Blockchain Revealed: Why so mysterious?
SMPTE Technology Webcast Sponsors

- Thank you to our sponsor for their generous support:

[Image of AJA Video Systems]

SMPTE Technology Webcasts

- Series of monthly 60- to 90-minute online, interactive webcasts covering a variety of technical topics
- Free professional development benefit for SMPTE members
- Sessions are recorded for member viewing convenience.
Views and opinions expressed during this SMPTE Webcast are those of the presenter(s) and do not necessarily reflect those of SMPTE or SMPTE Members.

This webcast is presented for informational purposes only. Any reference to specific companies, products or services does not represent promotion, recommendation, or endorsement by SMPTE.

Your Host

Joel E. Welch

Director of Education
SMPTE
Today’s Guest Speaker

Marc Zorn
Head of productions and content cybersecurity
HBO

What is a blockchain?

A sequence of datablocks that have been hashed, then linked by using summary hash as starter for next block

An analogy would be connecting pop beads together
The block in simplest form

The chain in simplest form

Connecting blocks using previous summary hash as starter
Hashing

- Hashing is the generation of a value or values from a string of text using a mathematical function.
- Secure Hashing Algorithm – Family 2 (SHA-2) is the method used for Bitcoin and many other applications.
- SHA-224, SHA-256, SHA-384, and SHA-512 are all SHA-2 with different bit lengths for strength or complexity.

Why do some call it a ledger?
How does Bitcoin work?

The Anatomy of a Transaction

Timestamp Servers

(Creating timestamped hashes)
Nonce (or \( n \)-once)

- A number created for a single use or purpose
- A Nonce for cryptocurrency is used as supplemental input to cause the resultant hash value to fit the target format

**Difficulty Target**
Calculating nonce and creating a coin

- Calculate nonce to make summary hash fit the target format (i.e., Eight leading zeroes in SHA-256 hash)
- Finished block has all required transactions (including fee or new coin)
- Creation of stub header block with new timestamp and target
Examining Merkle Roots

Verifying blocks using hashes only

Proof-of-work, Nonce, Acceptance Calculation, and Next Block
Participation Incentive

- One of the transactions in the queue is the “fee”
- Miner countersigns the “fee” (claiming it) and calculates Nonce
- Nobody else can use “fee” once transaction is in the ledger
- MINE! MINE! MINE!

Networking and Transaction Contention

How do you decide who gets the credit (and the reward?)
Anonymity

Trusted third-party vs stand-alone identities

How does Bitcoin work?

The recipe and procedure
1. Start with next stub block
2. Gather requested transactions
3. Add fee or new coin transaction
4. Calculate nonce
5. Check for ledger updates
6. Create next stub block
7. Publish finished block and stub to ledger
8. Add reward to your electronic wallet
Is the Bitcoin framework of blockchain a good fit for M&E?

• Difficulty target / nonce – severe performance limitation
• Rewards – Is it necessary?
• One-way transactions – Requires analysis
• Public ledger – Possible advantage for communications
• Timestamp servers – Necessary for some logistics
• Networking and transaction contention – Artifact of broadcasting
• Anonymity – Think hard before giving up ID control
What about using Ethereum or another existing framework?

- Thoroughly understand framework before doing analysis
- Most existing frameworks have similar drawbacks or limitations
- Does the framework already fit your use case?
- Why are we afraid to build our own framework?
- Why not build a new framework for each use case or project?
- Build in only those components that are necessary
- Use security strength to fit exposure
- Streamline for best performance and flexibility
- Destroy it when the project concludes

What components might we need for M&E?

Build framework for use case not for convenience or economy of scale

- Hashing (perhaps not always SHA-2, MD5, or others)
- FederatedID (decentralized digital certificates)
- C4 workflows
- Industry standard formats (i.e., ST-2110, IMF, camera RAW)
- Best-fit Encryption
- Published trust relationships – perhaps by project certificate authority
- Establish rules of transactions for specific activities
- What else is needed to facilitate specific case?
Example Use Case: Movement and tracking of digital assets?

- treatments / scripts
- Contracts
- Schedules
- Set / location information
- shot lists
- production metadata
- production material
- transportation logistics
- Dailies
- image/sound data
- color / calibration data
- CDLS
- media metadata
- work assignments
- VFX assets
- sound files
- EDLS
- subtitles/captions
- language/versioning
- mezz data
- distribution data
- watermarking / DRM / security metadata
- marketing data
- credits / royalties
- box office data
- archive metadata

Other Candidate Use Cases

- Open bidding of work from “transaction queue”
- Smart Contracts - digital agreements and auto-fulfillment
- Communication mechanism with blockchain for stream integrity
- Down-stream transcoding
- Distribution methods with feedback of ownership and DRM / digital fingerprinting
- New types of purchase and payment systems, like digital tool rental or licensing
- Viral content – “Bitmedia”? “Mediacoin”?
- New and non-traditional use cases we haven’t thought of yet
What advantages does blockchain provide that other methods or technologies don’t?

Higher performance?  Simpler implementation in public space?
Lower cost?  Based on accepted standards?
New encryption methods?  Promotes competition?
Decentralized security?  Democratized playing field?
New ways of collaborating?

The big question: Do we need blockchain for this kind of activity?

Can we address case by using more established components (i.e., DAM)
Do we need centralized or decentralized management?
Do we need anonymity, FederatedID, or central authority?
Do we need object storage or other cloud-based resources?
Do we need to create a new distribution mechanism?
Do we understand the required data flow patterns?
Do we have multiple contributors for the same work?
What needs to be public, semi-private, or tightly-controlled?
Can blockchain solve any or all of these requirements?
This solution is based on blockchain because...?

If the only tool you have is a hammer, you tend to see every problem as a nail.

Abraham Maslow

Questions & Discussion
(Oral) Questions?

Marc Zorn
Head of productions and content cybersecurity
HBO

SMPTE Technology Webcast Sponsors

• Thank you to our sponsor for their generous support:

AJA VIDEO SYSTEMS