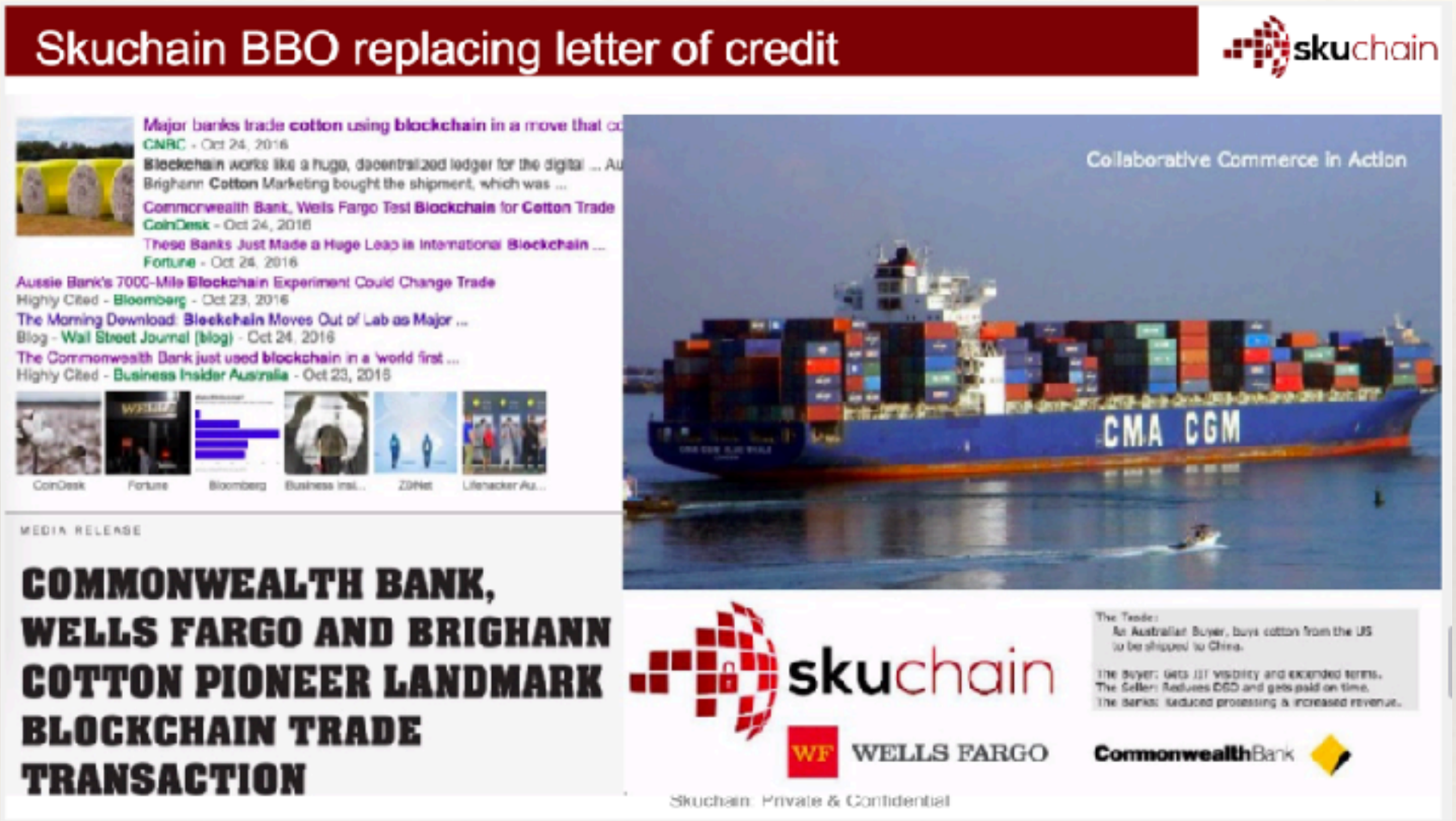
Fabric as a research platform

A Blockchain of Opaque Blobs
For BPASE Stanford Jan 2017

Intro:

- Zaki Manian
- Cofounder of Skuchain
- Skuchain has users in Banking, Industrial and Trade Finance world.
- I’m in the business of appropriating cryptocurrency technologies for other ends

The Value Proposition of an Authoritative Record



Fabric 1.0 as a Research Tool

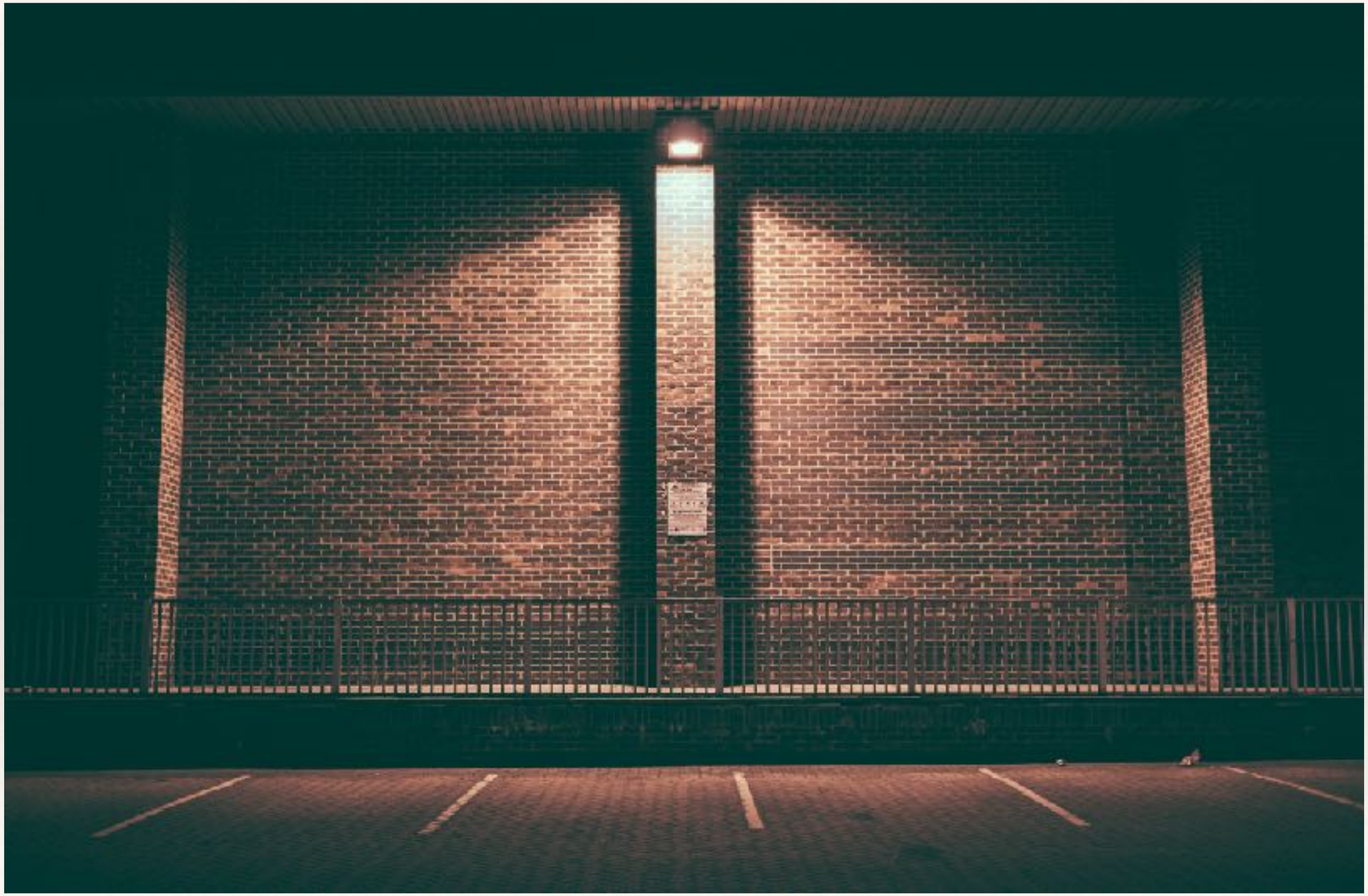
- In ~March, Fabric will ship their 1.0 architecture.
- This will be helpful for commercial users of their stack because it will broaden the deployment opportunities
- Argue that Fabric 1.0 could be a boon to academic community's ability explore what's possible, useful and interesting in blockchain model computing.

Blockchain Model of Computations

- A Total Order | Some kind of distributed consensus
- A Peer to Peer network
- Private and Public Computation Channels

FABRIC | QUORUM | ASSEMBLY and others follow this basic abstraction

Barriers to Entry



Reducing Barriers to Entry

- There is a high barrier to entry to experimental blockchain systems.
- Either deep expertise in an existing blockchain technology like Ethereum or Bitcoin is needed
- New systems need to built from the ground up.
- The ultimate cause is implicit dependencies between subsystems.

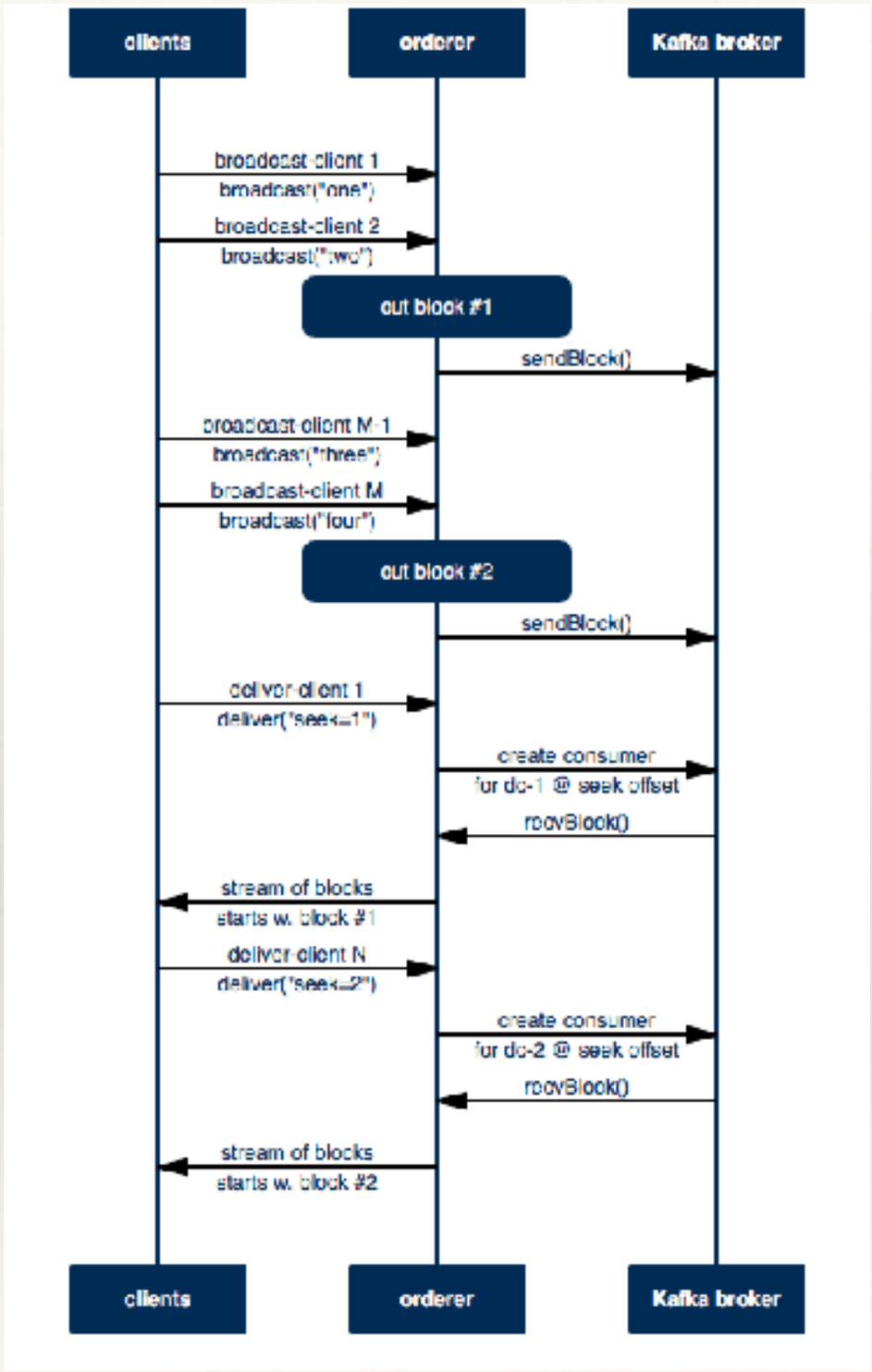
Opaque Blobs?

- Opaque in the sense that the daemon never deserializes the data upon which it's operating.
- The data is frequently encrypted.
- The opaque blob approach forces explicit dependencies between elements of the system.

Consensus

- The Consensus API for Fabric has 2 calls.
  - Submit Blob
  - Return a Block of Blobs at a given block height
- Consensus can provided by any system that can respond to these two APIs.

Fabric State Diagram



What might more Consensus Tech do?

- Larger more dynamic consensus groups are going to be interesting to for some Fabric applications
- But I'm going to admit, some fancy next-gen consensus tech is going to have more impact in the public blockchain world than the enterprise in the next 3-5 years.
- But Fabric will get you a working Proof of Concept pretty fast vs right now white paper to something useful is about 2-3 years.

Chaincode

- Chaincode are the transaction processing engines.
- They execute agreed upon business logic
  - They are excellent for agreeing on and executing on on shared data.
- Fundamentally, chaincode transformer a user provided blob of bytes and the current state of a merkle tree into a new state of the merkle tree

Chaincode Properties

- Who is the admin here?
- BFT guarantees of immutability and liveness
- The net result is an authoritative information utility.

Do We need Cryptography in Chaincode

- Fabric already contains a sophisticated PKI system. See Jonathan and David's talk
- The cryptographic attributes from this system are available within the business logic of chaincode
- Do we need anything more?

Business Logic + extended Cryptography

- Business Logic can be attached to arbitrary credentials
- Signatures, SNARKS, oblivious Bloom filters…
- Computations are strongly ordered by the total ordering systems
- Why?

Peers are not the real users

- A neutral multilateral authoritative platform enforces cryptographic computation
- Delegate authority all the way to end users, hardware devices
- The end users of the system shouldn't have to fully transfer their privacy interests to peers.
- Private channels are just part of the needed toolkit

Problems I'm thinking about

- Predicate systems where all possible signers are not enumerated when the predicate is specified but are replay resistant.

- Signature systems for partial and redacted time series data records.

What's Fabric Got to Offer

- Ready access to cryptography libraries in existing language.
- Simple integration paths
- What I'm hoping we will see:
  - Protocols, rules and languages for credentials in blockchain computation
  - A structured way of thinking about what is secure in this setting

Conclusions

- Fabric has minimized implicit dependencies between components
- This makes it easier to do certain kinds of experiments in Blockchain applications
- The results of these experiments are useful in commercial applications

FIN