Minutes of IRTF Side Meeting on Distributed Internet Infrastructure

July 17, 2017
IETF-99, Prague

Presentation material available at https://trac.ietf.org/trac/irtf/wiki/blockchain-federation

Agenda

1. Melinda & Dirk: Background and Purpose
2. Selected Use Cases and Related Efforts
   - Jordi Paillissé Vilanova An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings
     - https://datatracker.ietf.org/doc/draft-paillisse-sidrops-blockchain/
   - Benno Overeinder: Lightest Project Overview
     - http://lightest.eu/
   - Lixia Zhang: Breaking out of the cloud: Local trust management and rendezvous in NDN
3. Discussion of Next steps

Minutes

Background & Purpose (Dirk & Melinda)

Dirk presenting

An analysis of the applicability of blockchain to secure IP addresses allocation, delegation and bindings (Jordi Paillissé Vilanova): https://datatracker.ietf.org/doc/draft-paillisse-sidrops-blockchain/

Ekr: What is the blockchain part buying you -- why do you need a distributed consensus algorithm?

Jordi: Management is easier -- you don't need CAs.

Ekr: What if you did not have consensus? What is the impact?

Jordi: it would be devastating.

Ekr: In Bitcoin, yes, but here double-spending (double-delegation) would not be a problem

Melinda: This seems to be a replacement for SIDR

Ekr: Yes, but why is double-delegation a serious attack in this system?

Jordi: You would get inconsistencies in the routing system

Jordi: could simplify the system

Ekr: sure -- but let's take continue offline.

Philip Hallam-Baker: I wanted to have a system that provides linked node-free lists for 30 years. Original proposal: publish digests in newspaper once a day. Give you all the stability of bitcoin without the hashing overhead.

Melinda: he is proposing proof of stake

PHB: What I want is a system that gives me this capability, but uses more modern approach than publishing in a newspaper -- but is as clear and precise. Proposing joining different transaction ledgers togethers, with centralized servers that receives peak residues and distributes master residue.

Jordi: but then you are trusting the central server

PHB: actually, because of dynamics of different linked logs. If each independent log incorporates top residue, they become all interconnected and none of the logs can defect without all logs defecting.

Albert: I am co-author. 2 points: 1) not claiming that this is better than RPKI. 2) Proposal here: Proof-of-stake (not what bitcoin uses), no hashing at all

Does your approach provide a solution if keys are compromised?

Jordi: only a problem for the last transactions?

Dmitry Belyavskiy: does your proposal address the problem of compromised private keys?

Jordi: Somebody stealing our keys could create new transactions -- so could steal your IP addresses

Dmitry: how do I restore control when keys have been lost?

Jordi: implementation issue

Dmitry: no

Jordi: if you spun up a blockchain node, you just store your private keys, like you do with traditional (?) certificates.

Eric Osterweil: If I lose my private keys, the lack of a recovery mechanism could be a problem (when you lost your keys). Corresponding address blocks are immutable.

Jordi: could think about extended transactions (needing more signatures, like three out of five)

Melinda: blockchain recalculation in Ethereum etc.

Eric: IP allocation is public chain. You can think of different schemes, like three out of five, but eventually, disasters happen.

Jordi: You can also do other schemes (two out of ten etc.)

Eric: yes, but if you operate infrastructure, you know that disasters always happen

Jordi: If I was an ISP, and I would lose 90 keys, I would be ashamed.

Albert: Yes, Eric is right, you have to be able to address the problem that somebody loses their private, through solutions like the ones Jordi described. But it’s also a good thing is that you only need your private key to update and change your address allocation. Nobody else can do it.

Eric: not advocating for RKPI. if you lose your private key, you loose a public resource

Jordi: agree

Melinda: related question: IP addresses are a public good. Proof-of-stake consensus algorithms do allow for the development of a monopoly over the blockchain.

Jordi: depends on how resources are distributed. You also have to implement a good consensus algorithm.

Melinda: how would you disincentivized monopolies?

Jordi: in this case it would depend on how address blocks are allocated in the Internet right now. If we built this with blockchain, we'd need to give blocks of addresses to their current holders. I don't know how this distribution is performed right now.

PHB: can understand how to appled linked notary logs -- up to the point when someone introduces the use of bitcoin. Proposing to return to simpler approach: Doing the SIDR by simply having ARIN and all other RIRs publish, daily, a list of all the allocation they have made that day, and the PKs and the blocks, including the hash of the day before. Would be more usable and simpler than RPKI today. If you got one hash chain and you link it to the others. Need to find ways to make chains immutable -- but not PoW.

Jordi: yes, we propose Proof-of-stake

Ekr: slide 24, PoS. Right now, IANA owns all IPv6 space (unallocated). I.e., IANA control consensus per PoS.

Jordi: yes

Ekr: how do you get past that problem?

Jordi: can trust IANA, and would not hold space for long time

Ekr: it would for a long time

Jordi: yes, you are right. In IPv4, it would not be a problem.

Albert: this proposal is best understood in IPv4 where address space is more distributed. For IPv6, you could modify consensus algorithm to put more stake in allocated space.

Ekr: but IANA could just allocated space as it wants

Albert: yes, per PoS, you have to trust the entities that own most of the stake

Paul Hoffmann: (when IANA started allocating IPv6 addresses) IANA handed out space, but nothing has ever been returned. Maybe could think about new proof of stake concepts, like "Explicitly untrust IANA", i.e., don't allow the Uber-holder. But then you would incentivize people to get more space from IANA. One other thought: come up with completely different approach for Proof-of-Stake. "Who do you trust and how do you design the PoS accordingly." This could be one the research questions for an IRTF activity. Not easy, but possible. Will most likely be a single-purpose solution.

Albert: yes, correct -- we would like to investigate new consensus mechanism that make sense for the use case and the trust model at hand. This is just a proposal.

Michael McCool: what if you weighted the stakes wrt how recently they were allocated?

Jordi: could create some skew, I think

Michael: because then the value of a stake would decay over time

Jordi: good point

Lightest Project Overview (Benno Overeinder): http://lightest.eu/

Dmitry: what happens if you cannot access the resource?

Benno: no service

Dmitry: do you have a default trust model in these cases?

Benno: haven't discuss it yet. That's also a problem in other systems such as payment systems.

Breaking out of the cloud: Local trust management and rendezvous in NDN (Lixia Zhang)

Paper: https://named-data.net/publications/ndn-breaking-out-of-cloud-iotdi-2017/

PHB: agree that we need to have cloud-independent IoT design. E.g., when IoT devices are tied to a cloud that goes away. Also, all the different IoT devices are siloed and outside of user control.

Lixia: see NIST NDN workshop: Van Jacobson talk (https://www.nist.gov/news-events/events/2016/05/workshop-named-data-networking)

Benno: In Lightest, we chose DNS (not blockchain) to avoid name conflicts. Any views?

Lixia: 1) There is a namespace that has a structure. 2) There is a trust structure (not necessarily overlapping). Conflicting names is all about who certified what name, and whether you trust one certifier more than another one.

N.N. (IETF-T-shirt): security updates in scope?

Lixia: NDN makes everything so simple, at least conceptually. Everything is a piece of data that is signed. Every piece of data is immutable.

Discussion of Next Steps (Dirk & Melinda)

Dirk: presenting last part of chairs' slides

Eve Schooler: limited to distributed ledger, or also open to trust management (without ledger)?

Dirk: Initially the idea was to figure out how ledger technologies could be applied to decentralize Internet Infrastructure -- we are open to discuss the scope here

Michael: should first define the problem. Could be around "centralized systems in the Internet can break". Should look into details and technologies such as distributed ledgers. Also ICN, web of trust. Should open it much broader than just ledgers. But first find the problem, before.

Carsten Bormann: talks today were about signed data. Also important: understanding what data means, e.g., in Data exchange (i.e, security information). This is much easier in a centralized design than in a decentralized design. Also, everything evolves. Meaning of data that is being exchanged and signed can change or at least evolve and lead to additional semantic interop problems. Not sure what it means, but it's really interesting.

PHB: wrote a draft about trust model for PRISM-proof e-mail system. Showing that you can combine PGP and S/MIME trust ideas. Introduced concept of
work-factor for PKI. Haven't discussed fingerprints (of data). Fingerprint of digital signature key - could be used for establishing trust in dynamic website. These mechanisms could be used in distributed infrastructure and could be discussed here.

Andrew Sullivan: 1) Agree that there is interesting research to do here. not happy with term "distributed Internet Infrastructure" -- many things going on, like "distributed management", "distributed policy". Should tease these apart would be a good thing to do for an RG.
2) Other communities to reach out to could be economics, business school academics. There is a big incentive in current IoT model that did not come up: all the VC want to control who is signed up for this thing, so they want a unified stack. Trying to move to a decentralized model could be a serious, interesting problem.

Erik: many different approaches -- have their different pros and cons, e.g., blockchain. We could have a group to tease out the benefits of different approaches, so that we can apply the right technologies to the right problems.

Lixia: would agree that trust is fundamental issue. Fundamental thing: tech development to show how things can be made to work. Understand that blockchain is interesting, but group should have a broader agenda.

PHB: I don’t want to distribute control. I want to centralized control to what belongs to me. “User-centric control” of IoT.

PHB: Regarding updates in IoT: sometimes you don’t want cloud connectivity of your industry network to take over control. Applies also to home IoT gear.

Eve: formalizing trust models. Why not use trust anchors in the cloud when you can, but do not depend on them (i.e., use something else in these cases). Idea: different scopes of control to strengthen trust-worthiness

Erik Nordmark: Question is “who controls the policy”. centralizing things: user-centric control does not need to imply centralized services. Being able to separate out that aspect would be useful.

Edgar Ramos: Additional comment on use cases: for example, connectivity-challenged networks -- also other aspects than security/trust become important: what to prioritize when you get connectivity, so efficiency and privacy would also be important

Allison: need to have something that distinguishes this against other stuff within in the context in this community. This should be considered for the discussion as well.

Dirk: show of hands: who would show up at future meetings? Many

Dirk: show of hands; who would be willing to contribute: Many

Dirk: next steps: develop charter-like description before next IETF.