RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: LAB2-T09

BLOCKCHAIN APPLICATIONS AND THEIR WEAKNESSES: A PRACTICAL INVESTIGATION

LAB LEADER: **James Stanger, PhD**
Chief Technology Evangelist, CompTIA
Twitter: @jamesstanger

LAB FACILITATORS: **Chris Hodson**

Stephen Schneiter
Product Manager
CompTIA
@saschneiter

About James

James Stanger, PhD

Chief Technology Evangelist - CompTIA
Security+, Network+, MCSE, LPI Linux, Symantec STA

I work with SMEs and tech leaders around the world

- *Linux and open source*
- *Emerging technology*
- *Security analytics*
- *Risk management*
- *Penetration testing, risk assessment, IDS, SIEM*
- *Network administration*
- *Virtualization*
- *Web technologies*
- *Certification development*
- *Award-winning author and instructor*

About Chris

CompTIA

Chris Hodson

CISO, EMEA

Office of the CISO, EMEA Region, Zscaler

Trusted advisor to executives, board members, and stakeholders

- *Expertise in secure network design, architecture and management*
- *Mapping technical solutions to business concerns*
- *Cloud security*
- *Risk management strategies*
- *Threat management*
- *Privacy and security issues, including GDPR*
- *Applied security, including blockchain and cybersecurity*

zscaler

About Stephen

Stephen Schneiter

Product Manager, CompTIA

I am the product manager for CompTIA Security+ and the program manager for the CompTIA Instructor Network (CIN)

Areas of expertise along the lines of

- *Networking*
- *Cybersecurity*
- *Technical training*

CompTIA Instructor Network

CompTIA

Why we're here

Our job together is to:

Educate + Learn = Apply

Our job as lab leaders:
To facilitate discussion and hands-on learning

Your job:
To participate and provide input and learn about blockchain

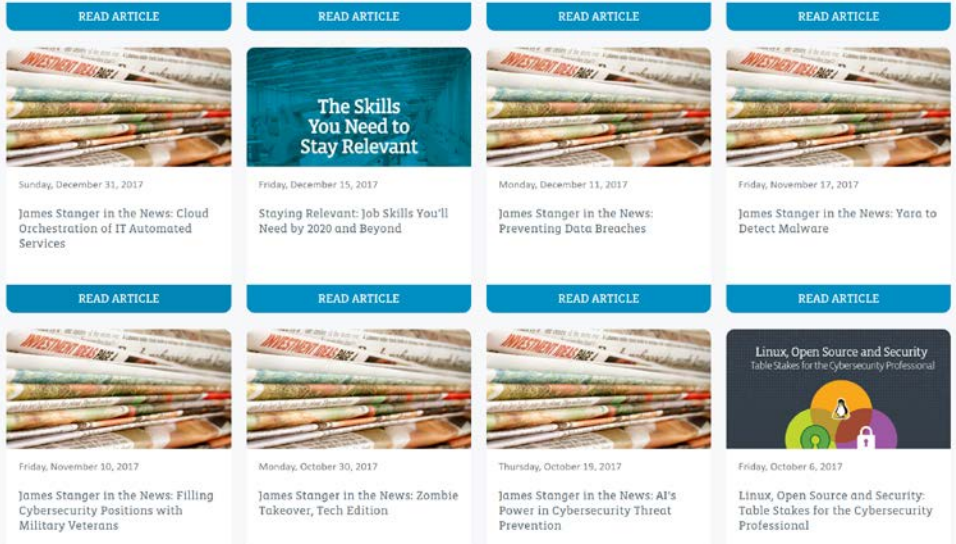
The "take away"
Anticipate practical issues with blockchain implementation

Let's get going!

DELIVERABLES

Deliverables

- White paper / report
  - From the “RSA 2018 San Francisco blockchain focus group”
  - Will report on our discussions today
  - Published on www.comptia.org
  - Discuss our findings
- Discussion of known weaknesses
  - Platform and supporting technology considerations
  - Threat modeling matrix
  - Discussion of exposure time and blockchain

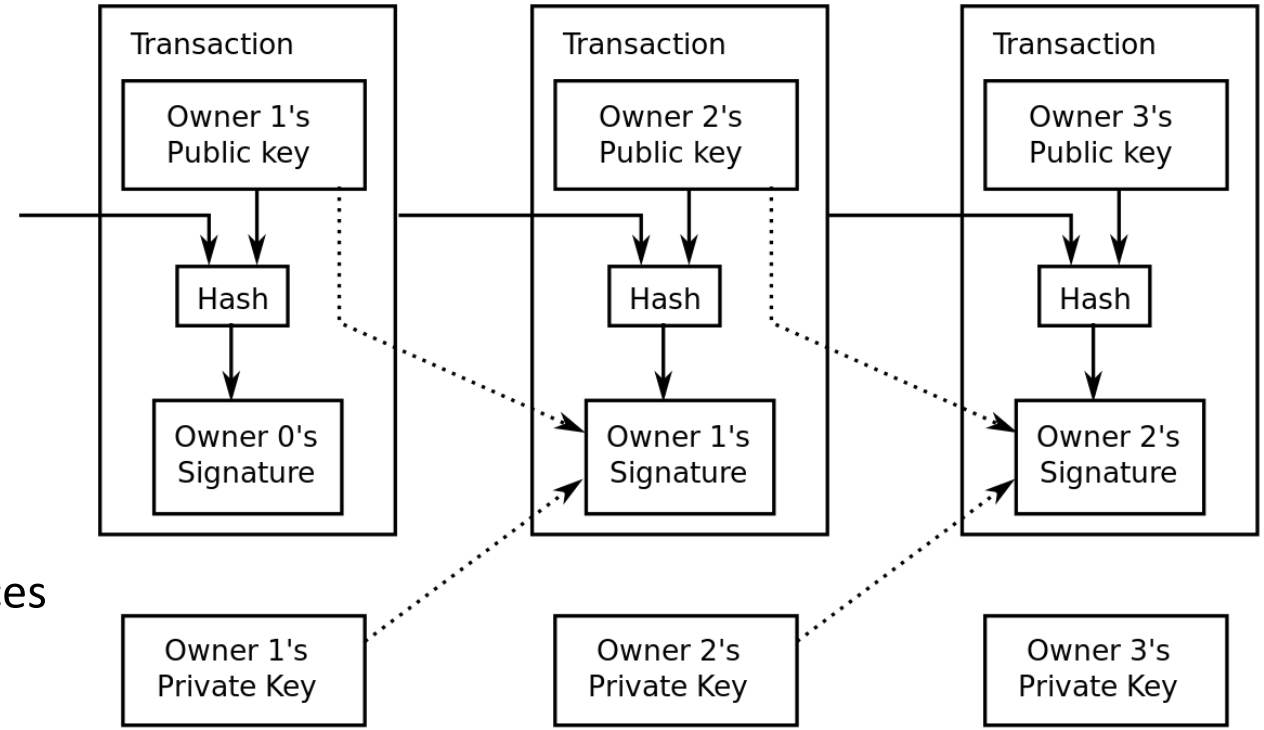


SECTION 1: UNDERSTANDING SPECIFIC SECURITY ISSUES IN THE BLOCKCHAIN PROTOCOL ITSELF

A discussion

Institutional uses and challenges

- Uses – the “plus side”
  - Practical uses
  - Benefits of disruption
- Challenges
  - Malevolence
    - Where blockchain can be misused
    - Where blockchain implementations can “break”
  - Unintended consequences of disruption



What business problems does blockchain solve?

Question helps identify real uses – and *real-time blockchain hacks*

Problems solved and solutions given can include:

1. Trust / Nonrepudiation
   - Remember: Satoshi created blockchain to solve a cryptocurrency need: Trust
   - Read Satoshi's white paper
   - Authoritative proof of transactions (traceability)
2. Disintermediation – *eliminate the middle players*
3. Replace / disrupt traditional services
   - Contract management / lawyers
   - Notary, title companies
- Chain of custody (Supply chain management)

Business solutions (cont'd)

Under what conditions is (public) blockchain useful?

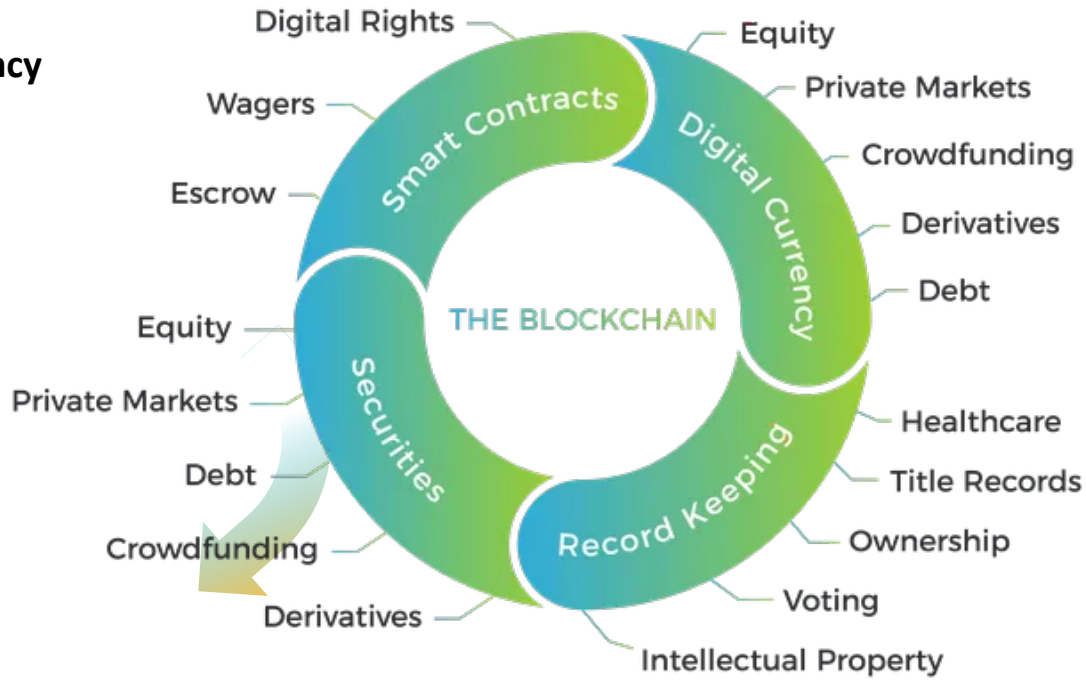
Conditions	Notes
Multiple parties involved	Can be used for cash-like transactions
Low – or no – trust environment	Blockchain acts as a trust mechanism
Need for auditability and *speed*	Do you want tracking?
Replacement for slow-moving solutions	Is blockchain going to work better, or are you just getting on the "bandwagon?"
Need for "disintermediation"	Get rid of the middle man!

Practical uses for blockchain

Research conducted by CompTIA

Uses by sector – way beyond cryptocurrency

1. Manufacturing
2. IT administration
   - Cloud – proof of work
   - Password augmentation / replacement
3. IT security
   - Authentication / multifactor / Packet tracing(?)
   - Chain of custody
4. Finance / real estate
   - Smart contracts
   - Crypto-currency
- Transportation
- Entertainment



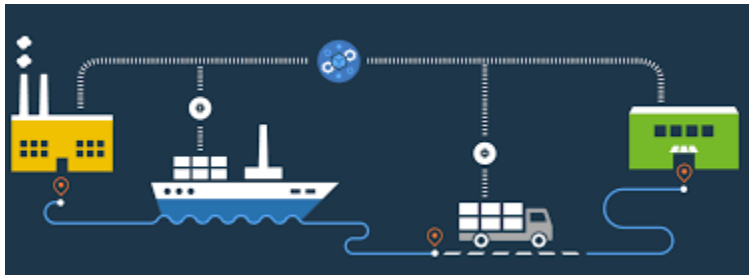
Blockchain types

- Let's break it into two categories
  - Public
  - Private
- Like the public and private cloud debates of old right?

Public	Private
Decentralized Federated Peer-to-peer	Less decentralized – many to many bb2b
Consensus authentication	Central authentication
Transactions viewed by public	No public transactions
Supports anonymous transactions High immutability factor Totally decentralized trust	Transactions don't have to be anonymous Allows fungibility – immutable to a point Scalability and performance

Institutional challenges

- By sector / vertical
  - Finance
  - Manufacturing
  - Retail (Walmart – food chain)
  - Healthcare
- Do you really want a public, immutable record?
- Regulatory concerns



GROUP DISCUSSION

Questions

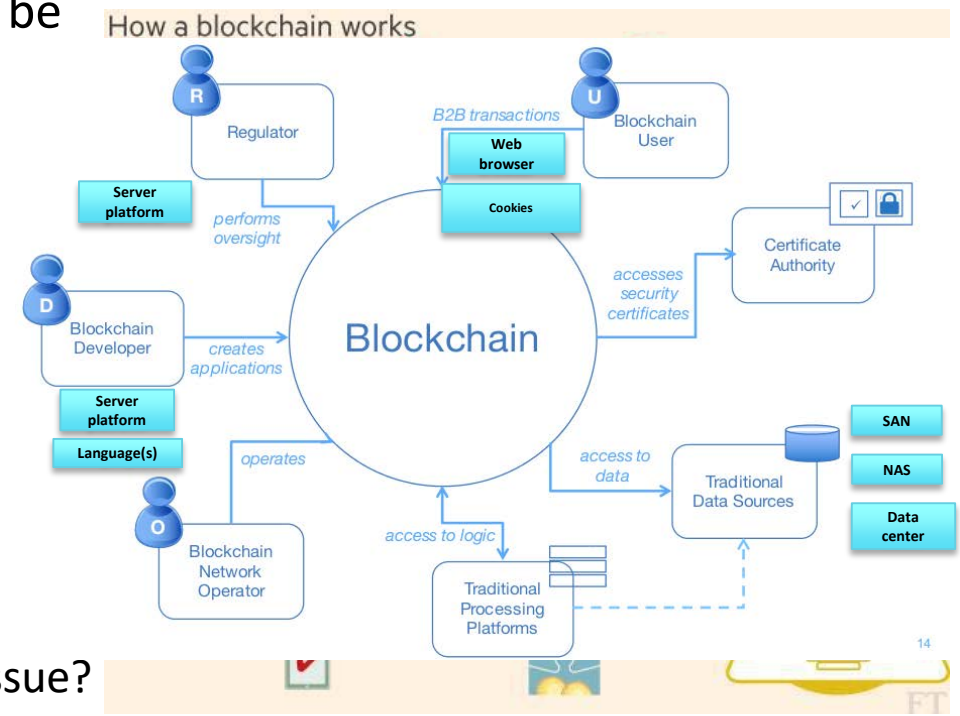
1. What practical uses of blockchain have you seen?
   - Please provide specific examples, not just theoretical uses
   - Go beyond simply listing terms such as smart contracts, supply chain management, cryptocurrencies, service tracking, user tracking
   - Discuss specific examples, and be prepared to report back on one good one per group
2. Where is your business/organization on its blockchain journey?
   * Innovation?
   * Incubation?
   * Nothing at all?
3. Which industry verticals do you think blockchain will have the greatest impact?

SECTION 2: PRACTICAL IMPLEMENTATION ISSUES – THE “INTERSTICES”

A discussion

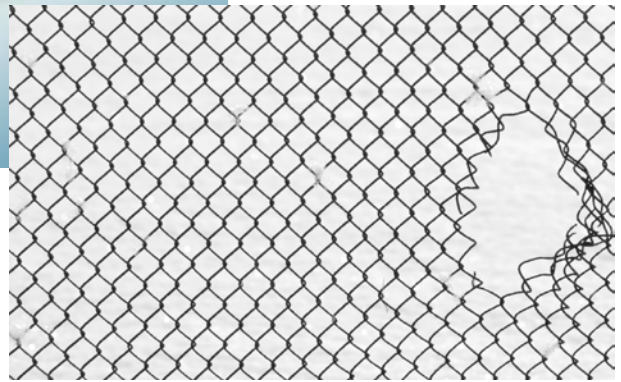
Network architecture issues - considerations

- What elements of the architecture will be put “under pressure” due to blockchain implementations?
  - End points
    - Processing encryption
  - Network elements
    - Routers
- Personal security – major issue
  - End user security remains the single-largest issue facing us today
    - Wozniak
    - Someone panics and deletes things
  - How will blockchain simply amplify this issue?



Where will the hackers look?

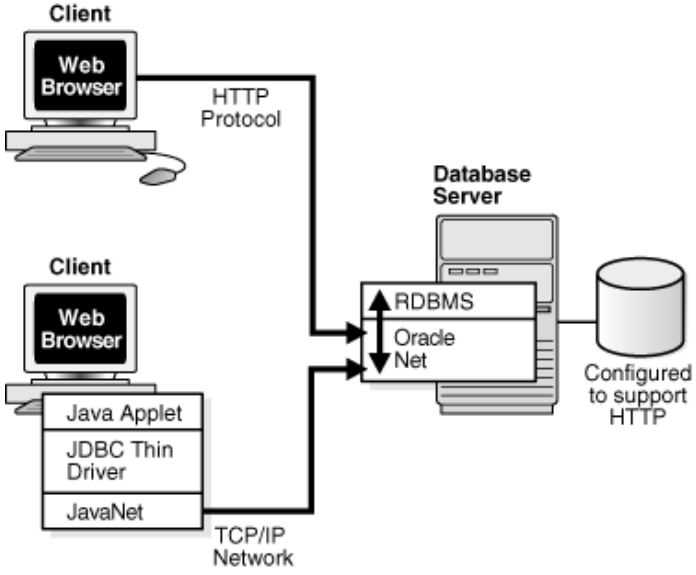
- *Interstices*
  - The “hard to reach” places
  - Dependencies
- Programming the protocol/solution
- Consensus building technologies
  - Parity issues
  - Smart contract security issues
- Key safety
  - No recourse for lost keys?
  - How well do we back up keys right now?

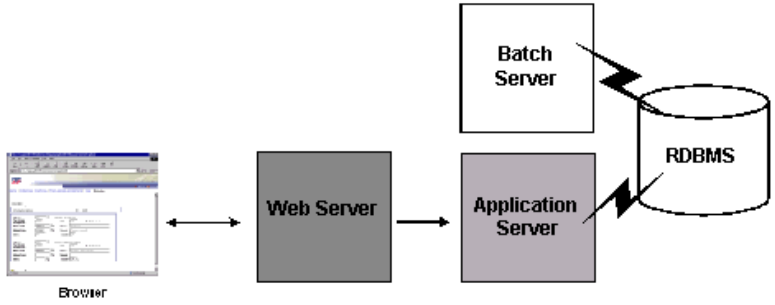


“The team then manually analyzed 3,759 contracts and found they could exploit vulnerabilities in 3,686 of them.”

Architecture elements that can be attacked

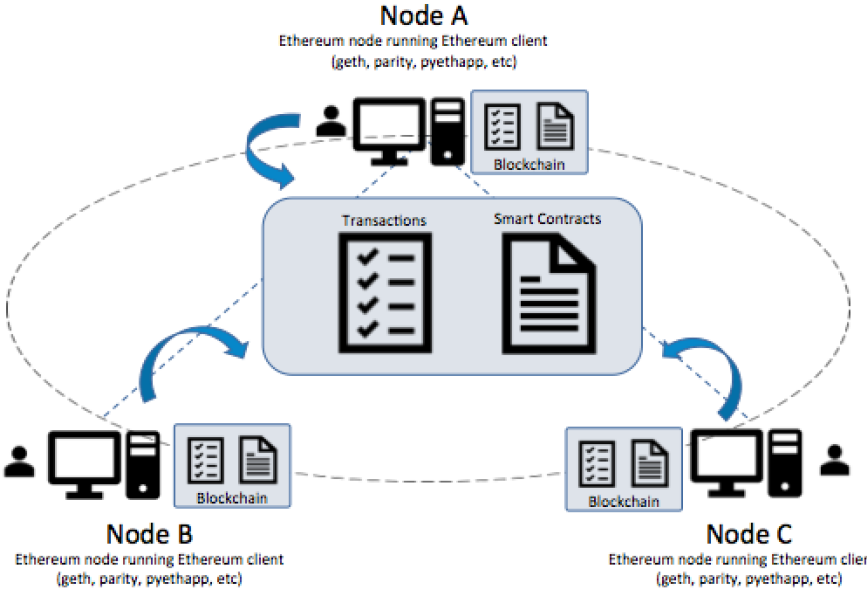
- Databases and Monero
  - Well-publicized Oracle issue
  - PeopleSoft
  - Weblogic servers
- Tidbit: Hackers used the vulnerability to mine cryptocurrency, and ignored the PII on the PeopleSoft implementation





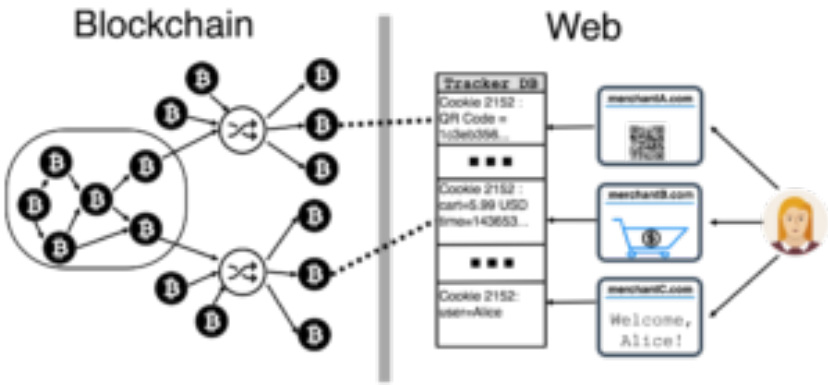
End points and blockchain security

- Wallets
- Bad code
- Lack of monitoring
- Infrequent updates?
- Dependencies
- Payment platforms
- Parity software and platforms



Browsers, cookies and blockchain

- Cookies leave . . . crumbs
- Crumbs lead to information leakage
- ConJoin anonymity technique
- Wallet issues
- Helps
  - Social engineers
  - Reconnaissance
- JavaScript and other languages



ETHEREUM DEMONSTRATION

SECTION 3: GETTING DEEPER INTO THE ISSUES

A discussion

Attacks (cont'd)

- Social engineering: The human element
  - Who learns that you're a bitcoiner in the first place?
  - Networks of attackers
  - Only as safe as the platform where information is stored
    - Network connected?
    - Physical security?
    - The old principles still apply
- Only as safe as the person using blockchain
- Transactions can't be undone

Information leakage
Browser
ISP / mobile provider
Associated services
SMS/SS7 hacks

GROUP DISCUSSION: SOCIAL ENGINEERING

Social engineering and blockchain

The fundamental things apply. . .

* Social engineering

* Platform security

* Multifactor authentication

Crypto Investor Ian Balina Hacked for Millions in Ether During Livestream

Most pressing issues for blockchain: What order?

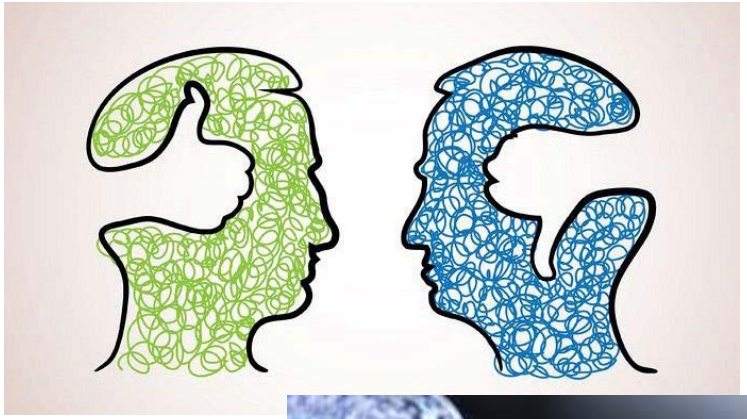
- What are the most likely problems that blockchain will experience?
  - Social engineering
  - Software development lifecycle issues (e.g., buffer overflows, race conditions)
  - Problems with the protocol
  - Problems with underlying platforms and associated protocols
  - Data corruption / manipulation
  - Other (list the problem, in order)
- Your job is the take the above and put it into what you feel is the most likely order – and we want to see you justify that order

Security issues: Wallets and keys

- Components
  - Ethereum wallet
  - Problem: Coding bug in wallet parity code software
  - Solution
    - Bug fix? Create a “strong fork”
    - How well thought through is this?
  - Private key
    - What if you lose it?
    - Recourse mechanism?
    - We’re not very good at backing up private keys as an industry

Business issues

- Do we really want transparency?
- Do we really want an indelible record?
  - Never changed?
  - What if you want to change the contract?
  - How are such things announced?



SECTION 4: SAMPLE IMPLEMENTATIONS AND HACKS

A discussion

Attacks (cont'd)

- Progress of attacks
  - Finney (2011)
  - Vector 76 (one confirmation) 2011
  - Time jacking (2011)
  - Double spend / race (2012
    Brute force (2013)
  - > 50% (2013+)
  - Wallet theft (2014)
  - DDoS (2014)
  - Transaction malleability (2015)
  - Refund (2017)
  - Hijacking (2017, 2018)
  - Fork (2013, 2016, 2018)

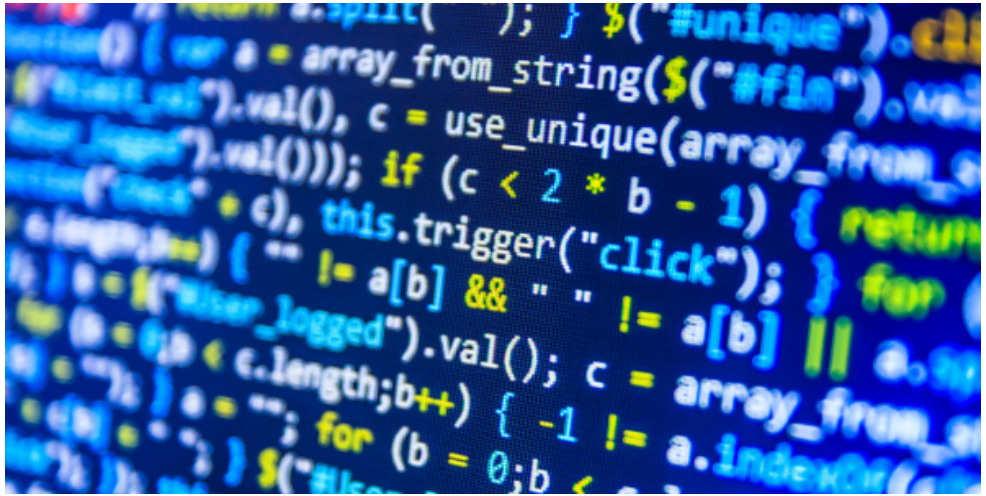
Attack	Description	Primary targets	Adverse effects	Possible countermeasures
Bribery attacks [75]	adversary bribe miners to mine on her behalf	miners and merchants	increases probability of a double spend or block withholding	increase the rewards for honest miners, make aware the miners to the long-term losses of bribery [75]
Refund attacks [78]	adversary exploits the refund policies of existing payment processors	sellers or merchants, users	merchant losses money while honest users might lose their reputation	publicly verifiable evidence [78]
Punitive and Feather forking [77] [79]	dishonest miners blacklist transactions of specific address	users	freeze the bitcoins of user for forever	remains an open challenge
Transaction malleability [80] [4]	adversary change the TXID without invalidating the transaction	Bitcoin exchange centers	exchanges loss funds due to increase in double deposit or double withdrawal instances	multiple metrics for transaction verification [81], malleability-resilient "refund" transaction [80]
Wallet theft [21]	adversary stole or destroy private key of users	individual users or businesses	bitcoins in the wallet are lost	threshold signature based two-factor security [82] [83], hardware wallets [84], TrustZone-backed Bitcoin wallet [85], Password-Protected Secret Sharing (PPSS) [86]
Time jacking [87]	adversary speed-up the majority of miner's clock	miners	isolate a miner and waste its resources, influence the mining difficulty calculation process	constraint tolerance ranges [87], network time protocol (NTP) or time sampling on the values received from trusted peers [88]
DDoS [89] [90]	a collaborative attack to exhaust network resources	Bitcoin network, businesses, miners, and users	deny services to honest users/miners, isolate or drive away the miners	Proof-of-Activity (PoA) protocol [91], fast verification signature based authentication
Sybil [23]	adversary creates multiple virtual identities	Bitcoin network, miners, users	facilitates time jacking, DDoS, and double spending attacks, threatens user privacy	Xim (a two-party mixing protocol) [92]
Eclipse or netsplit [3]	adversary monopolizes all incoming and outgoing connections of victim	miners, users	inconsistent view of the network and blockchain, enable double spends with more than one confirmation	use whitelists, disabling incoming connections [3]
Tampering [43]	delay the propagation of transactions and blocks to specific nodes	miners, users	mount DoS attacks, wrongfully increase mining advantage, double spend	improve block request management system [43]
Routing attacks [5]	isolate a set of nodes from the Bitcoin network, delaying block propagation	miners, users	denial of service attack, increases possibility of 0-confirmation double spends, increases fork rate, waste the mining power of the pools	increase the diversity of node connections, monitor round-trip time, use gateways in different ASes [5]
Deanonymization [93] [94]	linking IP addresses with a Bitcoin wallet	users	user privacy violation	mixing services [95], CoinJoin [96], CoinShuffle [97]

Attacks (cont'd)

- Additional attack (digital signatures)
- Vector76 attack (attacks exchange– *involves pre-mining*)
- Brute force
- > 50% / 51% attack, "Goldfinger" (*hypothetical*)
- Bitcoin hijacking
- Refund attacks
- DDoS
- Block discarding

Ethereum – Parity hack

- $32 million loss
  - Vulnerability in the wallet software
  - Not in the protocol, *per se*
- What lessons can we learn?



Coincheck hack

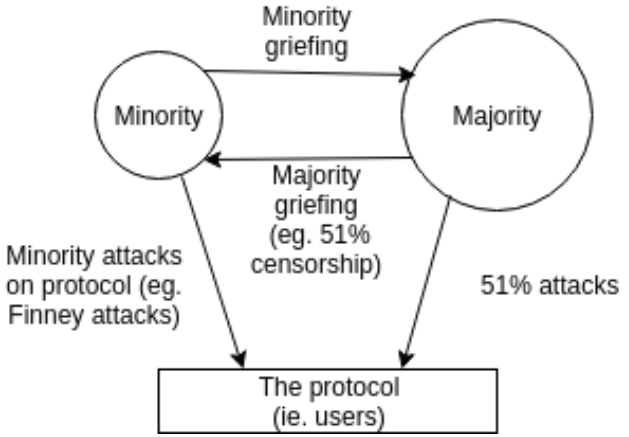
- $530 million stolen?
- Private key stolen
- Basic security measures not followed
  - Internet-connected “hot wallet”
  - Should have used cold storage instead
  - No multifactor authentication
  - Weak private key storage techniques
  - Social engineering involved
  - No IDS on key resources
  - No analytics – no “red team, blue team”

Weaknesses

- Timing is everything
- Remember the old NTP issues of old?
- A similar (analogous) issue
- Two different modes for verifying application
  - Full
  - Simplified
- Scalability
  - Cost
  - Energy

Weaknesses (cont'd)

- Hijacking (Sybil attack)
  - The entire connection
  - Fake network
  - Untrusted Internet connection / mobile wallet
- Race conditions (timing, sort of)
  - Broadcast two invalid transactions at the same time
  - Attacker needs to make a network connection directly ot the victim – relatively theoretical
- Double spend (timing)



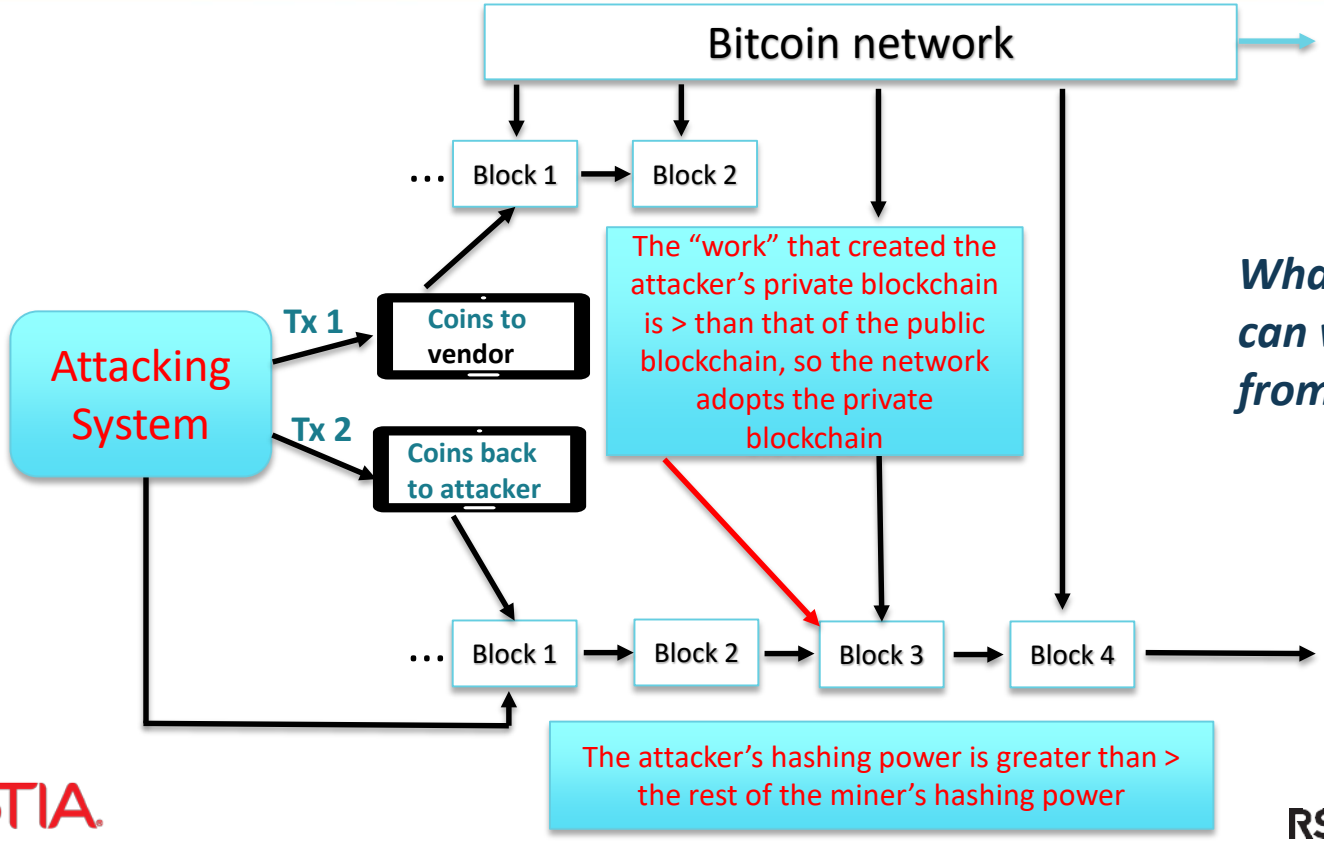
Finney attack

- Attacker is mining blocks – *must be a miner*
- The block he tries to use includes a transaction
- This transaction sends some of his/her own coins back to himself without broadcasting the transaction
- When attacker finds a block, he does not broadcast it

Involves *pre-mining*

- Sends the same coins to a different merchant to purchase something
- After the merchant accepts payment and irreversibly provides the service, the attacker then broadcasts his/her block
- The transaction that sends the coins back to the attacker, which is included in this block, overrides the unconfirmed payment to the merchant

Finney attack (cont'd)

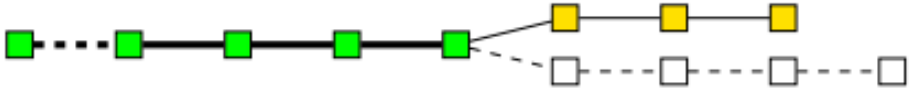


What larger lessons can we learn from this issue?

Another form of double spend attack

(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.



(c) The attacker succeeds in making the fraudulent branch longer than the honest one.

(d) The attacker's branch is published and is now considered the valid one.

What larger lessons can we learn from this issue?

Weaknesses and today's companies

- To Dell's customers, the risk is chump change
- Cost / benefit ratio
- Hack / benefit ratio

SECTION 5: ANTICIPATING AND RECTIFYING BLOCKCHAIN SECURITY ISSUES – AND USING BLOCKCHAIN TO RECTIFY SECURITY ISSUES

A discussion

Elements to attack: WiFi and browsers

- User sessions (blockchain faucets)
- Why? To mine cryptocurrency more cheaply
- Distributed networking
- WiFi
  - CoffeeMiner
  - Additional attacks
- Browsers
  - Browser hijack
  - Cryptojacking

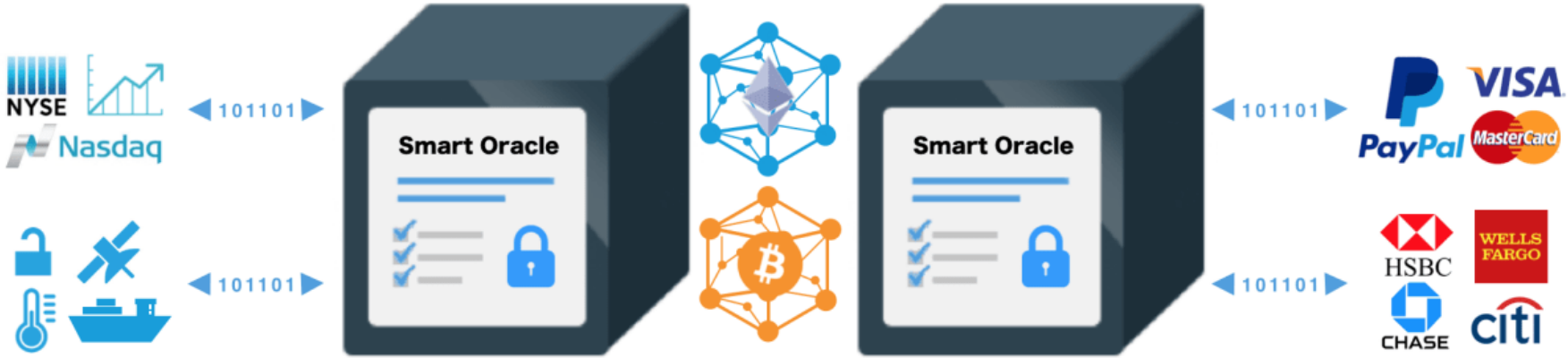
Elements to attack

- The cryptocurrency “oracle”
- A “translator” for information provided outside of a blockchain
- Elements
  - Software
  - Hardware
  - Inbound
  - Outbound
  - Consensus

“Oracles provide the necessary data to trigger smart contracts to execute when the original terms of the contract are met. These conditions could be anything associated with the smart contract - temperature, payment completion, price changes, etc. These oracles are the only way for smart contracts to interact with data outside of the Blockchain environment.”

How are these implemented?
How can they be manipulated or compromised?

Elements to attack: Blockchain oracle



Source: https://cointelegraph.com/explained/blockchain-oracles-explained

Wallets – how would you attack them?

- Hot
  - Internet-connected
  - Like carrying cash
- Cold
  - Holding funds
  - Transfer ability available
- Physical stores
  - Physical
  - Side channel attack

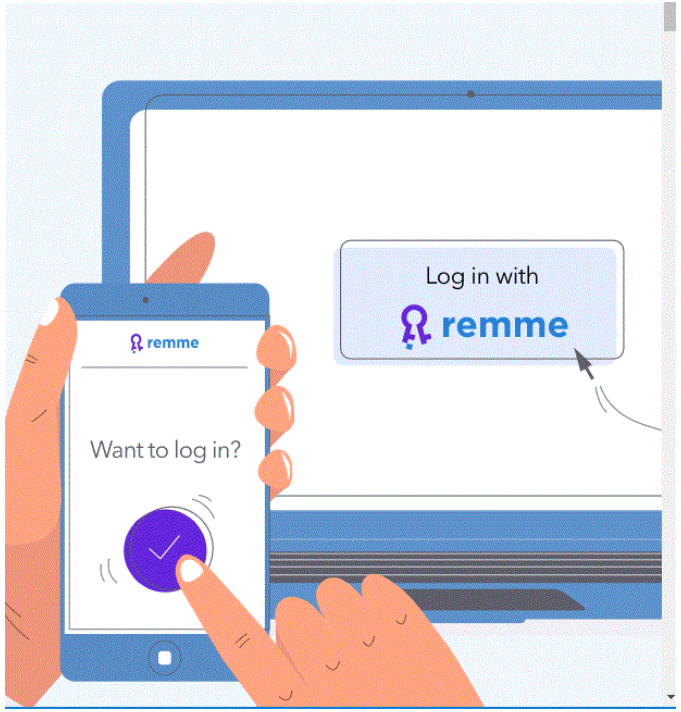
Hand-implanted NFC chips open this man's bitcoin wallet

By LIAT CLARK

Tuesday 11 November 2014

Blockchain and passwords?

- Password replacement / augmentation
  - Who will introduce it?
  - Remember fingerprint scanners?
    - Banks tried
    - Apple had to popularize
- Considerations
  - Popularization – who will explain it?
  - Privacy issues and perceptions
  - Form factor – how to implement?



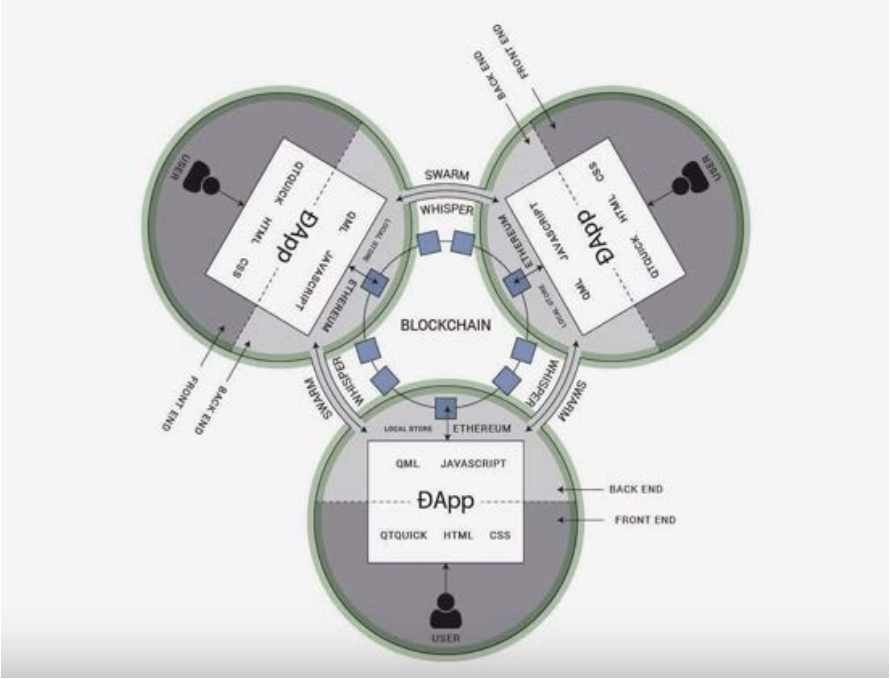
GROUP DISCUSSION

Question 4

4. What specific security vulnerabilities are you seeing?
   - Different to anything we've seen before?
   - Just hype?
   - Are you seeing innate dangers?

Question 5: Secure development lifecycle and blockchain

- The same principles apply
- It's clear blockchain is being developed in the standard languages.
- We already struggle as an industry in this area.
- What existing issues will we port over to blockchain?
- What new issues will arise?
  - Smart contracts, identity management



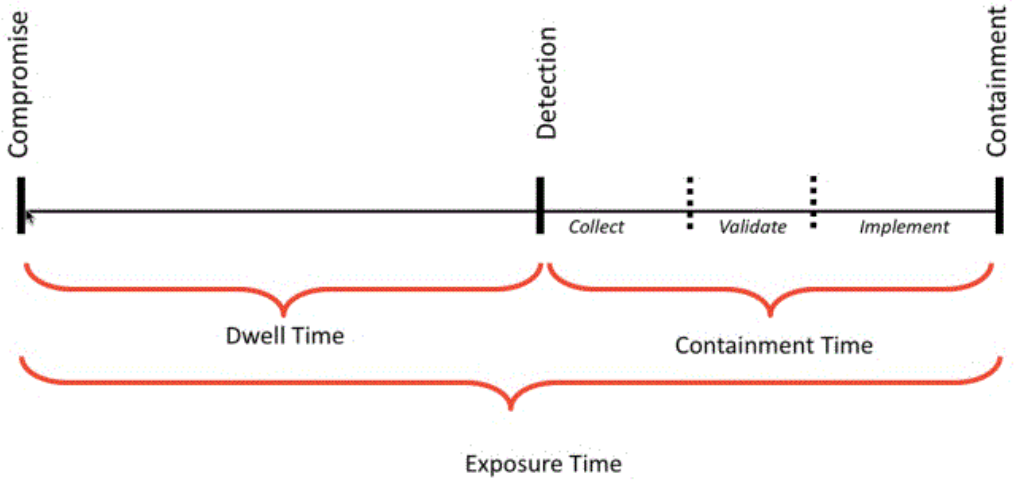
SECTION 6: APPLYING WHAT WE'VE LEARNED

GROUP ACTIVITY – THREAT MODELING

Blockchain threat modeling matrix

Blockchain platform / element / supporting technology (e.g server, protocol, wallet, browser)	Possible attack	Result / Indicator of compromise (i.e., artefact left behind)
Example: **Blockchain protocol**	Example: > 50 attack	Example: Data manipulation / suspect or delayed confirmations on data blocks

Incident response and blockchain: Exposure time



FINAL DISCUSSION

Question 6: Cybersecurity use cases

How can blockchain be used to provide cybersecurity services?

* Authentication, authorization

* PKI replacement / supplementation

* What other technologies already exist, and can they do a better job?

* DDoS mitigation?

DDoS and blockchain: An applied example?

- Traditional DDoS "straightjacket" services already exist
- Can we use blockchain to supplement?
- Pro
  - Eliminates – or reduces – anonymity and packet forging
  - Tracking
- Con
  - Cost of blockchain per packet on routers
  - Computing cost to create blockchain associations

Question 7: Skills shortage and blockchain

We already have a considerable skills gap.

- How will blockchain mitigate the skills gap?
- How will it make the problem worse?
- Issues to consider:
  - Developers
  - People who run infrastructure
  - Impact on existing jobs
  - New job roles

TO SUM THINGS UP . . .

Summary

Focus on the practical implementations!

- Fundamental cybersecurity principles
- In many ways, yet another platform to secure!
- Consider
  - Data manipulation
  - Platform interdependencies and “interstices”
  - Software development lifecycle
  - Eventual protocol issues that will arise
  - Threat modeling

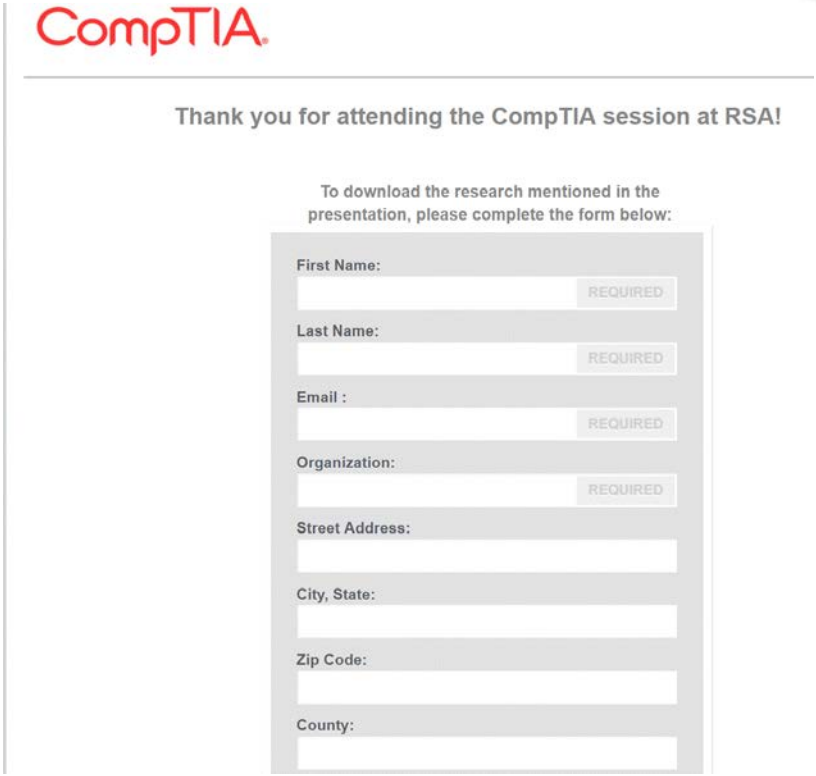
Look for the focus group report, white paper, and other resources on Comptia.org!

For more information

For the latest slides,
and additional blockchain
research, please
to the
following URL:

http://www.land.certification.comptia.org/RSA

CompTIA



Thank you!

#RSAC

Chris Hodson
chodson@zscaler.com
+1 44 (0)7538 923922
Twitter: @ChrisHInfoSec
https://www.linkedin.com/in/christopherjhodson

Articles:
https://www.csoonline.com/author/Chris-Hodson

James Stanger, PhD
jstanger@comptia.org
+1 (360) 970-5357
Twitter: @jamesstanger
Skype: stangernet
CompTIA hub:
https://certification.comptia.org/it-career-news/hub/James-Stanger

Stephen Schneiter
sschneiter@comptia.org
+1 (630) 6788503
Twitter: @TeachCompTIA
Skype: stephen.schneiter

Latest articles and blog entries:

Cloud Orchestration with Chef – Admin Magazine

Threat Hunting with Yara – Admin Magazine

How to engage with the C-Suite on cyber risk management

CISOs: What you can control – and what you can't – in GDPR

A New Year Cybersecurity two-fer: Meltdown and Specter

The Whole Story about Equifax?

From Ransomware to Wiperware

Don't Hack Me, Bro!

5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it

The old has become new again

CompTIA

RSAConference2018