SDC 20

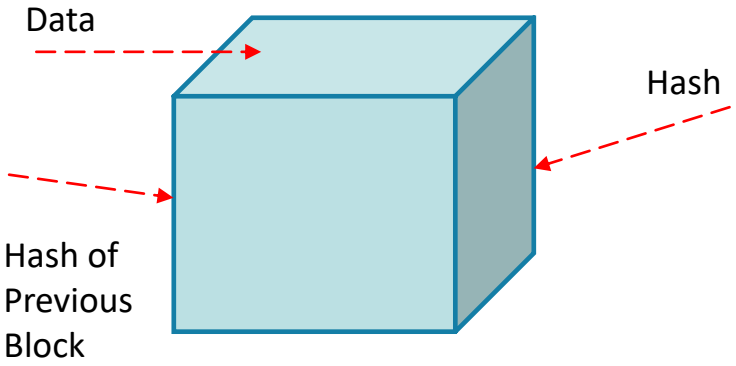
BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

Blockchain in Storage Applications

ActionSpot
Andrey Verbitsky
Olga Buchonina

WHAT IS BLOCKCHAIN?



- Blockchain is a distributed database of records stored in blocks.
- Blockchain is secured using peer validation in cryptography.
- Blockchain as a technology has several facets that directly or indirectly can impact user depending on implementation.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Blockchain, Hash and Consensus protocol

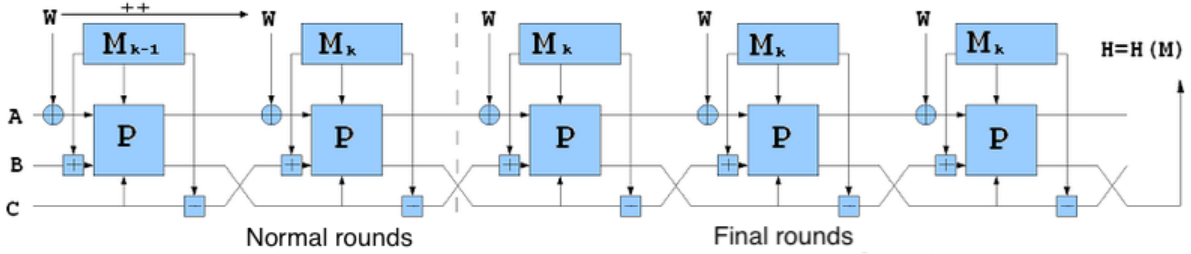
- Blockchain can use different cryptographic hash algorithms such as SHA-256 (one of the most popular), Whirpool, RIPEMD (RACE Integrity Primitives Evaluation Message Digest), Dagger-Hashimoto and others).
  - Mercle tree is a blockchain construct which allows to build a chain by using hashes and data blocks.
- Consensus protocols is protocol for decision making such as Proof of Work, Proof of Space, Proof of Stake and etc. Each consensus protocol is using the distributed ledger to make a record for the block of data transferred.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Blockchain in Storage Applications Today

WHAT IS PROOF OF CAPACITY

- Proof of Capacity uses the outputs of the shabal-256 cryptographic function to validate capacity to be used in mining.
- Shabal-256 currently is ASIC-resistant due to the IO requirements (as it requires writes).
- One time hashing process(plotting) versus continuous hashing.
- Mining process only involves reading the plots every new block(~ 4 min. average) and submitting the answers plus deadline(time to read to actual nonce).
- Power requirements for reading the plots greatly reduce overall energy consumed by the burstcoin blockchain.



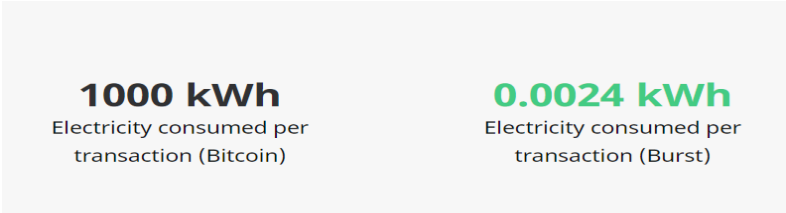
Shabal Algorithm

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

PROOF OF SPACE

- **Proof of space** (**PoSpace**), also called **Proof-of-capacity** (**PoC**), is a means of showing that one has a legitimate interest in a service (such as sending an email) by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.
- Proof of space are very similar to proof of work, except that instead of computation, storage is used. Proof-of-space is related to, but also considerably different from, memory-hard functions and proofs of retrievability.
- After the release of Bitcoin, alternatives to its PoW mining mechanism were researched and PoSpace was studied in the context of cryptocurrencies.
- Proofs of space are seen as a fairer and greener alternative due to the general-purpose nature of storage and the lower energy cost required by storage.

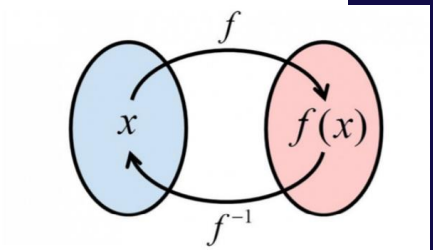
  - Example : BurstCoin vs Bitcoin

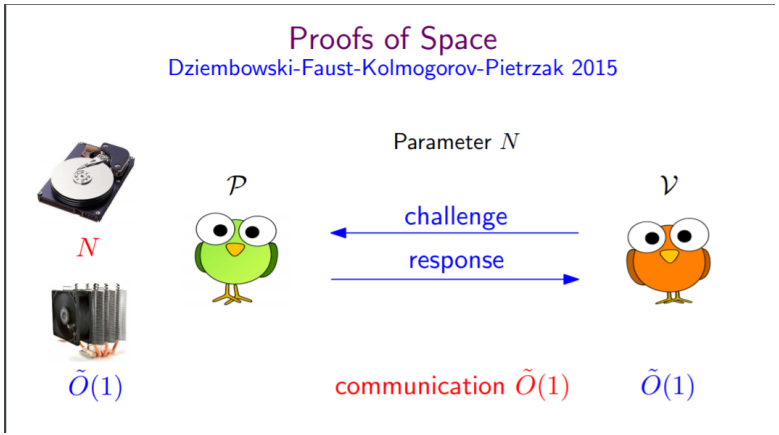


2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

HOW IT WORKS - PROOF OF SPACE ?

- A proof-of-space is a piece of data that a prover sends to a verifier to prove that the prover has reserved a certain amount of space.
- For practicality, the verification process needs to be efficient, namely, consume a small amount of space and time.
- For soundness, it should be hard for the prover to pass the verification if it does not actually reserve the claimed amount of space.
- Way to implement:
  - One way of implementing PoSpace is by using hard-to-pebble graphs.
  - The verifier asks the prover to build a labeling of a hard-to-pebble graph.
  - The prover commits to the labeling.
  - The verifier then asks the prover to open several random locations in the commitment.



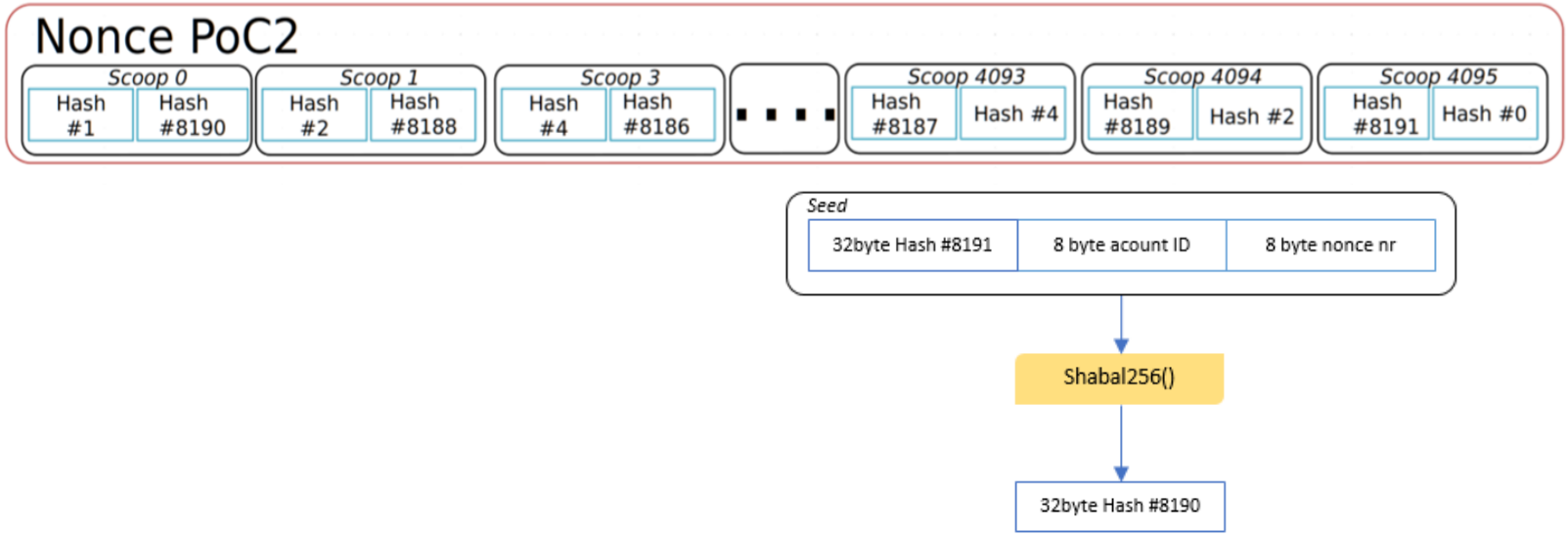


Krzysztof Pietrzak presenting at IST Austria
https://spotniq.files.wordpress.com/2018/08/spotniqbertinoro.pdf

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

BLOCKCHAIN AND PROOF OF CAPACITY

- Plotting is the process of generating plot files, which are just files storing a large number of pre-computed hashes. Each *plot* file contains one of more groups of 8192 hashes, these groups are called *nonces.* A nonce is exactly 256KB in size (8192 x 32 bytes per hash). Additionally, each nonce is divided into 4096 pairs of hashes, the pairs are referred to as *scoops*. Each nonce can also be identified by its index number, ranging from 0 to 2^64.

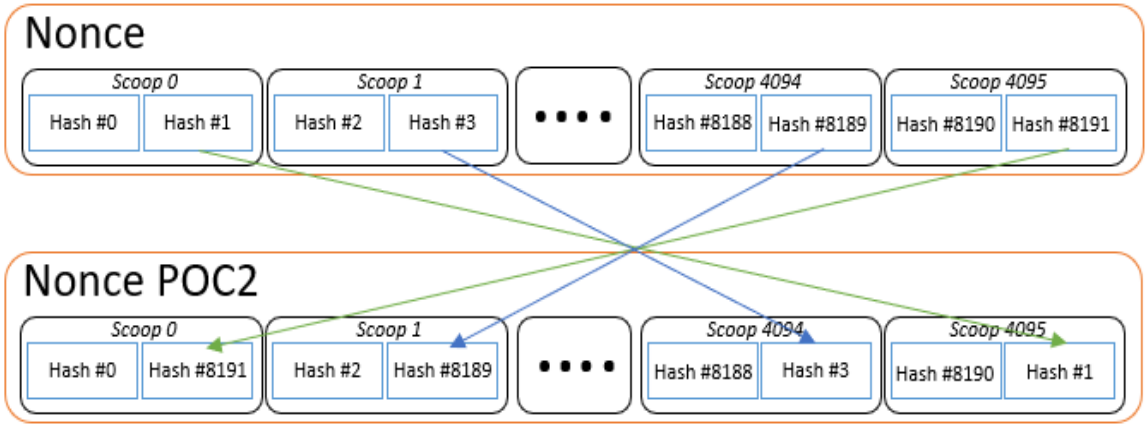


2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

POC2

The POC2 nonce format is created the same way as when we create POC1 with a slight addition to the end of the process. To create a POC2 formatted nonce we need to shuffle the data around. If we divide the nonce in 2 halves we get a range with scoops 0-2047 and 2048-4095. Let's call 0-2047 the low scoop range and 2048-4095 the high scoop range. To shuffle the data into correct place we take the second hash from a scoop in the low range and swap it with the second hash in its mirror scoop found in the high range. The mirror scoop is calculated like this:

MirrorScoop = 4095 – CurrentScoop



2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Burstcoin

- Burstcoin was the first cryptocurrency to use the proof-of-capacity algorithm. (2014)
- Burstcoin was the first cryptocurrency to implement working, "Turing complete" smart contracts in a live environment in the form of *Automated Transactions* (AT), this occurred before both Ethereum and Counterparty.
- Burstcoin's ATs include decentralized crowdfunding.
- Atomic cross-chain transactions (ACCT), a more recent innovation by Burstcoin and Qora allows for full decentralized trading between two cryptocurrencies without the need for any third-parties such as online exchanges.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Burstcoin

- Burstcoin is an open-source decentralized blockchain that connects individuals, businesses, and financial institutions.
- Burstcoin allows everyday individuals to begin plotting and mining in their empty hard drive space.
- Due to the ease of mining there are currently individuals mining in various parts of the world.
- We have a wide range of businesses currently interacting with the Burstcoin Blockchain in many capacities, payments, renting out solar mining space, building mining systems or solutions to provide extra transparency for their day to day operations.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

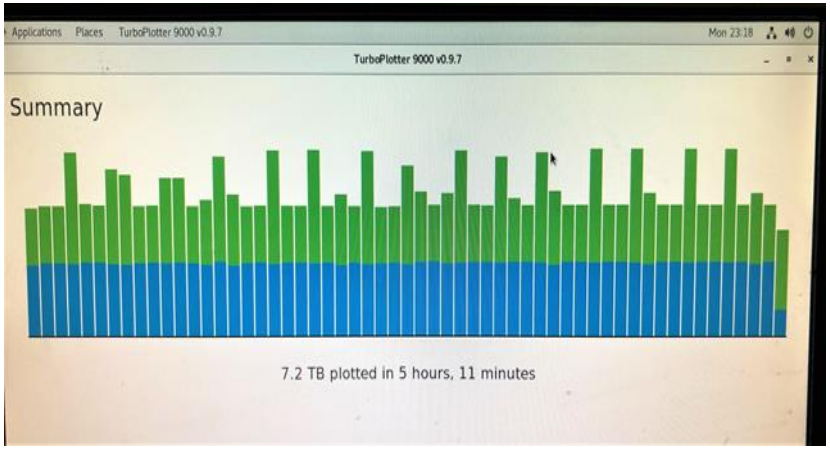
Burstcoin

- Users are able to mine Solo (standalone) or in Pools (with other miners).
- A solo miner submits to the network directly through their node without going into a pool.
- There are different types of pools based on what the pool operator wishes to run, miners then choose the pools that are more appealing to them.
- Some of these pools use a portion of their proceeds for additional projects or fundraising.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Examples of Plotting and Mining with Western Digital

Plotting



2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Decentralized concept can be effectively utilized in NVMe

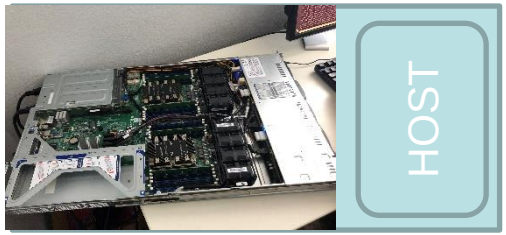
Architectural decentralization
Political decentralization
Logical Decentralization

Advantages	Disadvanges
Fault tolerance	Lack of Focus – too many decision makers
Attack resistance	Speed of Action
Collusion Resistance	Duplication of Work

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Building Blockchain using NVMe and NVMe-oF end to end solutions

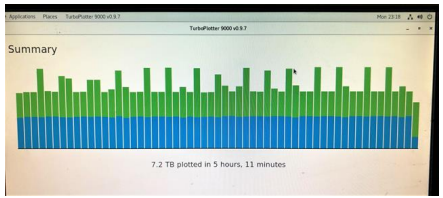
The architecture and setup for Blockchain Proof of Capacity Miner



NVMe-oF

NVMe Devices

Plotting – MEM WRITES



PoC Miners
(Scavenger for Burst)

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Why create common specification for Blockchain

What needs to be addressed

- Scalability issues
- Transaction cost issues
- Interoperability & adoption issues
- Special case of rights transfer

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Why we do not want a concept of a Single “Chain”

- Only participants do really care about the particular transaction
- Different countries and companies would like to keep some information private (or “data behind the walls”)
- 90% of data in a chain will become obsolete really fast
- With a single chain we have extreme restrictions on the size of the chain

Having a single chain creates unsolvable scalability and performance problems and incurs the risk of fork

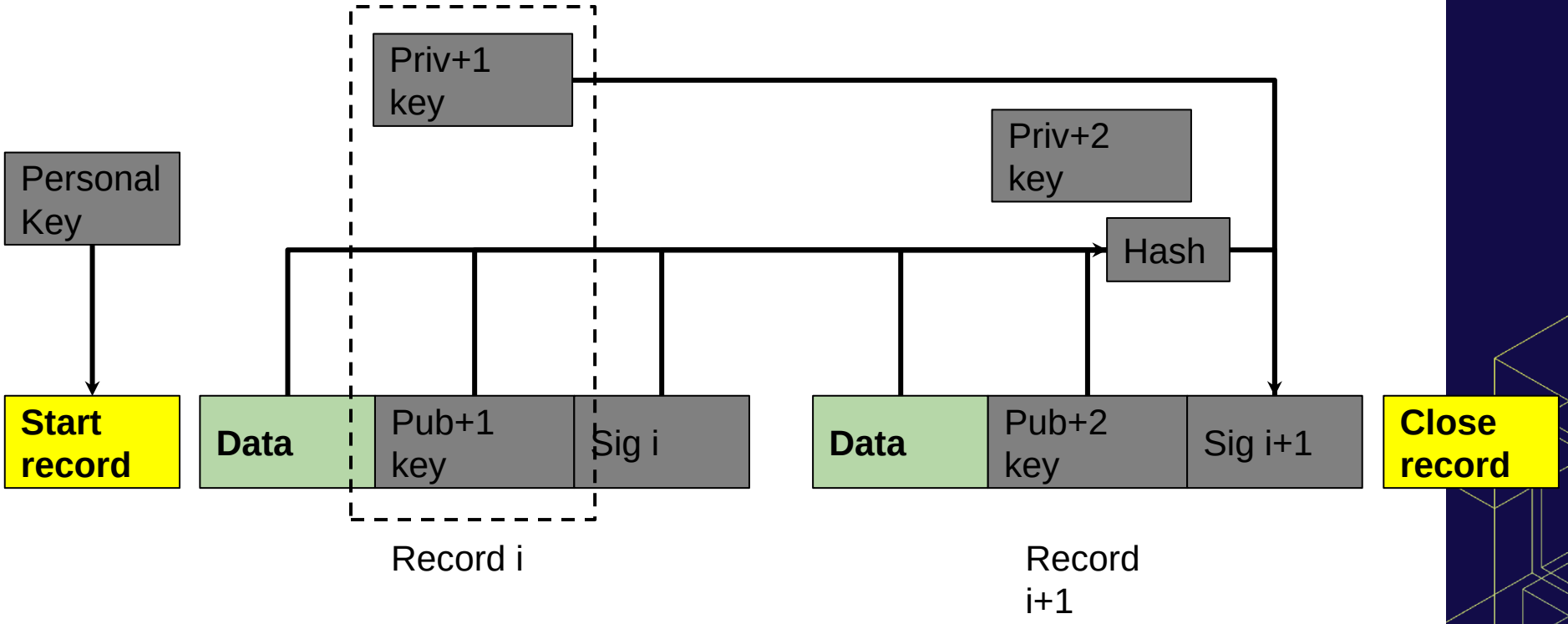
2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Solution: Multiple Chains

- Having multiple chains we can focus only on an active chains with actual data
- With multiple chains we can easily implement sharding
- With multiple chains we can implement “private chains” and “public chains” with different level of visibility

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Chain Integrity



Each new record is created using private key associated with the public key from the previous block

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Is “Traditional” Consensus on 0 Level viable solution?

- It is too expensive for low-value small transactions (like IoT)
- It works well only for “simple accounting tasks” and it is useless for unstructured data (how can nodes “agree” on a medical report?)
- It is required only if the potential harm of transaction is bigger the cost of its verification

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

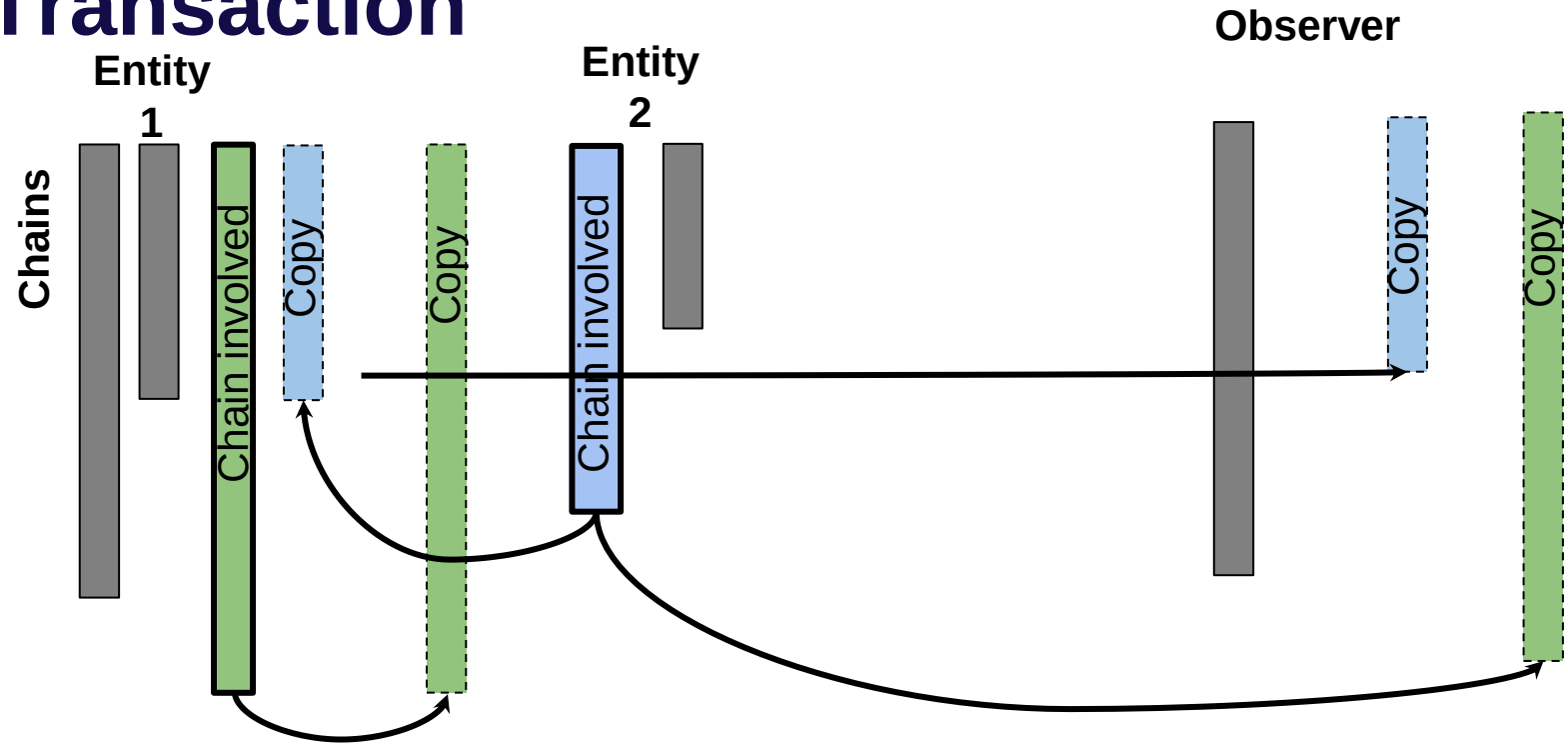
Solution: Chain That Can Work Without Consensus

- Any chain represents a personal record of “statements” of a single entity (no consensus required to add a new record to your own “book”), where the initial record is signed with personal private key
- Transactions between multiple entities will use data from chains from all this entities (and may even create cross-links between ledgers)
- Any entity can have a copy of a chain from any other entity

Identity of the chain is crucial - we can trust data in a chain as long as we can trust the issuer of the data

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Example: Two Entities Execute Transaction



Participants in a transaction observe & copy (stream) the relevant chains (and the data inside) from other participants

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Security of Private Keys is not always optimal for user

We cannot count on people's abilities to keep multiple passwords in mind

Like with passwords and credit cards they will be eventually compromised

The more people will use private keys the more the risk of them being compromised

Real-world transactions that include out-of-chain actions would require to know the identity of participants

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Solution: Focus on Preventing The Harm

Like with credit cards we need to focus on minimizing the potential harm from compromised keys by “blocking” them from modifying the chain

Like with credit cards (or security certificates), we need to have “proof of identity” of owner” and a mechanism to issue a new one keys automatically

Policy can enforce issuing new keys on a regular base

Deals that include out-of-chain actions would require to know the identity of participants

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Private Protocols Are Bad For Adoption

Private protocols leads to “standards wars”

Real businesses trying to avoid “vendor lock in” for business-critical operations

Like telecommunications, the biggest value of blockchain is in interoperability

We need to make sure, that all participants would feel safe - vendors, businesses, regulators etc.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Solution: Open Sourcing

We need to open source protocol/signaling (aka “common language”)

We need to open source network/node architecture & API (aka “blueprint”, building blocks)

We need to open source leger structure

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Special Case - Rights Transfer

One of the most common cases is transfer the rights (ownership, usage, etc.) from one entity to the other.

Different assets (money, shares, objects etc.) require different logic to be transferred from one owner to the other, but all of them require proof of issue and ownership.

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

Solution: Protocol Extension

A special protocol extension that will accomodate the logic of rights transfer, compliance, ownership and authenticity check and will create a full history of ownership

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

What Are Our Assumptions?

We don’t need “traditional” consensus

We don’t need a single “chain”

We don’t have to worry about protection of personal private key

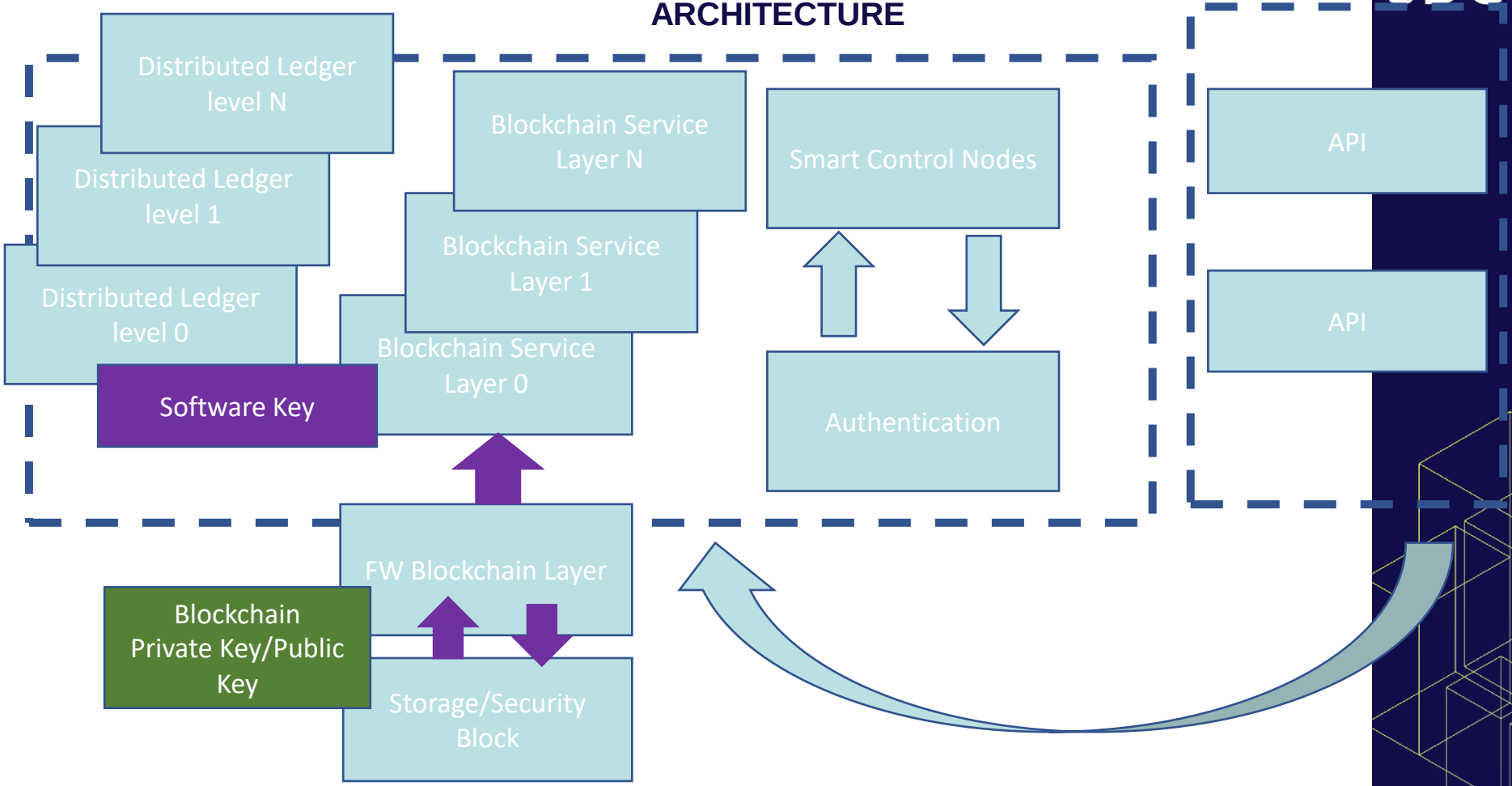
We need to protect chain integrity

We need to accommodate complexity of the real world

We need to open source key elements

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

PROPOSED BLOCKHAIN INTEROPERABILITY ARCHITECTURE



2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

HOW TO GET INVOLVED?

JOIN SNIA AND Technical Blockchain Group

CONTACT :

membership@snia.org

or olga@myactionspot.com

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.

QUESTIONS?

2020 Storage Developer Conference. © Insert Your Company Name. All Rights Reserved.