

Blockchains and Cryptocurrencies

Joe Blankenship

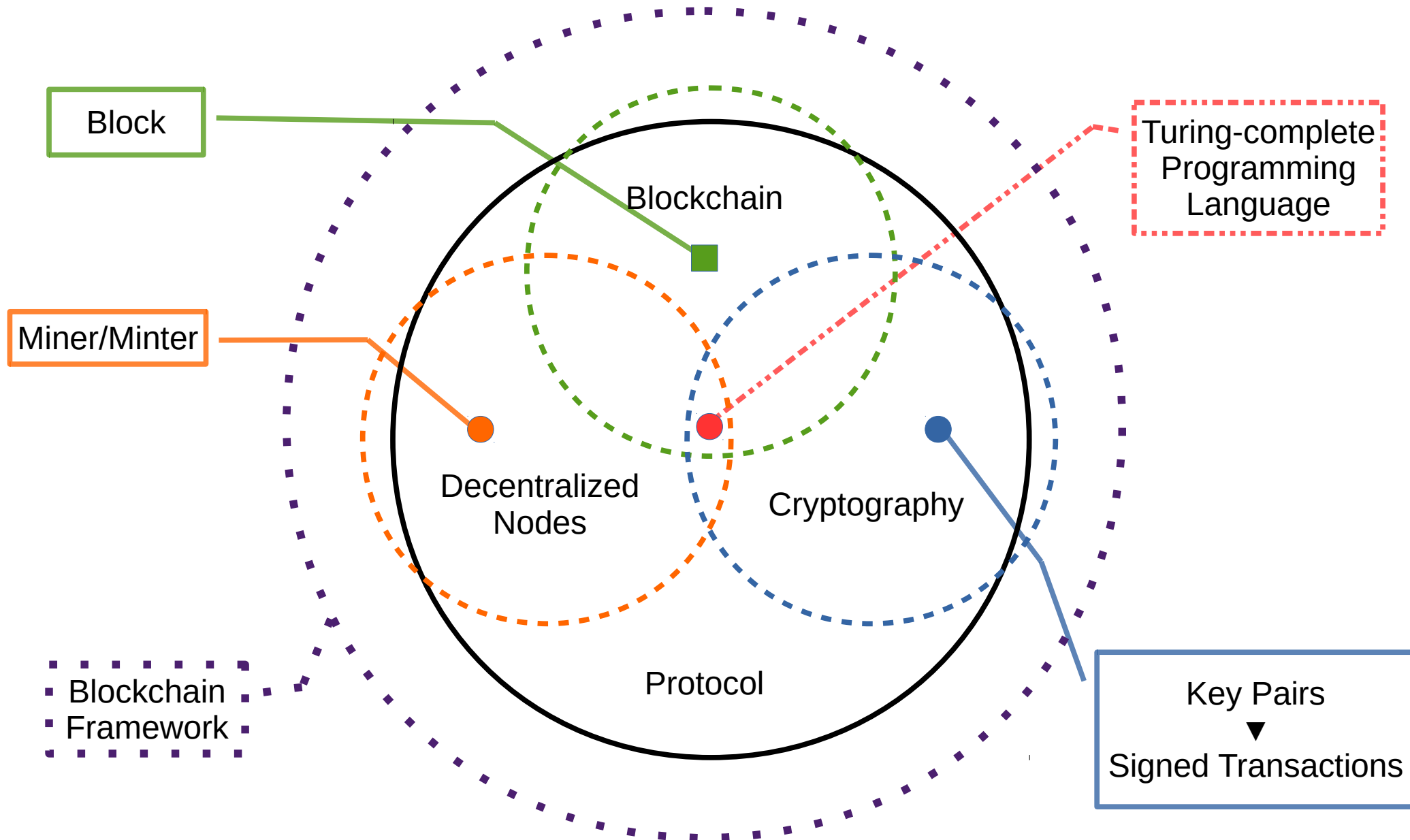
Lead Data Scientist, CGRII
www.thejoeblankenship.com

On behalf of Wyrd Solutions

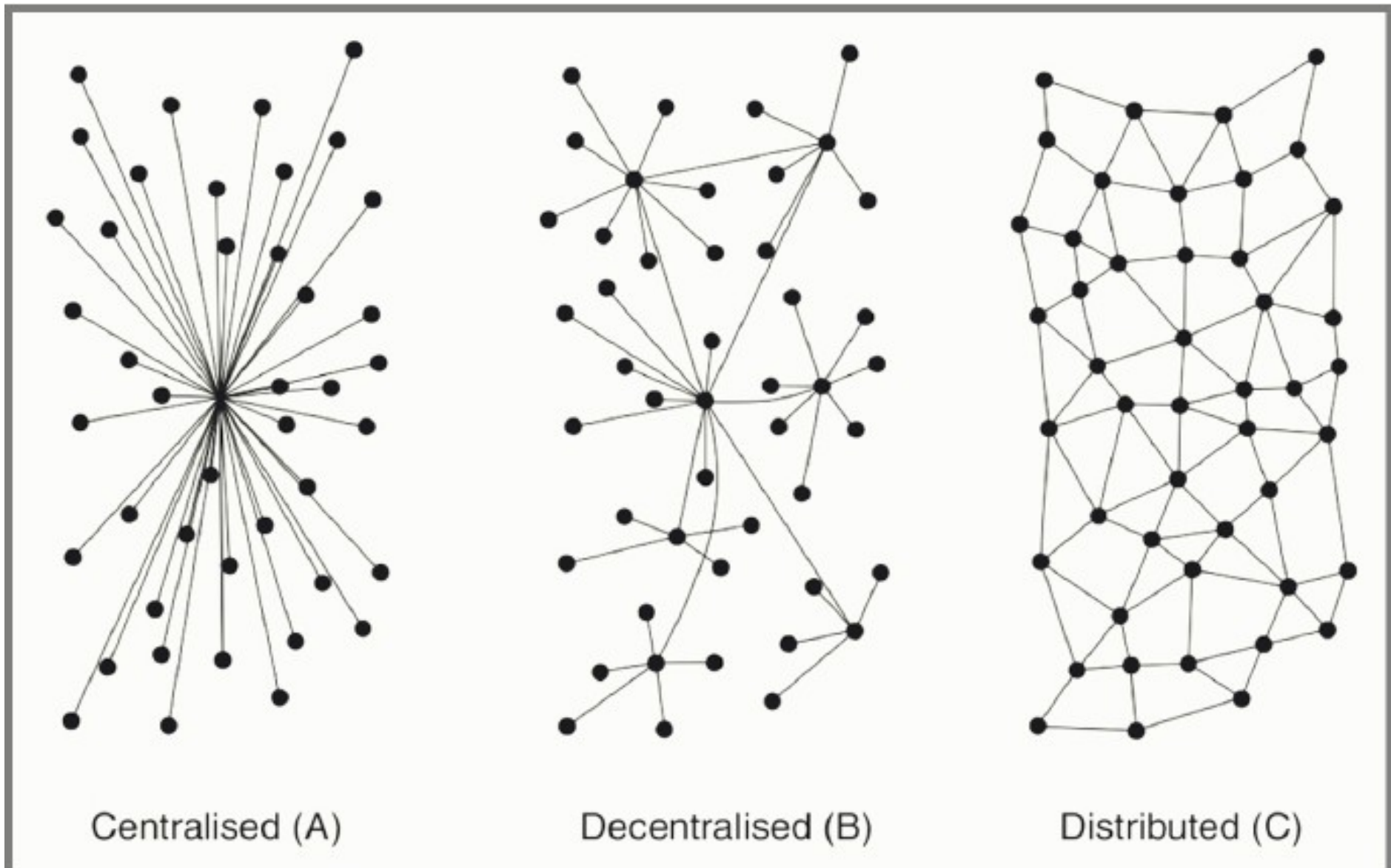
Introduction

- 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



Introduction

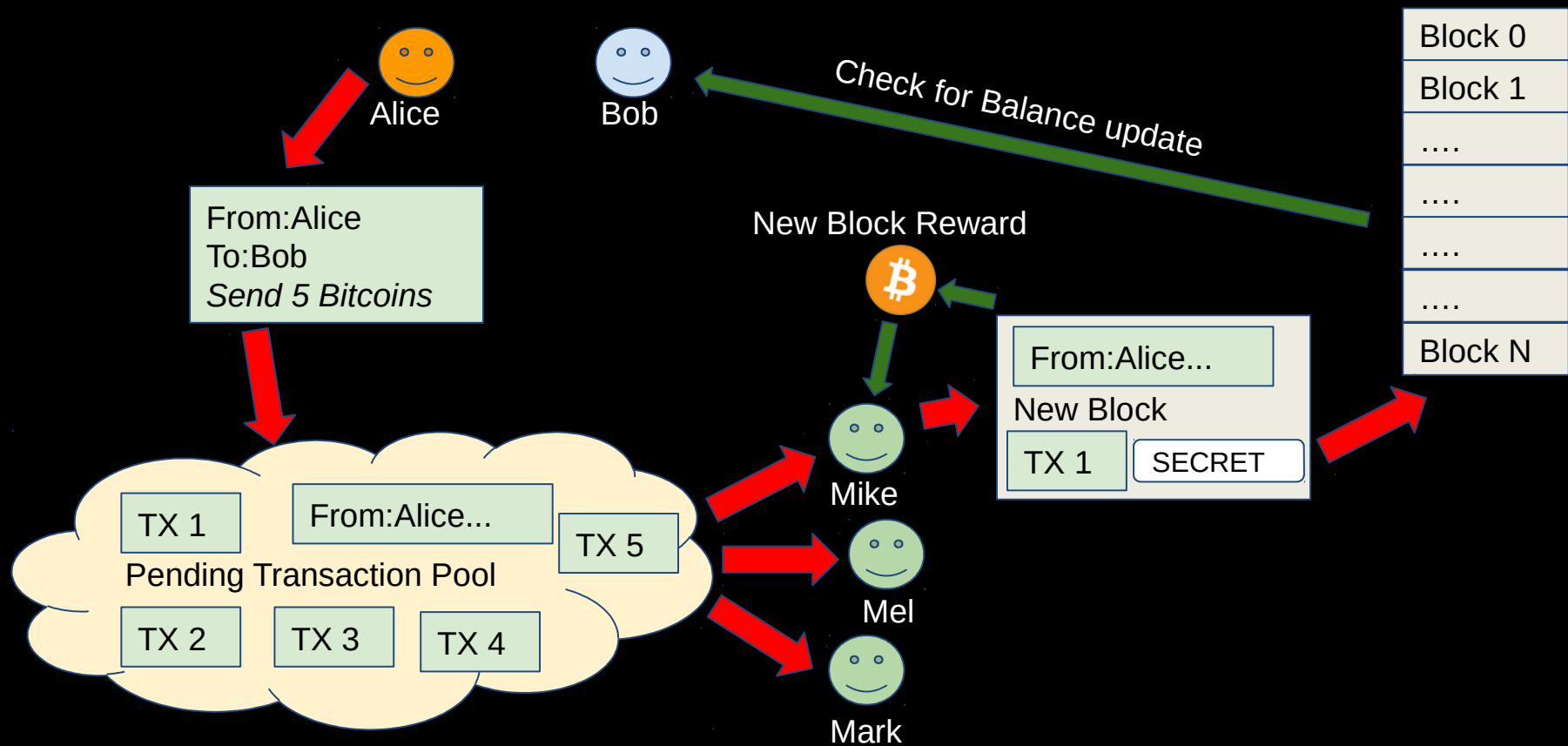


Introduction

- Hashing Algorithms
 - SHA encryption
 - Merkle/Radix (Hash) Tree Structures
- Proof-of-work
 - Computational power
- Hard fork vs. Soft fork
- Consensus/Governance Algorithms
 - Bitcoin Protocol
 - Ethereum Protocol
 - Many others
- Public vs. Private (permissioned)

Introduction

How the Blockchain works



Key Players



- Bitcoin - the birth of the blockchain
 - Created by “Satoshi Nakamoto” in 2008
 - Volunteer computer network for transferring Bitcoins
 - Maximum 21 Mil Bitcoins, ~16.4 Mil circulating today
 - Market Cap ~36.6 Billion USD (as of 31 May, 2017)
 - 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



- 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 ~92.1 Million circulating
 - Fast transaction confirmation times (~15 seconds)
 - Forked in Aug 2016 to reverse a hack; Ethereum Classic (ETC) retained the hack

Key Players









- 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



- 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

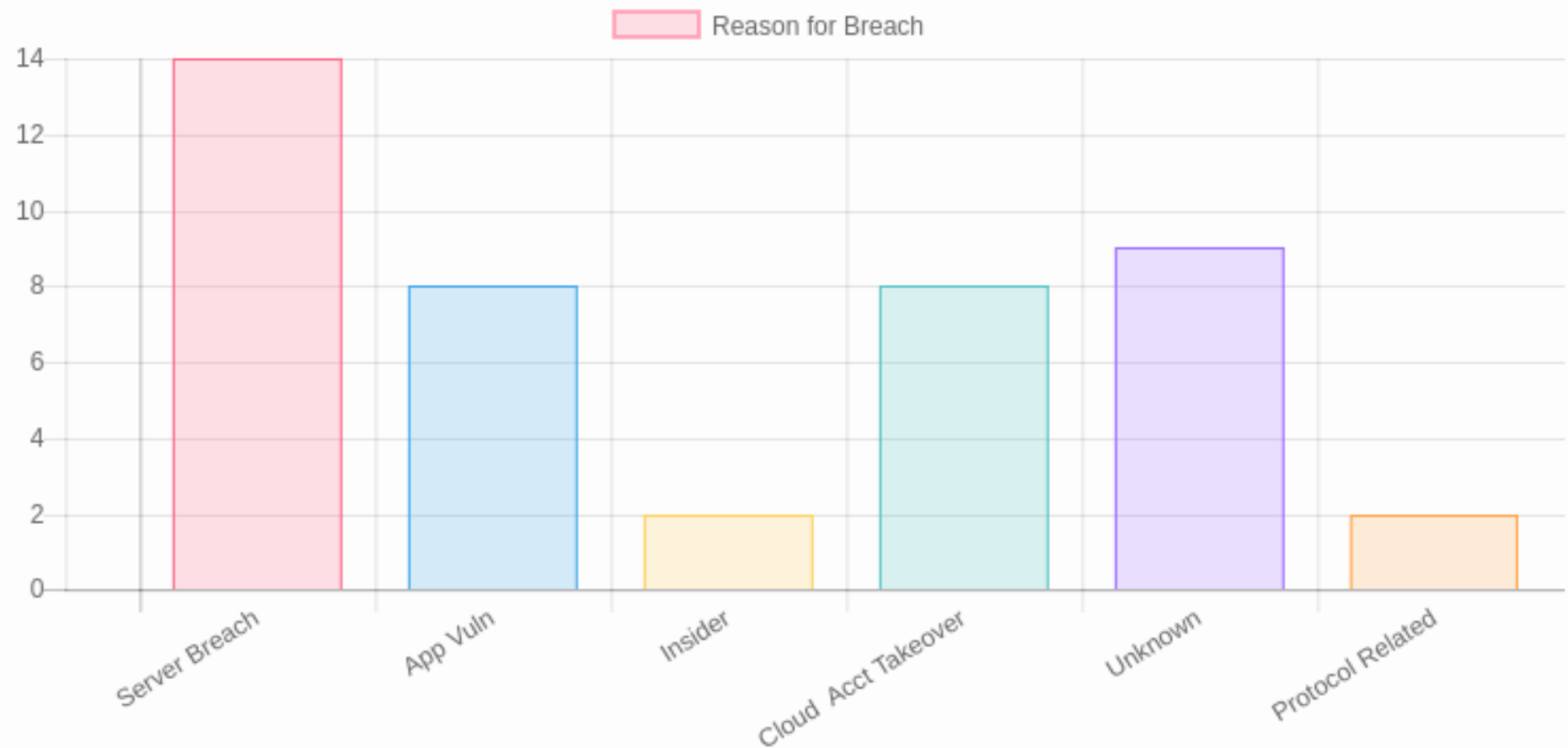
Key Players

	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

Hacks

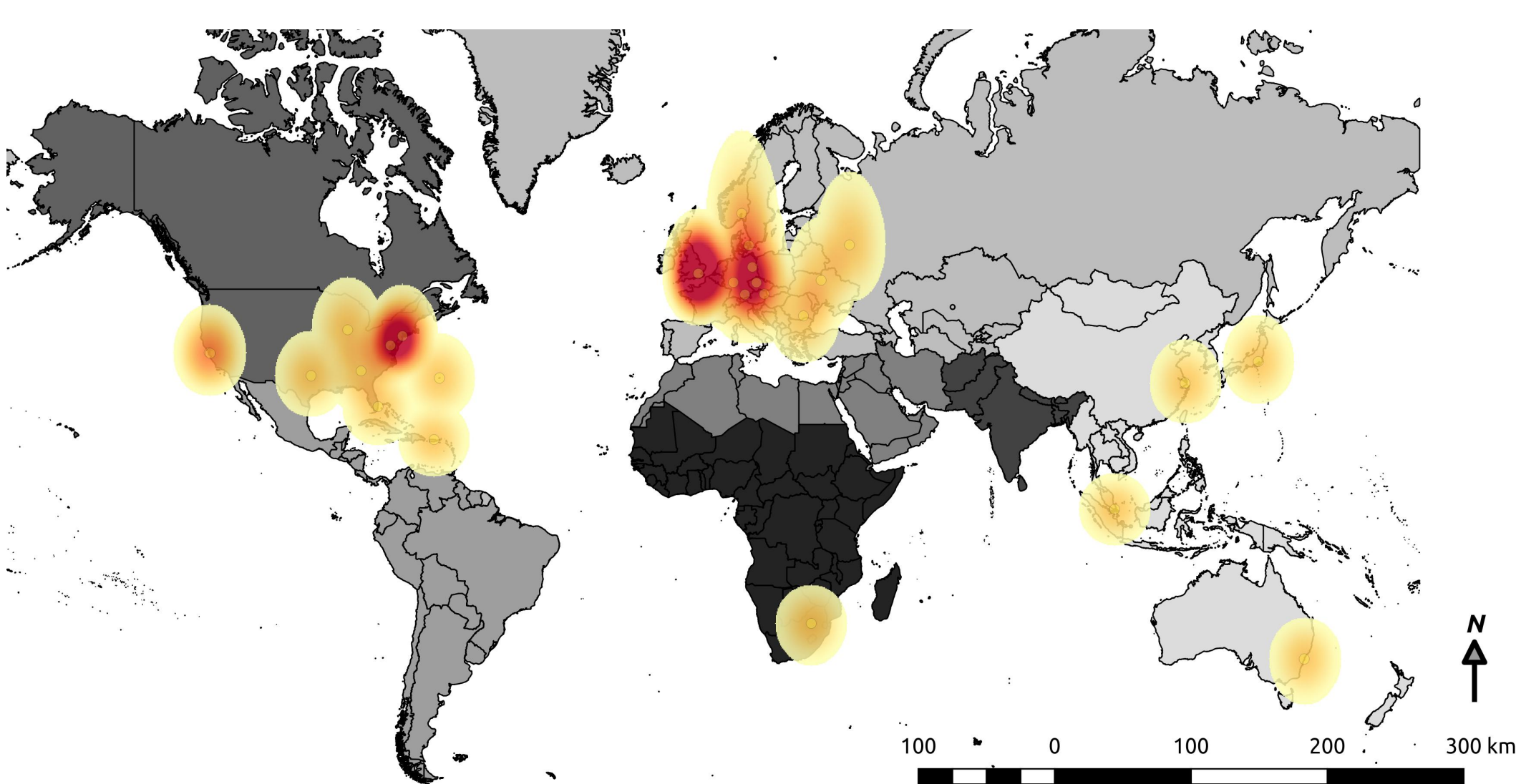
ROOT CAUSE ESTIMATES

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



Hacks

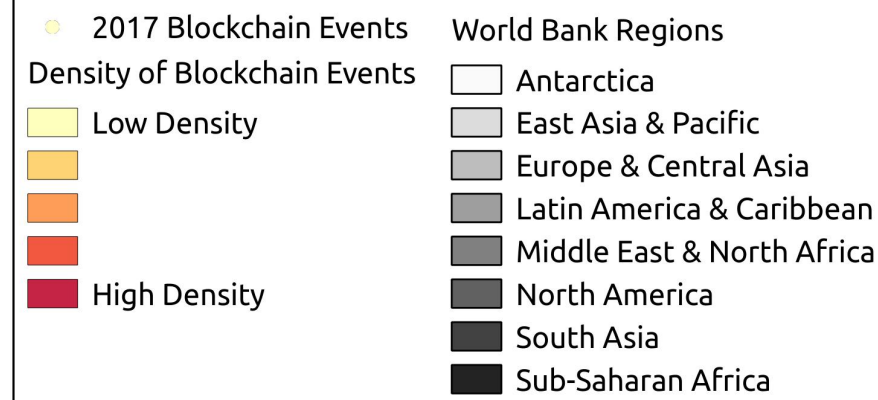
- 51% attack
- Recursive calling
- Hot wallets/Cold storage of keys
- API vulnerabilities
- Dependency backdoors
- Spear-phishing
- Embedded scripts (emailed docs)
- Admin access
 - Servers
 - Cloud infrastructure
- 3rd party plugins
- SQL Injection
- Man in the middle
 - Simultaneous requests
- DNS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



2017 Blockchain Events

This maps show the locations as listed in the January 16th, 2017 article "These are the world's best blockchain conferences and expos to attend in 2017." The regions are colored by regions as designated by the World Bank. The density of events ranges from lower numbers of events in light yellow to high density in red.

Created by: Joe Blankenship
 Data Used: Andrew Meola/Business Insider
 (<http://www.businessinsider.com/blockchain-conferences-2017-1>);
 Natural Earth Country data



Future of Blockchain

- Decentralization & distribution
 - Political and economic balances > Power dynamics
 - Corporations/Governments may be formalized through DAO governance
- Alternative Economies
 - “Middle Men” & Labor Dynamics
 - “Micro-employment”
 - Personal currencies backed by personal value
 - Patents, Intellectual Property, Immaterial Property (data)
- 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, Blockchain Alliance, B3i, Ethereum
- 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

Human Trafficking Efforts

- Microsoft, ConsenSys, Blockstack Labs
 - Blockchain-based Identity
- Chainalysis
 - Pattern Matching – Time Series Analysis
- OneName, ShoCard, and uPort
 - Digital Identity
- Provenance
 - Logistical Tracking

Questions and Discussion

Thank you!

Joe Blankenship

www.thejoeblankenship.com

@CGRIforg