1. CCS 2017

1.1. Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin

Author: Yujin Kwon(Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea), Dohyun Kim, Yunmok Son, Eugene Vasserman(Kansas State University, Manhattan, KS, USA), Yongdae Kim

Abstract:

participants organize mining pools and split the rewards from the pool in proportion to each participant's contribution. However, several attacks threaten the ability to participate in pools. The block withholding (BWH) attack makes the pool reward system unfair by letting malicious participants receive unearned wages while only pretending to contribute work. When two pools launch BWH attacks against each other, they encounter the miner's dilemma: in a Nash equilibrium, the revenue of both pools is diminished. In another attack called selfish mining, an attacker can unfairly earn extra rewards by deliberately generating forks.

In this paper, we propose a novel attack called a fork after withholding (FAW) attack. FAW is not just another attack. The reward for an FAW attacker is always equal to or greater than that for a BWH attacker, and it is usable up to four times more often per pool than in BWH attack. When considering multiple pools — the current state of the Bitcoin network – the extra reward for an FAW attack is about 56% more than that for a BWH attack. Furthermore, when two pools execute FAW attacks on each other, the miner's dilemma may not hold: under certain circumstances, the larger pool can consistently win. More importantly, an FAW attack, while using intentional forks, does not suffer from practicality issues, unlike selfish mining. We also discuss partial countermeasures against the FAW attack, but finding a cheap and efficient countermeasure remains an open problem. As a result, we expect to see FAW attacks among mining pools.

Paper full text

Presentation video

1.2. Betrayal, Distrust, and Rationality: Smart Counter-Collusion Contracts for Verifiable Cloud Computing

Author: Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, and Aad van Moorsel (Newcastle University)

Abstract:

Cloud computing has become an irreversible trend. Together comes the pressing need for verifiability, to assure the client the correctness of computation outsourced to the cloud. Existing verifiable computation techniques all have a high overhead, thus if being deployed in the clouds, would render cloud computing more expensive than the on-premises counterpart. To achieve verifiability at a reasonable cost, we leverage game theory and propose a smart contract based solution. In a nutshell, a client lets two clouds compute the same task, and uses smart contracts to stimulate tension, betrayal and distrust between the clouds, so that rational clouds will not collude and cheat. I n the absence of collusion, verification of correctness can be done easily by crosschecking the results from the two clouds. We provide a formal analysis of the games induced by the contracts, and prove that the contracts will be effective under certain reasonable assumptions. By resorting to game theory and smart contracts, we are able to avoid heavy cryptographic protocols. The client only needs to pay two clouds to compute in the clear, and a small transaction fee to use the smart contracts. We also conducted a feasibility study that involves implementing the contracts in Solidity and running them on the official Ethereum network.

Paper full text

Presentation video

1.3. Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services

Author: Matteo Campanelli and Rosario Gennaro (City College of New York); Steven Goldfeder (Princeton University); Luca Nizzardo (IMDEA Software Institute and Universidad Politécnica de Madrid)

Abstract:

Zero Knowledge Contingent Payment (ZKCP) protocols allow fair exchange of sold goods and payments over the Bitcoin network. In this paper we point out two main shortcomings of current proposals for ZKCP, and propose ways to address them.

First we show an attack that allows a buyer to learn partial information about the digital good being sold, without paying for it. This break in the zero-knowledge condition of ZKCP is due to the fact that in the protocols we attack, the buyer is allowed to choose common parameters that normally should be selected by a trusted third party. We implemented and tested this attack: we present code that learns, without paying, the value of a Sudoku cell in the “Pay-to-Sudoku” ZKCP implementation. We also present ways to fix this attack that do not require a trusted third party.

Second, we show that ZKCP are not suited for the purchase of digital services} rather than goods. Current constructions of ZKCP do not allow a seller to receive payments after proving that a certain service has been rendered, but only for the sale of a specific digital good. We define the notion of Zero-Knowledge Contingent Service Payment (ZKCSP) protocols and construct two new protocols, for either public or

private verification. We implemented our ZKCSP protocols for Proofs of Retrievability, where a client pays the server for providing a proof that the client’s data is correctly stored by the server.We also implement a secure ZKCP protocol for “Pay-to-Sudoku” via our ZKCSP protocol, which does not require a trusted third party.

A side product of our implementation effort is a new optimized circuit for SHA256 with less than a quarter than the number of AND gates of the best previously publicly available one. Our new SHA256 circuit may be of independent use for circuit-based MPC and FHE protocols that require SHA256 circuits.

Paper full text

Presentation video

1.4. Revive: Rebalancing Off-Blockchain Payment Networks

Author: Rami Khalil and Arthur Gervais (ETH Zürich)

Abstract:

Scaling the transaction throughput of decentralized blockchain ledgers such as Bitcoin and Ethereum has been an ongoing challenge. Two-party duplex payment channels have been designed and used as building blocks to construct linked payment networks, which allow atomic and trust-free payments between parties without exhausting the resources of the blockchain.

Once a payment channel, however, is depleted (e.g., because transactions were mostly unidirectional) the channel would need to be closed and re-funded to allow for new transactions. Users are envisioned to entertain multiple payment channels with different entities, and as such, instead of refunding a channel (which incurs costly on-chain transactions), a user should be able to leverage his existing channels to rebalance a poorly funded channel.

To the best of our knowledge, we present the first solution that allows an arbitrary set of users in a payment channel network to securely rebalance their channels, according to the preferences of the channel owners. Except in the case of disputes (similar to conventional payment channels), our solution does not require on-chain transactions and therefore increases the scalability of existing blockchains. In our security analysis, we show that an honest participant cannot lose any of its funds while rebalancing. We finally provide a proof of concept implementation and evaluation for the Ethereum network.

Paper full text

Presentation video

1.5. Concurrency and Privacy with Payment-Channel

Networks

Author: Giulio Malavolta (Friedrich-Alexander University Erlangen Nuernberg); Pedro Moreno-Sanchez and Aniket Kate (Purdue University); Matteo Maffei (TU Wien); Srivatsan Ravi (University of Southern California)

Abstract:

Permissionless blockchains protocols such as Bitcoin are inherently limited in transaction throughput and latency. Current efforts to address this key issue focus on off-chain payment channels that can be combined in a Payment-Channel Network (PCN) to enable an unlimited number of payments without requiring to access the blockchain other than to register the initial and final capacity of each channel. While this approach paves the way for low latency and high throughput of payments, its deployment in practice raises several privacy concerns as well as technical challenges related to the inherently concurrent nature of payments that have not been sufficiently studied so far.

In this work, we lay the foundations for privacy and concurrency in PCNs, presenting a formal definition in the Universal Composability framework as well as practical and provably secure solutions. In particular, we present Fulgor and Rayo. Fulgor is the first payment protocol for PCNs that provides provable privacy guarantees for PCNs and is fully compatible with the Bitcoin scripting system. However, Fulgor is a blocking protocol and therefore prone to deadlocks of concurrent payments as in currently available PCNs. Instead, Rayo is the first protocol for PCNs that enforces non-blocking progress (i.e., at least one of the concurrent payments terminates). We show through a new impossibility result that non-blocking progress necessarily comes at the cost of weaker privacy. At the core of Fulgor and Rayo is Multi-Hop HTLC, a new smart contract, compatible with the Bitcoin scripting system, that provides conditional payments while reducing running time and communication overhead with respect to previous approaches. Our performance evaluation of Fulgor and Rayo shows that a payment with 10 intermediate users takes as few as 5 seconds, thereby demonstrating their feasibility to be deployed in practice.

Paper full text

Presentation video

1.6. Bolt: Anonymous Payment Channels for Decentralized Currencies

Author: Matthew Green and Ian Miers (Johns Hopkins University)

Abstract:

Bitcoin owes its success to the fact that transactions are transparently recorded in the blockchain, a global public ledger that removes the need for trusted parties. Unfortunately, recording every transaction in the blockchain causes privacy, latency, and scalability issues. Building on recent proposals for “micropayment channels” — two party associations that use the ledger only for dispute resolution — we introduce techniques for constructing anonymous payment channels. Our proposals allow for secure, instantaneous and private payments that substantially reduce the storage burden on the payment network. Specifically, we introduce three channel proposals, including a technique that allows payments via untrusted intermediaries. We build a concrete implementation of our scheme and show that it can be deployed via a soft fork to existing anonymous currencies such as ZCash.

Paper full text

Presentation video

1.7. Practical UC-Secure Delegatable Credentials with Attributes and Their Application to Blockchain

Author: Jan Camenisch (IBM Research - Zürich); Manu Drijvers (IBM Research - Zürich/ETH Zürich); Maria Dubovitskaya (IBM Research - Zürich)

Abstract:

Certification of keys and attributes is in practice typically realized by a hierarchy of issuers. Revealing the full chain of issuers for certificate verification, however, can be a privacy issue since it can leak sensitive information about the issuer’s organizational structure or about the certificate owner. Delegatable anonymous credentials solve this problem and allow one to hide the full delegation (issuance) chain, providing privacy during both delegation and presentation of certificates. However, the existing delegatable credentials schemes are not efficient enough for practical use.

In this paper, we present the first hierarchical (or delegatable) anonymous credential system that is practical. To this end, we provide a surprisingly simple ideal functionality for delegatable credentials and present a generic construction that we prove secure in the UC model. We then give a concrete instantiation using a recent pairing-based signature scheme by Groth and describe a number of optimizations and efficiency improvements that can be made when implementing our concrete scheme. The latter might be of independent interest for other pairing-based schemes as well. Finally, we report on an implementation of our scheme in the context of transaction authentication for blockchain, and provide concrete performance figures.

Paper full text

Presentation video

1.8. Solidus: Confidential Distributed Ledger Transactions

via PVORM

Author: Ethan Cecchetti and Fan Zhang (Cornell University); Yan Ji (Cornell University); Ahmed Kosba (University of Maryland); Ari Juels (Cornell Tech, Jacobs Institute); Elaine Shi (Cornell University)

Abstarct:

Blockchains and more general distributed ledgers are becoming increasingly popular as efficient, reliable, and persistent records of data and transactions. Unfortunately, they ensure reliability and correctness by making all data public, raising confidentiality concerns that eliminate many potential uses.

In this paper we present Solidus, a protocol for confidential transactions on public blockchains, such as those required for asset transfers with on-chain settlement. Solidus operates in a framework based on real-world financial institutions: a modest number of banks each maintain a large number of user accounts. Within this framework, Solidus hides both transaction values and the transaction graph (i.e., the identities of transacting entities) while maintaining the public verifiability that makes blockchains so appealing. To achieve strong confidentiality of this kind, we introduce the concept of a Publicly-Verifiable Oblivious RAM Machine (PVORM). We present a set of formal security definitions for both PVORM and Solidus and show that our constructions are secure. Finally, we implement Solidus and present a set of benchmarks indicating that the system is efficient in practice.

Paper full text

Presentation video

1.9. Fairness in an Unfair World: Fair Multiparty Computation from Public Bulletin Boards

Author: Arka Rai Choudhuri, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers (Johns Hopkins University)

Abstract:

Secure multiparty computation allows mutually distrusting parties to compute a function on their private inputs such that nothing but the function output is revealed. Achieving fairness — that all parties learn the output or no one does – is a long studied problem with known impossibility results in the standard model if a majority of parties are dishonest. We present a new model for achieving fairness in MPC against dishonest majority by using public bulletin boards implemented via existing infrastructure such as blockchains or Google's certificate transparency logs. We present both theoretical and practical constructions using either witness encryption or trusted hardware (such as Intel SGX).

Unlike previous works that either penalize an aborting party or achieve weaker notions such as $\Delta$-fairness, we achieve complete fairness using existing infrastructure.

Paper full text

Presentation video

2. Crypto 2017

2.1. The Bitcoin Backbone Protocol with Chains of Variable Difficulty

Author: Juan Garay(Yahoo Research), Aggelos Kiayias(University of Edinburgh & IOHK), Nikos Leonardos(National and Kapodistrian University of Athens)

Abstract:

Bitcoin's innovative and distributedly maintained blockchain data structure hinges on the adequate degree of difficulty of so-called "proofs of work," which miners have to produce in order for transactions to be inserted. Importantly, these proofs of work have to be hard enough so that miners have an opportunity to unify their views in the presence of an adversary who interferes but has bounded computational power, but easy enough to be solvable regularly and enable the miners to make progress. As such, as the miners' population evolves over time, so should the difficulty of these proofs. Bitcoin provides this adjustment mechanism, with empirical evidence of a constant block generation rate against such population changes.

In this paper we provide the first formal analysis of Bitcoin's target (re)calculation function in the cryptographic setting, i.e., against all possible adversaries aiming to subvert the protocol's properties. We extend the q-bounded synchronous model of the Bitcoin backbone protocol [Eurocrypt 2015], which posed the basic properties of Bitcoin's underlying blockchain data structure and shows how a robust public transaction ledger can be built on top of them, to environments that may introduce or suspend parties in each round.

We provide a set of necessary conditions with respect to the way the population evolves under which the "Bitcoin backbone with chains of variable difficulty" provides a robust transaction ledger in the presence of an actively malicious adversary controlling a fraction of the miners strictly below 50% at each instant of the execution. Our work introduces new analysis techniques and tools to the area of blockchain systems that may prove useful in analyzing other blockchain protocols.

Paper full text

Presentation video

2.2. Bitcoin as a Transaction Ledger: A Composable

Treatment

Author: Christian Badertscher(ETH Zurich,Zurich,Switzerland), Ueli Maurer, Daniel Tschudi, Vassilis Zika

Abstract:

Bitcoin is one of the most prominent examples of a distributed cryptographic protocol that is extensively used in reality. Nonetheless, existing security proofs are property-based, and as such they do not support composition.

In this work we put forth a universally composable treatment of the Bitcoin protocol. We specify the goal that Bitcoin aims to achieve as a ledger functionality in the (G)UC model of Canetti et al. [TCC'07]. Our ledger functionality is weaker than the one recently proposed by Kiayias, Zhou, and Zikas [EUROCRYPT'16], but unlike the latter suggestion, which is arguably not implementable given the Bitcoin assumptions, we prove that the one proposed here is securely UC realized under standard assumptions by an appropriate abstraction of Bitcoin as a UC protocol. We further show how known property-based approaches can be cast as special instances of our treatment and how their underlying assumptions can be cast in (G)UC without restricting the environment or the adversary.

Paper full text

Presentation video

2.3. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Author: Aggelos Kiayias(University of Edinburgh and IOHK), Alexander Russell(University of Connecticut), Bernardo David(Tokyo Institute of Technology and IOHK), Roman Oliynykov(IOHK)

Abstract:

We present "Ouroboros", the first blockchain protocol based on proof of stake with rigorous security guarantees. We establish security properties for the protocol comparable to those achieved by the bitcoin blockchain protocol. As the protocol provides a "proof of stake" blockchain discipline, it offers qualitative efficiency advantages over blockchains based on proof of physical resources (e.g., proof of work). We also present a novel reward mechanism for incentivizing Proof of Stake protocols and we prove that, given this mechanism, honest behavior is an approximate Nash equilibrium, thus neutralizing attacks such as selfish mining.

Paper full text

Presentation video

3. SP 2017

Session #5: Bitcoin and Distributed Systems

3.1 Hijacking bitcoin: Routing attacks on cryptocurrencies

Author：Maria Apostolaki (ETH Zürich), Aviv Zohar (Hebrew University), Laurent Vanbever (ETH Zürich)

Abstract:

As the most successful cryptocurrency to date, Bitcoin constitutes a target of choice for attackers. While many attack vectors have already been uncovered, one important vector has been left out though: attacking the currency via the Internet routing infrastructure itself. Indeed, by manipulating routing advertisements (BGP hijacks) or by naturally intercepting traffic, Autonomous Systems (ASes) can intercept and manipulate a large fraction of Bitcoin traffic.

This paper presents the first taxonomy of routing attacks and their impact on Bitcoin, considering both small-scale attacks, targeting individual nodes, and large-scale attacks, targeting the network as a whole. While challenging, we show that two key properties make routing attacks practical: (i) the efficiency of routing manipulation; and (ii) the significant centralization of Bitcoin in terms of mining and routing. Specifically, we find that any network attacker can hijack few (<;100) BGP prefixes to isolate ~50% of the mining power-even when considering that mining pools are heavily multi-homed. We also show that on-path network attackers can considerably slow down block propagation by interfering with few key Bitcoin messages.

We demonstrate the feasibility of each attack against the deployed Bitcoin software. We also quantify their effectiveness on the current Bitcoin topology using data collected from a Bitcoin supernode combined with BGP routing data.

The potential damage to Bitcoin is worrying. By isolating parts of the network or delaying block propagation, attackers can cause a significant amount of mining power to be wasted, leading to revenue losses and enabling a wide range of exploits such as double spending. To prevent such effects in practice, we provide both short and long-term countermeasures, some of which can be deployed immediately.

Paper full text

Presentation video

3.2. Catena: Efficient Non-equivocation via Bitcoin

Author: Alin Tomescu (MIT), Srinivas Devadas (MIT)

Abstract:

We present Catena, an efficiently-verifiable Bitcoin witnessing scheme. Catena enables any number of thin clients, such as mobile phones, to efficiently agree on a log of application-specific statements managed by an adversarial server. Catena implements a log as an OP_RETURN transaction chain andprevents forks in the log by leveraging Bitcoin's security againstdouble spends. Specifically, if a log server wants to equivocate ithas to double spend a Bitcoin transaction output. Thus, Catena logs are as hard to fork as the Bitcoin blockchain: an adversarywithout a large fraction of the network's computational power cannot fork Bitcoin and thus cannot fork a Catena log either. However, different from previous Bitcoin-based work, Catena decreases the bandwidth requirements of log auditors from 90GB to only tens of megabytes. More precisely, our clients only need to download all Bitcoin block headers (currently less than35 MB) and a small, 600-byte proof for each statement in a block. We implement Catena in Java using the bitcoinj library and use itto extend CONIKS, a recent key transparency scheme, to witnessits public-key directory in the Bitcoin blockchain where it can beefficiently verified by auditors. We show that Catena can secure many systems today, such as public-key directories, Tor directory servers and software transparency schemes.

Paper full text

Presentation video

3.3. IKP: Turning a PKI Around with Decentralized Automated Incentives

Author：Stephanos Matsumoto (Carnegie Mellon University/ETH Zurich), Raphael M. Reischuk (ETH Zurich)

Abstract:

Despite a great deal of work to improve the TLS PKI, CA misbehavior continues to occur, resulting in unauthorized certificates that can be used to mount man-in-the-middle attacks against HTTPS sites. CAs lack the incentives to invest in higher security, and the manual effort required to report a rogue certificate deters many from contributing to the security of the TLS PKI. In this paper, we present IKP, a platform that automates responses to unauthorized certificates and provides incentives for CAs to behave correctly and for others to report potentially unauthorized certificates. Domains in IKP specify criteria for their certificates, and CAs specify reactions such as financial penalties that execute in case of unauthorized certificate issuance. By leveraging smart contracts and blockchain-based consensus, we can decentralize IKP while still providing automated incentives. We describe a theoretical model for payment flows and implement IKP in Ethereum to show that decentralizing and automating PKIs with financial incentives is both economically sound and technically viable.

Paper full text

Presentation video

3.4. Augur: Internet-Wide Detection of Connectivity Disruptions

Author: Paul Pearce (UC Berkeley), Roya Ensafi (Princeton), Frank Li (UC Berkeley), Nick Feamster (Princeton), Vern Paxson (UC Berkeley)

Abstract:

Anecdotes, news reports, and policy briefings collectively suggest that Internet censorship practices are pervasive. The scale and diversity of Internet censorship practices makes it difficult to precisely monitor where, when, and how censorship occurs, as well as what is censored. The potential risks in performing the measurements make this problem even more challenging. As a result, many accounts of censorship begin-and end-with anecdotes or short-term studies from only a handful of vantage points.

We seek to instead continuously monitor information about Internet reachability, to capture the onset or termination of censorship across regions and ISPs. To achieve this goal, we introduce Augur, a method and accompanying system that utilizes TCP/IP side channels to measure reachability between two Internet locations without directly controlling a measurement vantage point at either location. Using these side channels, coupled with techniques to ensure safety by not implicating individual users, we develop scalable, statistically robust methods to infer network-layer filtering, and implement a corresponding system capable of performing continuous monitoring of global censorship. We validate our measurements of Internet-wide disruption in nearly 180 countries over 17 days against sites known to be frequently blocked, we also identify the countries where connectivity disruption is most prevalent.

Paper full text

Presentation video

3.5. Scalable Bias-Resistant Distributed Randomness

Author: Ewa Syta (Trinity College), Philipp Jovanovic (École Polytechnique Fédérale de Lausanne), Eleftherios Kokoris Kogias (École Polytechnique Fédérale de Lausanne), Nicolas Gailly (École Polytechnique Fédérale de Lausanne), Linus Gasser (École Polytechnique Fédérale de Lausanne), Ismail Khoffi (École Polytechnique Fédérale de Lausanne), Michael J. Fischer (Yale University), Bryan Ford (École Polytechnique Fédérale de Lausanne)

Abstract:

Bias-resistant public randomness is a critical component in many (distributed) protocols. Generating public randomness is hard, however, because active adversaries may behave dishonestly to bias public random choices toward their advantage. Existing solutions do not scale to hundreds or thousands of participants, as is needed in many decentralized systems. We propose two large-scale distributed protocols, RandHound

and RandHerd, which provide publicly-verifiable, unpredictable, and unbiasable randomness against Byzantine adversaries. RandHound relies on an untrusted client to divide a set of randomness servers into groups for scalability, and it depends on the pigeonhole principle to ensure output integrity, even for non-random, adversarial group choices. RandHerd implements an efficient, decentralized randomness beacon. RandHerd is structurally similar to a BFT protocol, but uses RandHound in a one-time setup to arrange participants into verifiably unbiased random secret-sharing groups, which then repeatedly produce random output at predefined intervals. Our prototype demonstrates that RandHound and RandHerd achieve good performance across hundreds of participants while retaining a low failure probability by properly selecting protocol parameters, such as a group size and secret-sharing threshold. For example, when sharding 512 nodes into groups of 32, our experiments show that RandHound can produce fresh random output after 240 seconds. RandHerd, after a setup phase of 260 seconds, is able to generate fresh random output in intervals of approximately 6 seconds. For this configuration, both protocols operate at a failure probability of at most 0.08% against a Byzantine adversary.

Paper full text

Presentation video

4. USENIX 2017

4.1. SmartPool: Practical Decentralized Pooled Mining

Author: Loi Luu, National University of Singapore; Yaron Velner, The Hebrew University of Jerusalem; Jason Teutsch, TrueBit Foundation; Prateek Saxena, National University of Singapore

Abstract:

Cryptocurrencies such as Bitcoin and Ethereum are operated by a handful of mining pools. Nearly 95% of Bitcoin’s and 80% of Ethereum’s mining power resides with less than ten and six mining pools respectively. Although miners benefit from low payout variance in pooled mining, centralized mining pools require members to trust that pool operators will remunerate them fairly. Furthermore, centralized pools pose the risk of transaction censorship from pool operators, and open up possibilities for collusion between pools for perpetrating severe attacks.

In this work, we propose SMARTPOOL, a novel protocol design for a decentralized mining pool. Our protocol shows how one can leverage smart contracts, autonomous blockchain programs, to decentralize cryptocurrency mining. SMARTPOOL gives transaction selection control back to miners while yielding low-variance payouts. SMARTPOOL incurs mining fees lower than centralized mining pools and is designed to scale to a large number of miners. We implemented and deployed a robust SMARTPOOL implementation on the Ethereum and Ethereum Classic networks. To date, our deployed pools have handled a peak hashrate of 30 GHs from Ethereum miners, resulting in 105 blocks, costing miners a mere 0:6% of block rewards in transaction fees.

Paper full text

Slides

Presentation video

Project website

4.2. REM: Resource-Efficient Mining for Blockchains

Author: Fan Zhang, Ittay Eyal, and Robert Escriva, Cornell University; Ari Juels, Cornell Tech; Robbert van Renesse, Cornell University

Abstract:

Blockchains show promise as potential infrastructure for financial transaction systems. The security of blockchains today, however, relies critically on Proof-of- Work (PoW), which forces participants to waste computational resources.

We present REM (Resource-Efficient Mining), a new blockchain mining framework that uses trusted hardware (Intel SGX). REM achieves security guarantees similar to PoW, but leverages the partially decentralized trust model inherent in SGX to achieve a fraction of the waste of PoW. Its key idea, Proof-of-Useful-Work (PoUW), involves miners providing trustworthy reporting on CPU cycles they devote to inherently useful workloads. REM flexibly allows any entity to create a useful workload. REM ensures the trustworthiness of these workloads by means of a novel scheme of hierarchical attestations that may be of independent interest.

To address the risk of compromised SGX CPUs, we develop a statistics-based formal security framework, also relevant to other trusted-hardware-based approaches such as Intel's Proof of Elapsed Time (PoET). We show through economic analysis that REM achieves less waste than PoET and variant schemes.

We implement REM and, as an example application, swap it into the consensus layer of Bitcoin core. The result is the first full implementation of an SGX-based blockchain. We experiment with four example applications as useful workloads for our implementation of REM, and report a computational overhead of 5—15%.

Paper full text

Slides

Presentation video

5. CCS 2016

5.1. On the Security and Performance of Proof of Work Blockchains

Author: Arthur Gervais (ETH Zürich), Ghassan O. Karame (NEC Laboratories Europe), Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf and Srdjan Capkun (ETH Zürich)

Abstract:

Proof of Work (PoW) powered blockchains currently account for more than 90% of the total market capitalization of existing digital cryptocurrencies. Although the security provisions of Bitcoin have been thoroughly analysed, the security guarantees of variant (forked) PoW blockchains (which were instantiated with different parameters) have not received much attention in the literature. This opens the question whether existing security analysis of Bitcoin's PoW applies to other implementations which have been instantiated with different consensus and/or network parameters.

In this paper, we introduce a novel quantitative framework to analyse the security and performance implications of various consensus and network parameters of PoW blockchains. Based on our framework, we devise optimal adversarial strategies for double-spending and selfish mining while taking into account real world constraints such as network propagation, different block sizes, block generation intervals, information propagation mechanism, and the impact of eclipse attacks. Our framework therefore allows us to capture existing PoW-based deployments as well as PoW blockchain variants that are instantiated with different parameters, and to objectively compare the tradeoffs between their performance and security provisions.

Paper full text

Presentation video

5.2. A Secure Sharding Protocol For Open Blockchains

Author: Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert and Prateek Saxena (National University of Singapore)

Abstract:

Cryptocurrencies, such as Bitcoin and 250 similar alt-coins, embody at their core a blockchain protocol — a mechanism for a distributed network of computational nodes to periodically agree on a set of new transactions. Designing a secure blockchain protocol relies on an open challenge in security, that of designing a highly-scalable agreement protocol open to manipulation by byzantine or arbitrarily malicious nodes. Bitcoin's blockchain agreement protocol exhibits security, but does not scale: it processes 3–7 transactions per second at present, irrespective of the available computation capacity at hand.

In this paper, we propose a new distributed agreement protocol for permission-less blockchains called

ELASTICO. ELASTICO scales transaction rates almost linearly with available computation for mining: the more the computation power in the network, the higher the number of transaction blocks selected per unit time. ELASTICO is efficient in its network messages and tolerates byzantine adversaries of up to one-fourth of the total computational power. Technically, ELASTICO uniformly partitions or parallelizes the mining network (securely) into smaller committees, each of which processes a disjoint set of transactions (or “shards”). While sharding is common in non-byzantine settings, ELASTICO is the first candidate for a secure sharding protocol with presence of byzantine adversaries. Our scalability experiments on Amazon EC2 with up to $1, 600$ nodes confirm ELASTICO’s theoretical scaling properties.

Paper full text

Presentation video

5.3. The Honey Badger of BFT Protocols

Author: Andrew Miller (University of Maryland), Yu Xia (Tsinghua University), Kyle Croman, Elaine Shi (Cornell University) and Dawn Song (University of California)

Abstract:

The surprising success of cryptocurrencies has led to a surge of interest in deploying large scale, highly robust, Byzantine fault tolerant (BFT) protocols for mission-critical applications, such as financial transactions. Although the conventional wisdom is to build atop a (weakly) synchronous protocol such as PBFT (or a variation thereof), such protocols rely critically on network timing assumptions, and only guarantee liveness when the network behaves as expected. We argue these protocols are ill-suited for this deployment scenario. We present an alternative, HoneyBadgerBFT, the first practical asynchronous BFT protocol, which guarantees liveness without making any timing assumptions. We base our solution on a novel atomic broadcast protocol that achieves optimal asymptotic efficiency. We present an implementation and experimental results to show our system can achieve throughput of tens of thousands of transactions per second, and scales to over a hundred nodes on a wide area network. We even conduct BFT experiments over Tor, without needing to tune any parameters. Unlike the alternatives, HoneyBadgerBFT simply does not care about the underlying network.

Paper full text

Presentation video

5.4. On the Instability of Bitcoin Without the Block Reward

Author: Miles Carlsten, Harry Kalodner, S. Matthew Weinberg and Arvind Narayanan (Princeton University)

Abstract:

Bitcoin provides two incentives for miners: block rewards and transaction fees. The former accounts for the vast majority of miner revenues at the beginning of the system, but it is expected to transition to the latter as the block rewards dwindle. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the block chain.

We show that this is not the case. Our key insight is that with only transaction fees, the variance of the block reward is very high due to the exponentially distributed block arrival time, and it becomes attractive to fork a “wealthy” block to “steal” the rewards therein. We show that this results in an equilibrium with undesirable properties for Bitcoin’s security and performance, and even non-equilibria in some circumstances. We also revisit selfish mining and show that it can be made profitable for a miner with an arbitrarily low hash power share, and who is arbitrarily poorly connected within the network. Our results are derived from theoretical analysis and confirmed by a new Bitcoin mining simulator that may be of independent interest.

We discuss the troubling implications of our results for Bitcoin’s future security and draw lessons for the design of new cryptocurrencies.

Paper full text

Presentation video

5.5. Transparency Overlays and Applications

Author: Melissa Chase (Microsoft Research Redmond) and Sarah Meiklejohn (University College London)

Abstract:

In this paper, we initiate a formal study of transparency, which in recent years has become an increasingly critical requirement for the systems in which people place trust. We present the abstract concept of a transparency overlay, which can be used in conjunction with any system to give it provable transparency guarantees, and then apply the overlay to two settings: Certificate Transparency and Bitcoin. In the latter setting, we show that the usage of our transparency overlay eliminates the need to engage in mining and allows users to store a single small value rather than the entire blockchain. Our transparency overlay is generically constructed from a signature scheme and a new primitive we call a dynamic list commitment, which in practice can be instantiated using a collision-resistant hash function.

Paper full text

Presentation video

5.6. Making Smart Contracts Smarter

Author: Loi Luu, Duc-Hiep Chu (National University of Singapore), Hrishi Olickel (Yale-NUS College), Prateek Saxena (National University of Singapore) and Aquinas Hobor (Yale-NUS College & National University of Singapore)

Abstract:

Cryptocurrencies record transactions in a decentralized data structure called a blockchain. Two of the most popular cryptocurrencies, Bitcoin and Ethereum, support the feature to encode rules or scripts for processing transactions. This feature has evolved to give practical shape to the ideas of smart contracts, or full-fledged programs that are run on blockchains. Recently, Ethereum's smart contract system has seen steady adoption, supporting tens of thousands of contracts, holding millions dollars worth of virtual coins.

In this paper, we investigate the security of running smart contracts based on Ethereum in an open distributed network like those of cryptocurrencies. We introduce several new security problems in which an adversary can manipulate smart contract execution to gain profit. These bugs suggest subtle gaps in the understanding of the distributed semantics of the underlying platform. As a refinement, we propose ways to enhance the operational semantics of Ethereum to make contracts less vulnerable. For developers writing contracts for the existing Ethereum system, we build a symbolic execution tool called Oyente to find potential security bugs. Among 19, 336 existing Ethereum contracts, Oyente flags 8, 833 of them as vulnerable, including the TheDAO bug which led to a 60 million US dollar loss in June 2016. We also discuss the severity of other attacks for several case studies which have source code available and confirm the attacks (which target only our accounts) in the main Ethereum network.

Paper full text

Presentation video

5.7. Town Crier: An Authenticated Data Feed for Smart Contracts

Author: Fan Zhang, Ethan Cecchetti (Cornell University), Kyle Croman (Jacobs Institute), Ari Juels (Cornell Tech) and Elaine Shi (Cornell University)

Abstract:

Smart contracts are programs that execute autonomously on blockchains. Their key envisioned uses (e.g. financial instruments) require them to consume data from outside the blockchain (e.g. stock quotes). Trustworthy data feeds that support a broad range of data requests will thus be critical to smart contract ecosystems.

We present an authenticated data feed system called Town Crier (TC). TC acts as a bridge between smart contracts and existing web sites, which are already commonly trusted for non-blockchain applications. It combines a blockchain front end with a trusted hardware back end to scrape HTTPS-enabled websites and serve source-authenticated data to relying smart contracts.

TC also supports confidentiality. It enables private data requests with encrypted parameters. Additionally, in a generalization that executes smart-contract logic within TC, the system permits secure use of user credentials to scrape access-controlled online data sources.

We describe TC's design principles and architecture and report on an implementation that uses Intel's recently introduced Software Guard Extensions (SGX) to furnish data to the Ethereum smart contract system. We formally model TC and define and prove its basic security properties in the Universal Composibility (UC) framework. Our results include definitions and techniques of general interest relating to resource consumption (Ethereum's "gas" fee system) and TCB minimization. We also report on experiments with three example applications.

We plan to launch TC soon as an online public service.

Paper full text

Presentation video

5.8. The Ring of Gyges: Investigating the Future of Criminal Smart Contracts

Author: Ari Juels (Jacobs Institute), Ahmed Kosba (University of Maryland) and Elaine Shi (Cornell University)

Abstract:

Thanks to their anonymity (pseudonymity) and elimination of trusted intermediaries, cryptocurrencies such as Bitcoin have created or stimulated growth in many businesses and communities. Unfortunately, some of these are criminal, e.g., money laundering, illicit marketplaces, and ransomware. Next-generation cryptocurrencies such as Ethereum will include rich scripting languages in support of smart contracts, programs that autonomously intermediate transactions. In this paper, we explore the risk of smart contracts fueling new criminal ecosystems. Specifically, we show how what we call criminal smart contracts (CSCs) can facilitate leakage of confidential information, theft of cryptographic keys, and various real-world crimes (murder, arson, terrorism).

We show that CSCs for leakage of secrets (a la Wikileaks) are efficiently realizable in existing scripting languages such as that in Ethereum. We show that CSCs for theft of cryptographic keys can be achieved using primitives, such as Succinct Non-interactive ARguments of Knowledge (SNARKs), that are already expressible in these languages and for which efficient supporting language extensions are anticipated. We show similarly that authenticated data feeds, an emerging feature of smart contract systems, can facilitate CSCs for real-world crimes (e.g., property crimes).

Our results highlight the urgency of creating policy and technical safeguards against CSCs in order to realize the promise of smart contracts for beneficial goals.

Paper full text

Presentation video

6. S&P 2016

6.1. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts

Author: Ahmed Kosba and Andrew Miller (University of Maryland), Elaine Shi and Zikai Wen (Cornell University), and Charalampos Papamanthou (University of Maryland)

Abstract:

Emerging smart contract systems over decentralized cryptocurrencies allow mutually distrustful parties to transact safely without trusted third parties. In the event of contractual breaches or aborts, the decentralized blockchain ensures that honest parties obtain commensurate compensation. Existing systems, however, lack transactional privacy. All transactions, including flow of money between pseudonyms and amount transacted, are exposed on the blockchain. We present Hawk, a decentralized smart contract system that does not store financial transactions in the clear on the blockchain, thus retaining transactional privacy from the public's view.

A Hawk programmer can write a private smart contract in an intuitive manner without having to implement cryptography, and our compiler automatically generates an efficient cryptographic protocol where contractual parties interact with the blockchain, using cryptographic primitives such as zero-knowledge proofs. To formally define and reason about the security of our protocols, we are the first to formalize the blockchain model of cryptography. The formal modeling is of independent interest. We advocate the community to adopt such a formal model when designing applications atop decentralized blockchains.

Paper full text

Presentation video

7. USENIX 2016

7.1. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing

Author: Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford, École Polytechnique Fédérale de Lausanne (EPFL)

Abstract:

While showing great promise, Bitcoin requires users to wait tens of minutes for transactions to commit, and even then, offering only probabilistic guarantees. This paper introduces ByzCoin, a novel Byzantine consensus protocol that leverages scalable collective signing to commit Bitcoin transactions irreversibly within seconds. ByzCoin achieves Byzantine consensus while preserving Bitcoin’s open membership by dynamically forming hash power-proportionate consensus groups that represent recently-successful block miners. ByzCoin employs communication trees to optimize transaction commitment and verification under normal operation while guaranteeing safety and liveness under Byzantine faults, up to a near-optimal tolerance of f faulty group members among 3f +2 total. ByzCoin mitigates double spending and selfish mining attacks by producing collectively signed transaction blocks within one minute of transaction submission. Tree-structured communication further reduces this latency to less than 30 seconds. Due to these optimizations, ByzCoin achieves a throughput higher than Paypal currently handles, with a confirmation latency of 15-20 seconds.

Paper full text

Slides

Presentation video