The Five Grand Challenges

IC3 has several projects underway to address what we identify as five “Grand Challenges” to widespread blockchain adoption.

- Scaling and Performance: Scaling up blockchains to handle intensive global workloads for both permissionless decentralized blockchains, and permissioned/consortium blockchains supporting >100,000 transactions/sec.
- Correctness by Design and Construction: Making it easy, and even automatic, for blockchain developers to produce secure protocols and code, by utilizing (1) programming language techniques to create correct code, and (2) cryptographic protocols with security proofs.
- Confidentiality: Combining transparency with confidentiality in blockchains, by utilizing (1) cryptographic techniques, as well as (2) trusted-hardware.
- Authenticated Data Feeds: Supporting a robust ecosystem of trustworthy data feeds for blockchains and contributing high-trust data feed solutions.
- Safety and Compliance: Enabling techniques and protocols for effective monitoring and targeted intervention in blockchains, informed by evaluations of traditional contract law and risks of crime in smart contracts.

> The five Grand Challenges outlined above serve as a motivation and a project map for the following IC3 projects.

Projects

Solidus: A Centralized Future for Cryptocurrencies?

Support Grand Challenges: Scaling and Performance Confidentiality

Solidus is a cryptocurrency ("blockchain") that can be run by a confederation or consortium of trustworthy entities-- -banks, governments, auditors, etc. While it retains some of the benefits of decentralization, Solidus offers higher performance and tighter governance and control than existing cryptocurrencies such as Bitcoin. Many successful peer-to- peer technologies have

historically been eclipsed or supplanted by centralized or commercial systems (e.g., in the online music industry). Solidus addresses the possibility and desire by many financial institutions that cryptocurrencies and contracts will follow a similar path. For more info, please see the Solidus presentation at our 2016 IC3 Retreat (http://www.initc3.org/events/2016-05-17-IC3-Retreat-2016.html) in NYC.

Bitcoin-NG: A Next-generation Blockchain Protocol

Support Grand Challenges: Scaling and Performance

Bitcoin-NG is a new protocol pioneered by IC3. It addresses the scalability bottleneck of Bitcoin by enabling the Bitcoin network to achieve the highest throughput allowed by the network conditions. Paradoxically, not only does it improve transaction throughput, it also reduces transaction latencies -- it is possible to get an initial transaction confirmation in seconds rather than in minutes. And it does so without changing Bitcoin's open architecture and trust model. Our blockchain test bed Miniature World simulated Bitcoin-NG at 15% the size of the operational Bitcoin system, where we showed that Bitcoin–NG is only limited by the network. For more info, please see our paper (http://arxiv.org/abs/1510.02037).

Miniature World: A Test Bed for Simulating Real World Blockchain

Support Grand Challenges: Scaling and Performance

Miniature World is a large blockchain emulation test bed at Cornell University consisting of ~1000 nodes. This test bed enables us to run experiments on different blockchains, and a variety of use cases, using realistic internet latencies to evaluate real world scenarios (as referenced above for Bitcoin-NG). We make Miniature World available for our Industry Sponsors to evaluate various block chains and their use cases. For more info about becoming an IC3 Industry Sponsor, please see http://www.initc3.org/partners.html.

Fruitchain: A new Approach for Incentive Compatible Blockchains

Support Grand Challenges: Scaling and Performance

Most of today's blockchains, such as Bitcoin, are not "incentive compatible", meaning they are quite vulnerable to strategic gaming by dishonest adversaries. For example, IC3 has proven that the Bitcoin blockchain can be compromised by miners or mining pools with much less than 50%

of the mining hash power. Fruitchain is an innovative blockchain methodology that discourages dishonest gaming, by making it extremely unprofitable for an adversary with less than 50% of the hash power, achieving an epsilon-equilibrium or near-Nash equilibrium. For more info, please see the Fruitchain presentation by IC3 co-director Professor Elaine Shi at our 2016 IC3 Retreat (http://www.initc3.org/events/2016-05-17-IC3-Retreat-2016.html) in NYC.

Falcon Network: A High-Performance, Wide Area Interconnect for Blockchains

Support Grand Challenges: Scaling and Performance

The Falcon Network achieves gains over current approaches through minimal validation and cut-through routing. No special software is required on clients, and it is fundamentally faster than all other known techniques. For more info, please see http://www.falcon-net.org.

FLAC: A Calculus for Flow-Limited Authorization

Support Grand Challenges: Correctness by Design and Construction

Real-world applications routinely make authorization decisions based on dynamic computation. Integrity of the system might be compromised if attackers can improperly influence the authorizing computation. Confidentiality can also be compromised by authorization, since authorization decisions are often based on sensitive data such as membership lists and passwords. Flow-Limited Authorization Calculus (FLAC) is both a simple, expressive model for reasoning about dynamic authorization and also a language for securely implementing various authorization mechanisms. FLAC provides strong end-to- end information security guarantees even for programs that incorporate and implement rich dynamic authorization mechanisms. For more info, please see the presentation by Professor Andrew Myers “Verifying Information Security of Code in Dynamic Systems” at our 2016 IC3 Retreat (http://www.initc3.org/events/2016-05-17-IC3-Retreat-2016.html) in NYC.

Theoretical Foundations for Secure Decentralized Systems

Support Grand Challenges: Correctness by Design and Construction

This work explores the theoretical basis for the security and stability of open decentralized systems. The benefits of decentralization include resistance to many kinds of attacks, diversity, and diffusion of power. The novelty and inspiring success of Bitcoin has provided new evidence

that secure decentralized systems are more feasible than once thought. On the other hand, even Bitcoin risks becoming centralized if thrown off-balance, e.g. due to mining pools, ASIC farms, or political schisms. Furthermore, IC3 and collaborators just released a research paper that analyzed The Digital Autonomous Organization (DAO) and its voting mechanism. This paper identifies problems with The DAO's mechanism design that incentivize investors to behave strategically; that is, at odds with truthful voting on their preferences. We then outline potential attacks against The DAO made possible by these behaviors. For more info, please see http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium.

Hawk: Privacy-Preserving Blockchain & Smart Contracts

Support Grand Challenges: Correctness by Design and Construction | Confidentiality

Existing blockchain-based cryptocurrencies such as Bitcoin and Ethereum store all financial transactions in the clear on the blockchain. This compromises the privacy of financial transactions, which is essential in numerous applications. Hawk is a blockchain-based smart contract system that stores encrypted transactions on the blockchain, and relies on cryptography to retain the security of the cryptocurrency. For more info, please see http://oblivm.com/hawk.

Town Crier: Authenticated Data Feeds for Smart Contracts

Support Grand Challenges: Confidentiality | Authenticated Data Feeds

In order to reason about the real world, smart contracts in cryptocurrency systems will rely on informational input from what we call authenticated data feeds (ADFs); such information can include stock prices, meteorological reports, news, and other current events. It is therefore important that an ADF be trustworthy, in the sense of providing security against manipulation by an attacker attempting to influence the outcome of a contract. By utilizing trusted hardware to provide reliable, digitally signed attestations on data to client contracts, the Town Crier system can serve as a trustworthy ADF under minimal trust assumptions about its operator. For further details, please see our paper (http://www.initc3.org/files/tc.pdf).

Virtual Notary: A Free and Secure Electronic Attestation Service

Support Grand Challenges: Authenticated Data Feeds

Virtual Notary is a service for attesting to online factoids. Virtual Notary issues both freestanding certificates as well as immutable records on the Bitcoin blockchain. It has been operational for more than 3 years, and certified more than 600,000 factoids. For more info, please see http://virtual-notary.org.

EtherScrape: A Complementary Block Explorer for the Ethereum Blockchain

Support Grand Challenges: Authenticated Data Feeds

Smart Contracts in Ethereum are written in a high-level programming language (typically Serpent or Solidity) and then compiled down to bytecode for the Ethereum virtual machine. This compilation step removes a lot of the useful information found in the high level source code, such as comments, names of variables, etc. If you can identify the high-level source code for a contract, you have a better chance of figuring out what it does. EtherScrape uses fingerprinting to match each smart contract on the blockchain (that is, the compiled bytecode) to the high-level source code that created it. For more info, please see http://etherscrape.com.

Gyges: Crime in Decentralized Smart Contracts

Support Grand Challenges: Safety and Compliance

Two of the most widely desired goals for "Bitcoin 2.0" are privacy and more expressive smart contracts. Many uses of cryptocurrency have a clear and legitimate need for privacy (e.g., financial service companies are expected to protect the privacy of their clients' transactions). General purpose smart contract programming frameworks make it easy to tinker, prototype, and search for the next "killer application" for cryptocurrencies. These two directions seem to be at odds with each other; however, through the use of sophisticated cryptography (like zero knowledge proofs and multi-party computation), we explore how to achieve both goals at once. For further details, please see our paper at http://www.initc3.org/files/Gyges.pdf.

Honey BadgerBFT: The Honey Badger of BFT Protocols

Support Grand Challenges: Scaling and Performance

HoneyBadgerBFT is 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. For more info, please see our paper (https://eprint.iacr.org/2016/199.pdf).