Introduction to Blockchain Technology

Data Science Perspectives for Blockchains

Chris Williams – PURE Money Systems
Joe Blankenship - CGRII

Agenda

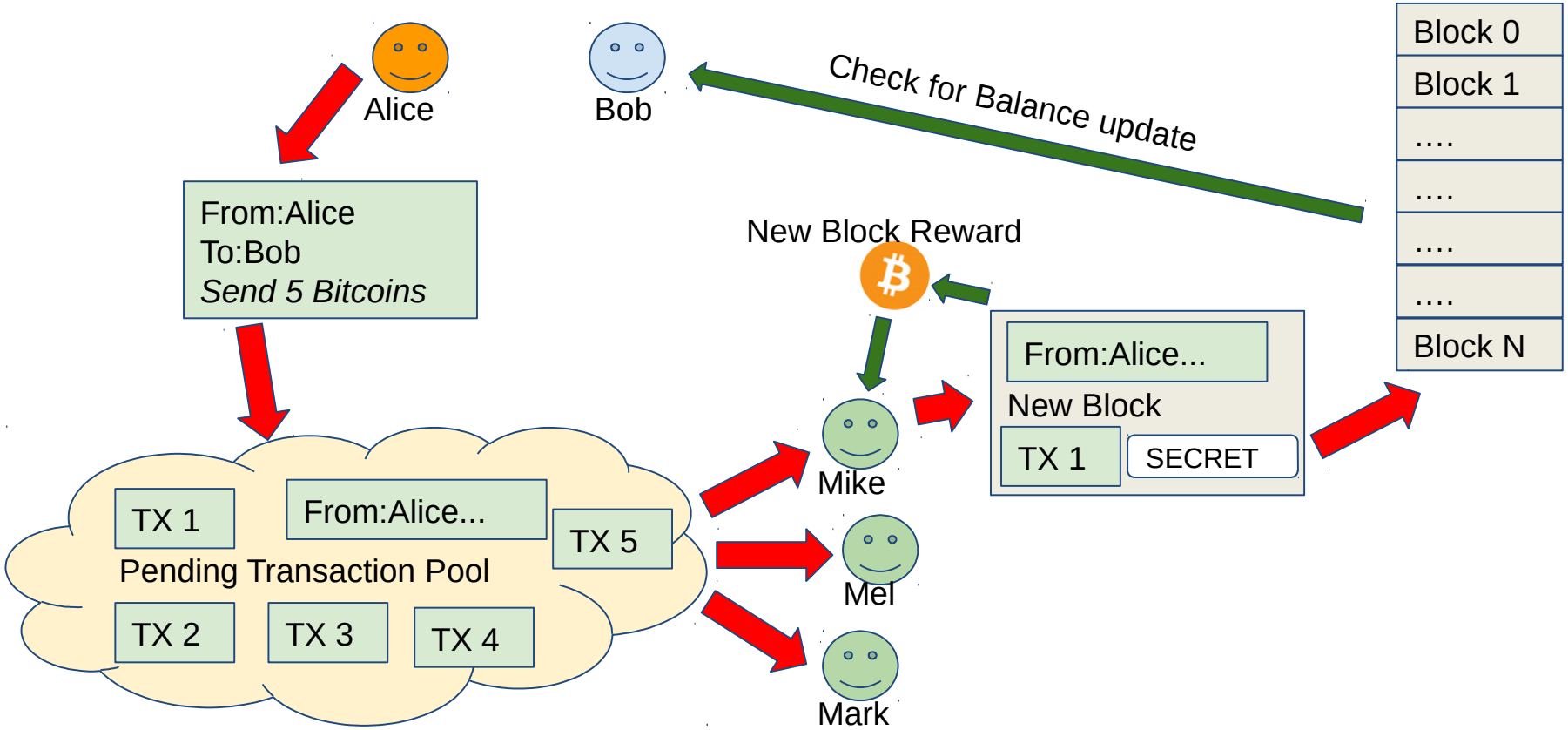
- Understand core concepts
- Major Projects
- Algorithms and Methodologies
- Implications
- Going Forward

Core Concepts

- **Blockchain**
  - a new type of database for storing transactions (series of blocks)
- **Miner**
  - a computer with special software that packages transactions into blocks to collect rewards
  - Proof of Work vs. Proof of Stake
- **Cryptofinance**
  - financial tasks guaranteed using strong cryptography
- **Cryptocurrency**
  - A currency system, secured by cryptography (keys, hashes)
- **Wallet**
  - Software on your computer storing private keys for your accounts
- **Smart Contract**
  - Code in accounts used to control transactions
- **DAO/DAC**
  - Decentralized Autonomous Organization/Corporation

Core Concepts

How the Blockchain works



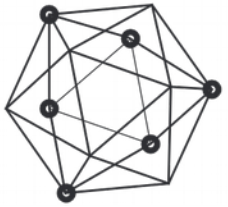
Major Projects

- **Bitcoin - the birth of the blockchain**
  - Created by “Satoshi Nakamoto” in 2008
  - Volunteer computer network for transferring Bitcoins
  - Maximum 21 mil Bitcoins, 15.7 Mil circulating today
  - Transactions occur directly between 2 people, no middle-men
  - All accounts, balances, and transactions are public
  - Transactions take 10 min. to finalize and are not reversible

Major Projects

- **Ethereum - the Smart Contract revolution**
  - Created by Vitalik Buterin in 2013 (first released in 2015)
  - The World Computer - compute, communication, storage, security
  - Smart contract code lives on the blockchain; users pay others to run the code
  - No maximum amount of Ether (ETH). Currently 83 Million circulating
  - Fast transaction confirmation times (~15 seconds)
  - Forked in Aug 2016 to reverse a hack; Ethereum Classic (ETC) retained the hack

Major Projects



- **HyperLedger - enterprise blockchains**
  - Multi-industry collaboration project started in 2015 by the Linux Foundation
  - Collaborators include every major financial institution and many tech companies
  - Private, permissioned blockchains for large companies, with arbitrary topologies
  - Intel’s blockchain project is called Sawtooth, targeting IoT (mobile, sensors, etc)
  - IBM’s blockchain project is called Fabric, targeting large enterprises
  - Developer tools are very mature, currently getting the most corporate interest

Major Projects

- **Open Transactions - blockchain gateways**
  - Created by Chris Odom in 2011 and released as open source
  - Currently being heavily developed by StashCrypto for voting pools
  - Client-Server architecture with no blockchain and no transaction history
  - Financial cryptography library for encryption, messaging, and balance tracking
  - Features anonymous digital cash, smart contracts, and custom asset types
  - Recommended usage as an exchange gateway, IoT clients,
  - mobile clients, disposable assets, and temporary tokens

Major Projects

	Namecoin	Censorship-resistant DNS	2011
	Litecoin	silver vs Bitcoin gold	2011
	Ripple	Near-free Paypal	2012
	Dash / Monero	Anonymous, instant transactions	2014
	CureCoin / GridCoin / PrimeCoin	Scientific Research	2014
	Steem / Synereo	Social media platform	2015
	MaidSafe	Distributed data and web apps	2016
CASH	ZCash	Private/selective transparency	2016

Algorithms and Methodologies

- **Hashing Algorithms**
  - SHA encryption
  - Merkle Tree Structures
- **Privacy Algorithms**
  - MIT OPAL/Enigma
- **Consensus/Governance Algorithms**
  - Bitcoin Protocol
  - Ethereum Protocol
  - Many others
- **Methodological Applications**
  - Sky’s the limit

Implications

- **Decentralization & distribution**
  - Political and economic balances → Power dynamics
- **Alternative Economies**
  - “Middle Men”
- **Speculation and Investment**
- **Cryptocurrency vs. Fiat vs. Credit**
  - Is it money? Is it capital?
- **Ethical Computation**

Going Forward

- **Within Existing Systems**
  - See Implications
- **In the future**
  - Distributed, anonymous, scam-resistant currency exchanges
  - Personal currencies backed by personal value (influenced by your actions, social networks, and biofeedback)
  - Infinite forms of money based on value systems
  - Corporations/Governments will be formalized through DAO governance (liquid democracy)
    - Individual forms of government participating in multiple micro-governance actions
  - “Micro-employment” where most work tasks are available to everyone and payment is based on results

Resources

- **Meetup.com**
  - https://www.meetup.com/Ethereum-Tampa/
  - https://www.meetup.com/Blockchain-Enthusiasts/
- **Facebook**
  - Ethereum Tampa - https://www.facebook.com/groups/446265188903009/
  - Tampa Bitcoineers - https://www.facebook.com/groups/206146076244552/
- **Github**
  - PURE Money Systems - https://github.com/PUREMoneySystems
  - CGRII - https://github.com/CGRII