

# Chaining the Future Blockchains and Security

Joe Blankenship  
[www.thejoeblankenship.com](http://www.thejoeblankenship.com)

# Agenda

Introduction to Blockchain

Key Players and Hacks

Future of Blockchain

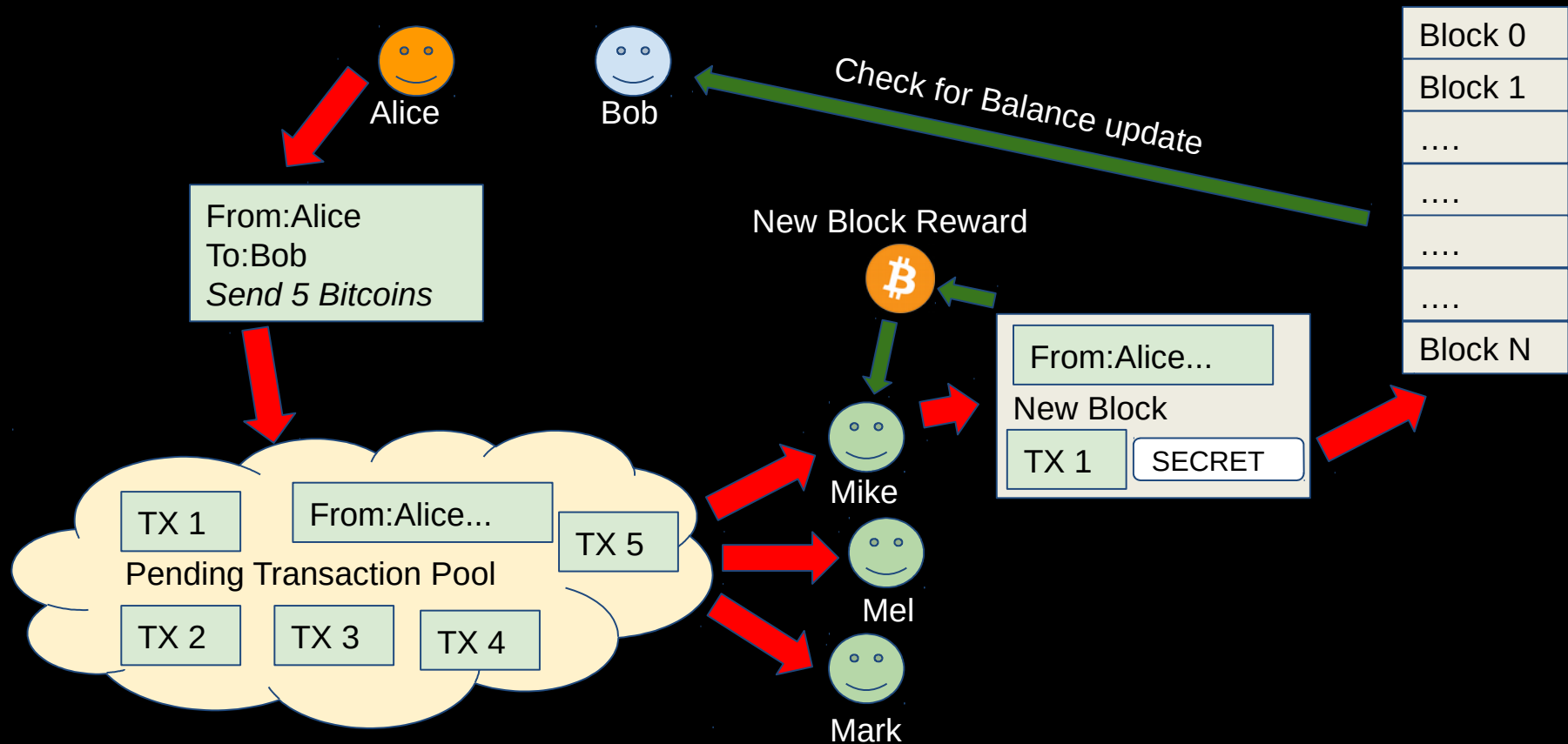
Questions

# Introduction

- 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

# Introduction

## How the Blockchain works



# Introduction

- 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

# Key Players and Hacks



- 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

# Key Players and Hacks



- 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

# Key Players and Hacks



- 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



# Key Players and Hacks



- 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

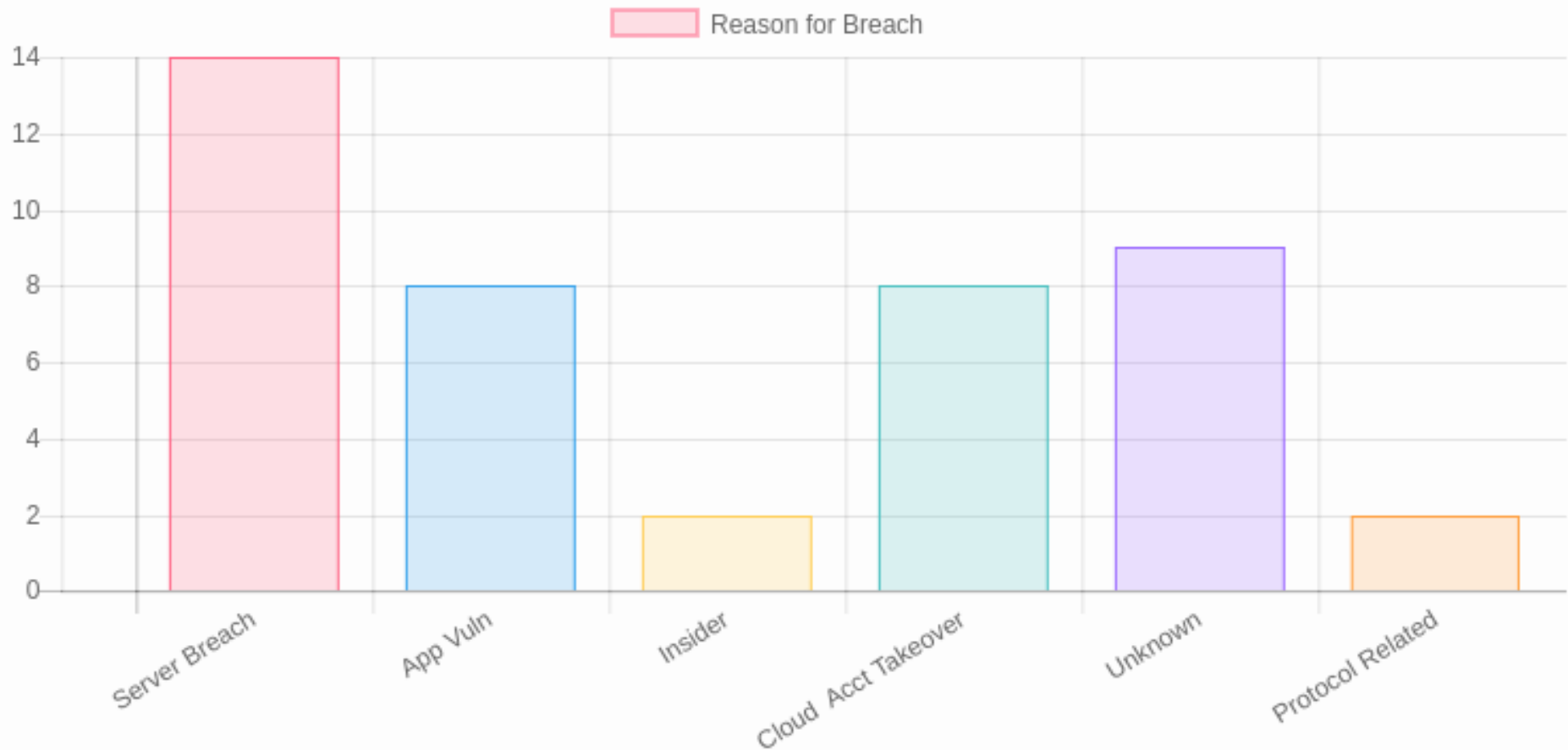
# Key Players and Hacks

	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
	ZCash	Private/selective transparency	2016

# Key Players and Hacks

## ROOT CAUSE ESTIMATES

The data below is roughly gleaned from publicly available data about **42** incidents.



# Key Players and Hacks

- 51% attack
- Recursive calling
- Hot wallets/Cold storage of keys
- API vulnerabilities
- Dependency backdoors
- Spear-phishing
- Embedded scripts (emailed docs)
- Admin access
  - Servers
  - Cloud infrastructure
- 3<sup>rd</sup> party plugins
- SQL Injection
- Man in the middle
  - Simultaneous requests
- DNS Hijack
- Stolen credentials

# Future of Blockchain

- Decentralization & distribution
  - Political and economic balances > Power dynamics
  - Corporations/Governments will be formalized through DAO governance
- Alternative Economies
  - “Middle Men” & Labor Dynamics
    - “Micro-employment”
  - Personal currencies backed by personal value
  - Patents, Intellectual Property
- Speculation and Investment
  - Distributed, anonymous, scam-resistant currency exchanges
- Cryptocurrency vs. Fiat vs. Credit
  - Is it money? Is it capital?
- Ethical Computation

# Future of Blockchain

- FinTech
  - Wall Street, HyperLedger, R3, Blockchain Alliance
- Data Storage & Record Keeping
  - IPFS, Storj, MaidSafe, Permacoin
- Voting/Legislation/Regulation
  - FollowMyVote, Estonia, Denmark
- Social Organization
  - Steem, Akasha
- Identity Protection
  - Dash, Monero, ZCash, BitNation, CryptID

# Questions

Thank you!

[www.thejoeblankenship.com](http://www.thejoeblankenship.com)