Blockchain Basics

John Lindsay

Blockchain: Peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updated by consensus among peer nodes.
Blockchain Basics

- Various blockchain based technologies and problem that they solve
  - Bitcoin (decentralized currency)
  - Ethereum (highly decentralized currency, Turing complete scripting language)
    - “Smart Contracts”
- Applications
  - Toll tag logging and payment
  - Smart City sensor data sharing in Singapore
  - Sexual consent logging
  - Walmart – supply chain tracking
Blockchain Basics

• Loose Plan
  – 1st Presentation - Blockchain Basics
    • Mile wide/inch deep
    • At least not wholly conflate Bitcoin and Blockchain
  – 2nd Presentation - Ethereum overview
    • Overview of Ethereum, “Smart Contracts,”
  – 3rd Presentation - Code along
    • Bring laptop and follow along
Blockchain Basics

• What is it?
  – Database (storage)
  – Distributed (across many nodes)
  – Immutable (extremely hard to change)

• What is a blockchain?
  – A series of linked blocks
  – Sequentially updated but not erased
  – Cryptographic hashes assure integrity of data

• What is a block?
  – A block with a (hash) pointer to a prior block

• Blockchain-ish permutations
  – Tangle (IOTA), Hashgraph, others
Blockchain Basics

- Various blockchain based technologies alter different aspects of:
  - Data
  - Distribution
  - Immutability

- Platform vs application (or hybrid)

- “Whitepapers” often address key questions:
  - Data
  - Distribution/Actors
  - Level of immutability
  - Interfaces/programming language
Blockchain Basics - Scenarios

- Bitcoin
  - Decentralized cryptocurrency
- Recording and settling toll tag transactions
  - Decreased toll infrastructure
- Smart City sensor array data access/exchange
  - Citizens access, entrepreneurs build upon
- Sexual consent logging/LegalFling
  - Sexual partners log consent to blockchain
Blockchain Basics - Data

• What is the data?
• It’s “just data” that would be stored in any database
  - Cryptocurrency transactions (signed transaction)
  - Toll tag number, toll gate, timestamp
  - Smart city data – sensor ID, sensor type, value, timestamp
  - Sexual consent – signature, audio/video, ???
Blockchain Basics

- Chain of “blocks”
- Block
  - Block number/index
  - Data
  - Hash/hash as pointer
- Immutability
- Demo (Data -> Hashes, -> Block -> Blockchain)
Blockchain Basics – Distribution & Immutability & Longest Chain

• Distributed/decentralized
  – Who are the actors? What is decentralized?
  – Extent of distribution/decentralization
    • Public vs permissioned
    – Anyone who has computation and/or storage resources?
  • “Mining” determines what is the next block in the blockchain
    – Incentive/reward for miners
      • By computing power (proof of work)
      • By rewards are proportional to the size of a user's holdings (proof of stake)
  – Lag in adding the block
Blockchain Basics – Distribution & Immutability & Longest Chain

- Immutability
  - Extent of immutability
  - Do we want 100% immutability?
    - Ethereum vs Ethereum classic
    - “Forks”
      - Who will the ecosystem actors follow?
- Demo (Multiple chains, consensus)
Blockchain Basics – Factors in Selection/Creation of a Blockchain

- Use Case? Simplicity/complexity?
- Who are the actors and what are their roles?
- What is the data? How much? How frequent?
- What interfaces are available?
- Do you need an existing ecosystem?
- What programming languages are available?
- What is the consensus mechanism for conflicts?
Blockchain Basics - Implementations

- Bitcoin – Use: Decentralized cryptocurrency
  - White papers – “Bitcoin: A Peer-to-Peer Electronic Cash System”
  - Platform vs application (Hybrid)
  - Data (signed bitcoin transactions)
  - Actors (bitcoin holders, miners)
  - Distribution (anyone can mine(*), anyone can own bitcoin)
  - Immutability (highest)
  - Interface (miners, “wallets”, “script”)
Blockchain Basics - Implementations

- Ethereum – Use: “Smart Contracts”
  - White papers – “A Next-Generation Smart Contract and Decentralized Application Platform”
  - Platform vs application (Platform)
  - Data (signed ethereum transactions, smart contracts, ...)
  - Actors (ethereum holders, parties to contracts, ...)
  - Distribution (anyone can mine(*), anyone can own bitcoin)
  - Immutability (high)
  - Interface (miners, “wallets”, “Smart Contract”, Solidity)
// Basic Block

class Block {
    constructor(blockIndex, data, previousBlockHash, timestamp = '') {
        this.blockIndex = blockIndex;
        this.previousBlockHash = previousBlockHash;
        this.timestamp = timestamp;
        this.data = data;
        this.hash = this.calculateHash();
    }

    calculateHash() {
        return SHA256(blockIndex + previousBlockHash + data + timestamp + ');
    }
}

Blockchain Basics – Pseudocode Walkthrough (the Blockchain)

```javascript
// Building the blockchain

class Blockchain{
    constructor() {
        this.chain = [this.createGenesisBlock()]; // special case
    }
    addBlock(newBlock) {
        newBlock.previousHash = this.getLatestBlock().hash;
        newBlock.hash = newBlock.calculateHash();
        this.chain.push(newBlock);
    }
    isChainValid() {
        // iterate through blocks from start to end,
        for (let i = 1; i < this.chain.length; i++){
            retrieve currentBlock
            retrieve previousBlock
            if (currentBlock.hash !== currentBlock.calculateHash()) {
                return false;
            }
            if (currentBlock.previousHash !== previousBlock.hash) {
                return false;
            }
        }
        return true;
    }
}
```
Blockchains Basics – Pseudocode Walkthrough (Usage)

1. `let johnCoin = new Blockchain();`
2. `johnCoin.addBlock(new Block(1, "20/07/2017", { amount: 4 }));`
3. `johnCoin.addBlock(new Block(2, "20/07/2017", { amount: 8 }));`
4. `// some stuff happens over time`
5. `console.log('Blockchain still valid: ', johnCoin.isChainValid());`
What can you bring to the table where IoT and blockchain truly add to world?

Questions?

John Lindsay
Patent Attorney
Coaster, Smooth Driver Application