol. 8, no. 3, pp. 185–196, 2014.
[5] Ethereum blockchain app platform. (2017). [Online]. Available:https://www.ethereum.org/
[6] Ripple, "Ripple." (2017). [Online]. Available: https://ripple.com
[7] Melonport, "Blockchain software for asset management." (2017)[Online]. Available: http://melonport.com
[8] J. P. Morgan and O. Wyman, "Unlocking economic advantagewith blockchain. a guide for asset managers." 2016, http://www.oliverwyman.com/our xpertise/insights/2016/jul/unlockingeconomic-advantage-with-blockchain.html, Last accessed: 2017.
[9] G. S. Group, "Blockchain: Putting theory into practice,"2016, http://www.goldmansachs.com/our-thinking/pages/blockchain/, Last accessed: 2017.
[10] T. T. A. Dinh, J. Wang, G. Chen, L. Rui, K.-L. Tan, and B. C. Ooi,"BLOCKBENCH: A benchmarking framework for analyzing privateblockchains," in Proc. ACM SIGMOD Int. Conf. Manag. Data,2017, pp. 1085–1100.
[11] Ethcore, "Parity: Next generation ethereum browser." (2017).[Online]. Available: https://ethcore.io/parity.html
[12] Hyperledger, "Blockchain technologies for business." (2017).[Online]. Available: https://www.hyperledger.org
[13] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technicalsurvey on decentralized digital currencies," IEEE CommunSurv. Tutorials, vol. 18, no. 3, pp. 2084–2123, Jul.–Sep. 2016.
[14] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W.Felten, "SoK: Research perspectives and challenges for bitcoin andcrypto-currencies," in Proc. IEEE Symp. Security Privacy, 2015,pp. 104–121.
[15] M. Stonebraker, S. Madden, D. J. Abadi, S. Harizopoulos,N. Hachem, and P. Helland, "The end of an architectural era (it'stime for a complete rewrite)," in Proc. 33rd Int. Conf. Very LargeData Bases, 2007, pp. 1150–1160.
[16] J. C. Corbett, et al., "Spanner: Google's globally-distributed database,"in Proc. 10th USENIX Symp. Operating Syst. Des. Implementation,2012, pp. 261–264.
[17] M. Castro and B. Liskov, "Practical byzantine fault tolerance," inProc. 3rd USENIX Symp. Operating Syst. Des. Implementation, 1999,pp. 173–186.

[18] Q. H. Vu, M. Lupu, and B. C. Ooi, Peer-to-Peer Computing Principlesand Applications. Berlin, Germany: Springer-Verlag, 2009.
[19] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining isvulnerable," in Proc. 18th Int. Conf. Financial Cryptography DataSecurity, 2014, pp. 436–454.
[20] K. Croman, et al., "On scaling decentralized blockchains," in Proc.3rd Workshop Bitcoin Blockchain Res., 2016, pp. 106–125.