Rethinking Blockchain Security

Vincent Chia[1], Pieter Hartel[2], Qingze Hum[2], Sebastian Ma[1],
Georgios Piliouras[2], Daniël Reijsbergen[2],
Mark van Staalduinen[1], Pawel Szalachowski[2]

[1] The Netherlands Organisation for Applied Scientific Research
[2] Singapore University of Technology and Design

2 August 2018

Rethinking Blockchain Security

BLOCK TEST

1 Incident Database

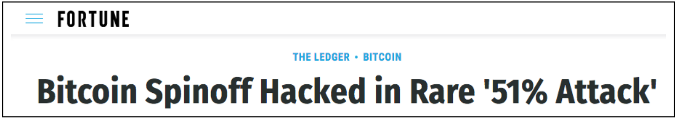
2 Smart Contract Testing

3 The PRESTO Framework

4 Conclusion

Blockchain in the News

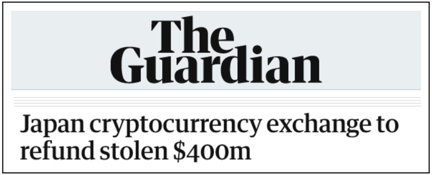
Blockchain is in the news, not always positively



FORTUNE

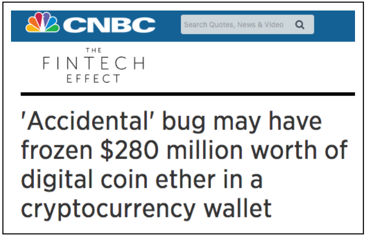
THE LEDGER • BITCOIN

Bitcoin Spinoff Hacked in Rare '51% Attack'



The Guardian

Japan cryptocurrency exchange to refund stolen $400m



CNBC

THE FINTECH EFFECT

'Accidental' bug may have frozen $280 million worth of digital coin ether in a cryptocurrency wallet

Blockchain Incidents Since April 2018

Major incidents between paper submission and now:

Bancor	smart contract	\$23M	July
Coinrail	hack	\$40M	June
Bithumb	hack	\$31M	June
Zencash	51% attack	\$700K	June
Litecoin Cash	51% attack	—	May/June
Bitcoin Gold	51% attack	\$18.6M	May
Verge	protocol attack	\$2.85M	April/May
Monacoin	block withholding	\$90K	May

Incident Database

Systematic categorisation of incidents is needed.

Available sources:

- Blockchain Graveyard
- Ethereum Blog Security Archives
- ....

Database format:

- STIX international standard for cybersecurity incidents

Three Incident Categories

OPSEC control of information or access to assets passwords, phishing
Smart Contracts contract bugs or honeypots
Consensus Protocol Incentives cheating network participants

Recent Incidents, Revisited

BLOCK TEST

Major incidents between paper submission and now:

Bancor	smart contract	$23M	July
Coinrail	hack	$40M	June
Bithumb	hack	$31M	June
Zencash	51% attack	$700K	June
Litecoin Cash	51% attack	—	May/June
Bitcoin Gold	51% attack	$18.6M	May
Verge	protocol attack	$2.85M	April/May
Monacoin	block withholding	$90K	May

□ : OPSEC

🟧 : Smart Contracts

🟦 : Protocol & Incentives

Top 8 Blockchain Incidents (USD)

1.	CoinCheck hack	$530M	2018
2.	MtGox ‘hack’	$450M	2014
3.	Parity multi-sig wallet frozen	$300M	2017
4.	BitGrail theft	$170M	2018
5.	Bitfinex hack	$78M	2016
6.	DAO hack	$60M	2016
7.	NiceHash breach	$60M	2017
8.	Coinrail hack	$40M	2017

□ : OPSEC

🟧 : Smart Contracts

🟦 : Protocol & Incentives

Our Approach

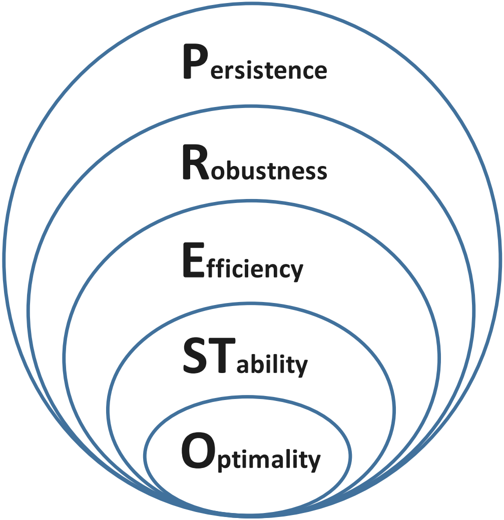
OPSEC	→	Known solutions. Same for crypto exchange as for bank.
Smart Contracts	→	Better tool-supported testing. No development life 'cycle'!
Protocol & Incentives	→	PRESTO framework. Performance/security trade-offs made explicit.

Smart Contract Testing

Research directions:

1. Better documentation.
2. Contract fuzzing.
3. Contract mutation.
4. Automatically generated tests

The PRESTO Framework



Conclusions

Blockchain security has a *long way* to go.

- Blockchain-specific incidents need more research
- Chance for academia to have a big impact
- Testing before deployment is essential
- Protocol trade-offs made explicit via PRESTO

Thank you for your attention.

Contact: `daniel_reijsbergen@sutd.edu.sg`