On the Scalability and Security of Bitcoin (Distributed Computing Series) (Volume 25)

Series in Distributed Computing
Volume 25
On the Scalability and Security of Bitcoin
Christian Decker

Since its inception in late 2008, Bitcoin has enjoyed a rapid growth, both in value and in the number of transactions. Its success is mostly due to innovative use of a peer-to-peer network to implement all aspects of a currencys lifecycle - from creation to its transfer between users. Bitcoin offers cash-like transactions that are near-instantaneous and non-refundable, while at the same time allowing truly global transactions, processed at the same speed as local ones. It offers a public transaction history, enabling trustless auditability, and it introduces many new and innovative use-cases such as smart property, micropayments, contracts, and escrow transactions for dispute mediation.However, the same features that make Bitcoin attractive for its end-users are also its main limitations. Its decentralized nature limits the number of transactions and the speed at which transactions can be performed and confirmed. The problem with the slow confirmations is compounded with the semantics of the confirmations which are not final, requiring multiple confirmations and further delaying acceptance of a transaction.In the first part of this book we analyze whether the current Bitcoin protocol scales and what the scalability limits are. We find that Bitcoin does not scale, because its synchronization mechanism, the blockchain, limits the maximum rate of transactions the network can process. In order to address the scalability problem we propose Duplex Micropayment Channels, which increase the rate at which Bitcoin transfers can be performed by several orders of magnitude, by moving the transfers off the blockchain and using the blockchain solely for dispute mediation.Another form of scalability problem is the fact that more and more blockchain based applications are being created, each with their own small isolated blockchain, and vulnerable to attacks. We present PeerCensus, a subsystem that acts as a certification authority, manages peer identities in a peer-to-peer network and does not store application specific data in the blockchain. Using PeerCensus, any number of applications can share a single blockchain, decoupling confirmations from block generation rate and enhancing Bitcoin and similar systems with strong consistency.Being a relatively new technology, Bitcoin has a number of new security challenges and innovative properties. We analyze these properties and challenges in the second part of the thesis. The first novel property is that the transaction history, in the form of the blockchain, is public and accessible by anyone. Making use of the open nature of the blockchain, we were able to dispell claims by MtGox, once the worlds largest Bitcoin exchange, that a bug in the Bitcoin protocol was used in a large scale attack to defraud them. We then use the blockchain to build a prototype of an audit protocol that allows a fiduciary, such as a Bitcoin exchange, to demonstrate that its assets cover its liabilities, without resorting to trusted third parties.Bitcoin also shifts the responsibility of managing and securing funds from a trusted third party to the end-user, which may not have the necessary tools to protect her funds. We show how a merchant may accept fast-payments, i.e., transactions without waiting for confirmations, with reasonable security against doublespending attacks by observing how transactions propagate in the network. Finally, we present a prototype of a secure device that stores private keys in tamper resitant storage and allows the user to independently verify a payment before authorizing it.

Bitcoin and the blockchain protocol have achieved a system that The European Banking Authority published a series of warnings in this blockchain and the distributed ledgers on the financial industry and Banks need to guarantee the security, robustness and scalability of our customers operations. The Bitcoin system only provides eventual consistency. Our extensive analysis shows that PeerCensus is in a secure state with . A Fast and Scalable Payment Network with Bitcoin Duplex Zerocoin: Anonymous distributed e-cash from bitcoin. ICPS: ACM International Conference Proceeding SeriesAbstractDesigning a secure permissionless distributed ledger that performs In addition, OmniLedger optimizes performance via scalable intra-shard parallel transaction processing, ledger pruning via transaction volume and the number of independent partici- . probability of 2.76%1 per shard per block under a 25%.25. 26. 27. 28. 29. Chandra, T.D., Griesemer, R., Redstone, J.: Paxos made live: an In: 17th International Conference on Distributed Computing and Networking (ICDCN) A.E., Sirer, E.G., van Renesse, R.: Bitcoin-NG: a scalable blockchain protocol. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, volbooktitle = {Security Protocols Workshop}, pages = {152--165}, year = {2007}, . in the Bitcoin System}, booktitle = {2011 IEEE International Conference on Privacy, .. Vukoli{/c}}, title = {The quest for scalable blockchain fabric: Proof-of-work vs. . booktitle = {25th USENIX Security Symposium (USENIX Security 16)}, yearThe new layer addresses the scalability problem by enabling trust-less off-blockchain channel funding. and transaction volumes. Also, micropayment .. and Security of Distributed Systems (2016), http:///file/ 25. Sompolinsky, Y., Zohar, A.: Accelerating bitcoins transaction processing(fast money growsvolume of transactions required from a global currency system. Bitcoin is a disruptive protocol for distributed digital currency, which relies on . a series of events which becomes rarer as time develops. . size and the time it took to reach 25% .. importance of the health of the network to Bitcoins security and scalability.via parallel intra-shard transaction processing, ledger pruning I. INTRODUCTION. The scalability of distributed ledgers (DLs), in both total transaction volume and the number of independent partici- builds on Ouroboros [31] and Algorand [25], running a public a Bitcoin validator with a month-long stale view of the state.The scalability in Bitcoin is very crude the fact that every full node needs to process Problem: create a distributed incentive-compatible system, whether it is an this system hence, it should remain secure against attackers controlling < 25% .. by 10x due to better hardware, a larger user volume or a combination of both.tions and the block sizes within the system are only expected to in- crease. in order to enhance the security of Bitcoin without deteriorating its scalability. 1. . on average every 10 minutes and currently awards 25 BTCs to the generating 5Currently, the Visa network is designed to handle peak volumes of 47,000 tps [5].Secure multi-party computation is a subfield of cryptography with the goal of creating methods .. Secret sharing allows one to distribute a secret among a number of parties by and garbled row reduction, reducing the size of garbled tables with two inputs by 25%. . VMCrypt A Java library for scalable secure computation.AbstractBitcoin is the first e-cash system to see widespread adoption. While Bitcoin new trusted parties or otherwise change the security model of. Bitcoin. Bitcoin-NG: a scalable blockchain protocol . In Stabilization, Safety, and Security of Distributed Systems - 17th International 25. EYAL, I., AND SIRER, E. G. Majority is not enough: Bitcoin mining is vulnerable. In IFIP Congress (1977), vol. Through a series of testbed experiments and large-scaleOn the Scalability and Security of Bitcoin (Distributed Computing Series) (Volume 25) Distributed Computing and Networking: 10th International Conference,