Incentive Attacks

Edgar.Weippl@tuwien.ac.at

Competence Centers for Excellent Technologies

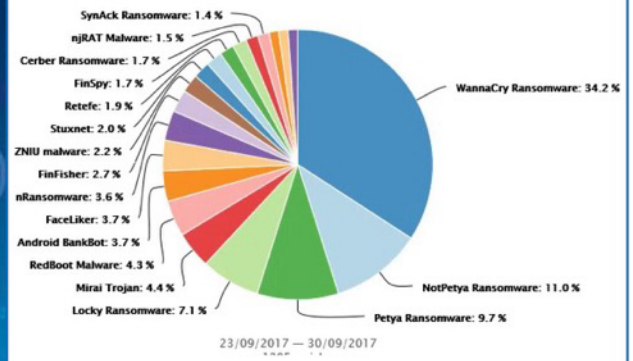
Bundesministerium Verkehr, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

Week: 39/2017

OSINT DASHBOARD

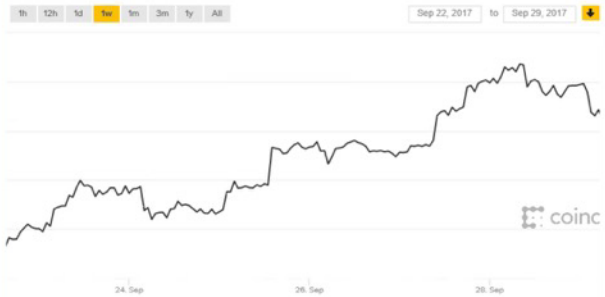
EUROPOL EC3 European Cybercrime Centre

Malware



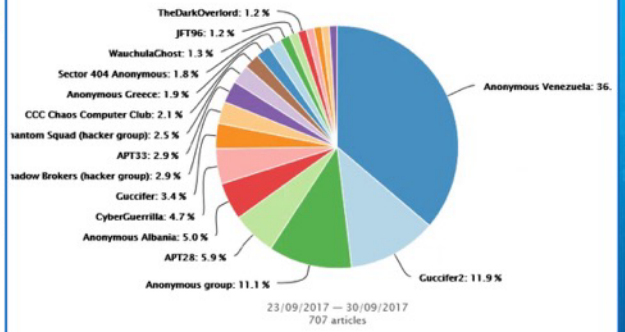
Digital Currencies

Bitcoin Price Index Chart



Underground/Anonymity

Trending Hackers Group Chart



- **Fileless Malware – Rising Trend in Malware Industry.** Fileless malware is becoming more popular in blackhat activities. What was first seen in some sophisticated targeted attacks is now becoming a standard partially due to the Vault 7 leak that revealed CIA's modus operandi. **Source**: DeepDotWeb.

- **Tech industry sounds alarm over draft online payment rules.** Twenty-seven e-commerce companies and lobby groups have asked the European Commission to change a draft proposal to regulate payment services, arguing that additional security measures will drive shoppers away from online platforms. **Source**: EurActiv.

- **Tor Browser Zero-Day Exploits Bounty.** ZERODIUM will pay a total of one million U.S. dollars in rewards to acquire zero-day exploits for Tor Browser on Tails Linux and Windows. The bounty is open until November 30th, 2017 at 6:00pm EDT, and may be terminated prior to its expiration if the total payout to researchers reaches one million U.S. dollars. **Source**: Zerodium.

North Korea may be mining bitcoin in addition to hacking it. Last month, North Korea was banned from exporting coal to China, its biggest buyer. The rogue regime may have found a new use for these idle coal supplies: powering bitcoin mines.The research identified activity that the firms believe is bitcoin mining in North Korea n May 17. The analysts don't know if the mining is ongo-

selling fentanyl via 'online super-
rs. A drug dealer who sold illegal synthetic opioid fentanyl to thou- web has been jailed for more than

On Way to Beard Contest. A sus- as been arrested in the US on the , it has emerged. Gal Vallerius, 38, al Airport at the end of August en o the competition in Austin, Texas.

hanges and Linux 4.12. Whenever n of its Firefox web browser, you pdate to the Tor Browser and the

TLP:GREEN

Digital currencies

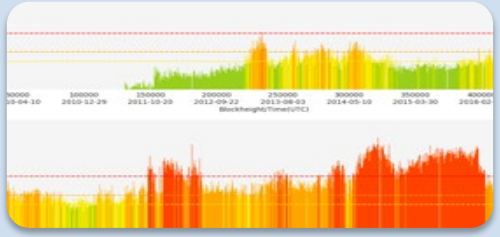
- **50k Servers Infected with Cryptomining Malware in Nansh0u Campaign.** A rapidly-expanding campaign has infected 50,000 servers with malware that mines an open source cryptocurrency called TurtleCoin. Servers were infected over the past four months as part of a high-profile cryptojacking campaign, believed to orchestrated by Chinese-language adversaries. **Source**: brica.

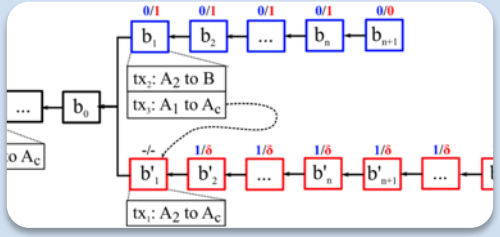
- **Bitcoin Blender Exits Cryptocurrency Mixing On Its Own Terms.** The long run of Bitcoin Blender cryptocurrency mixing service has reached an end this week as the business quickly shut down after a short announcement on the website's front page that asked customers to withdraw their funds. **Source**: bleepingcomputer.

- **North Korean hackers have allegedly attacked users of South Korean exchange UpBit with a clever phishing exploit.** The subject of the mail suggested that UpBit needed more information regarding a fictional sweepstakes payout for tax purposes. The mail did not come from the exchange but from another server outside of South Korea. **Source**: Coindesk.

- **Wave of SIM swapping attacks hit US cryptocurrency users.** SIM swapping is a type of ATO attack during which a malicious threat actor uses various techniques to transfers a victim's phone number to their own SIM card. The purpose of this attack is so that hackers can reset passwords or receive 2FA verification codes and access protected accounts. **Source**: Zdnet.

Research





Exploring Reality

Theoretical Foundations, Algorithms

Real-World Impact

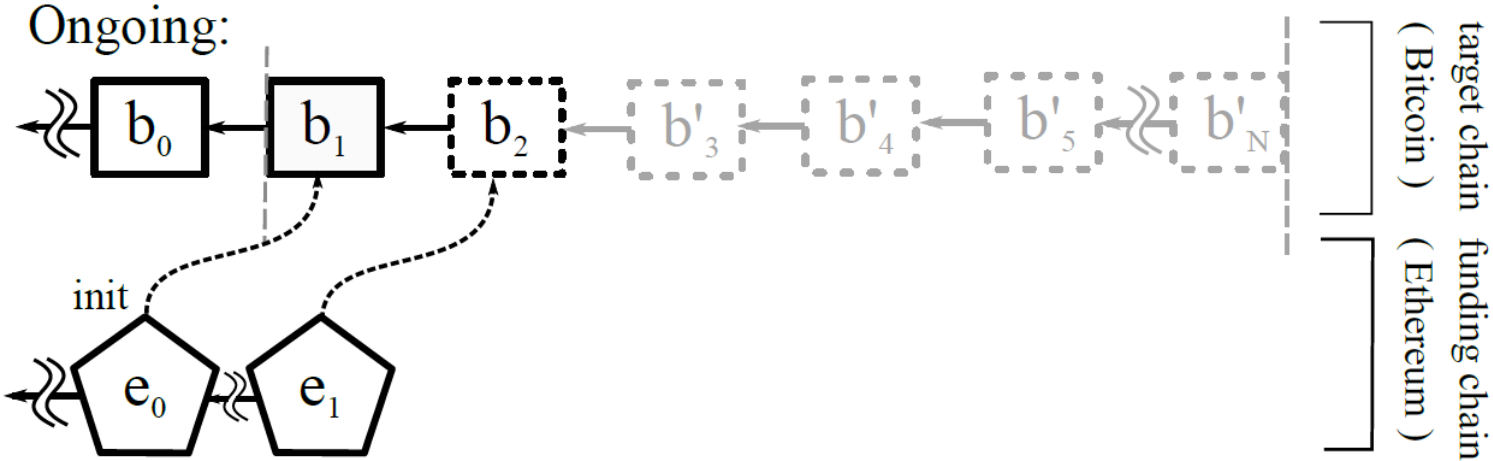
Pay-To-Win
Incentive Attacks on Blockchains

Aljosha Judmayer (SBA Research), Nicholas Stifter (SBA Research), Alexei Zamyatin (Imperial College London), Itay Tsabary (Technion, Israel), Ittay Eyal (Technion, Israel), Peter Gazi (IOHK), Sarah Meiklejohn (University College London), Edgar Weippl (SBA Research)

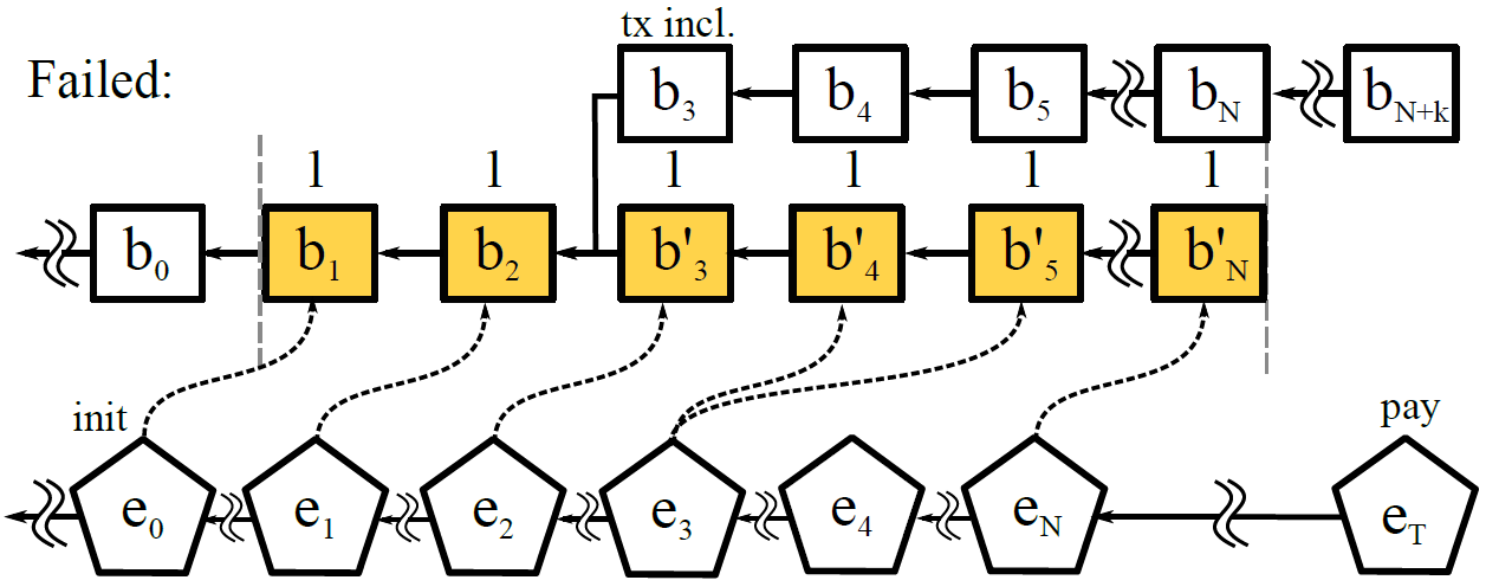
Incentive Attacks

- Impact on transactions
  - Transaction revision
  - Transaction ordering
  - Transaction exclusion
- Required interference with consensus
  - Deep fork
  - Near fork
  - No fork
- Attack chain
  - In-band attacks
  - Out-of-band attacks

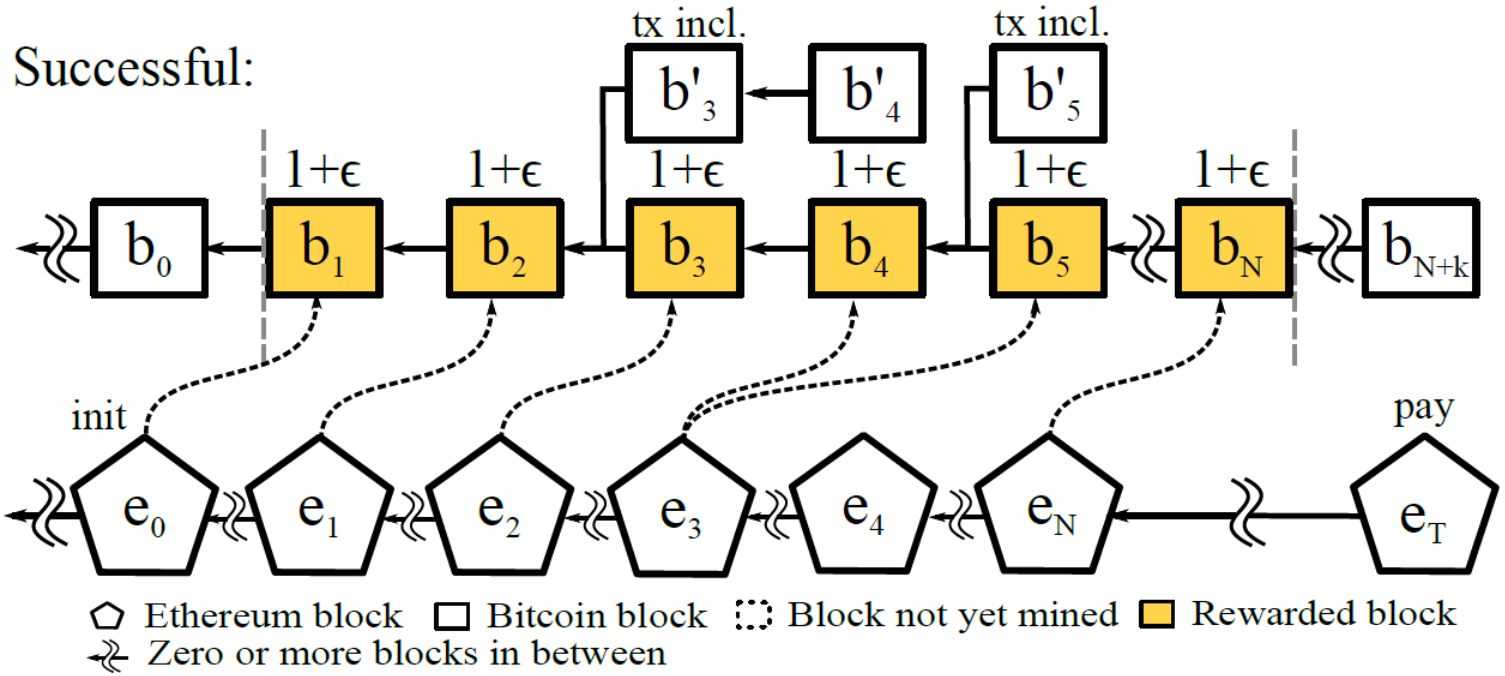
Out-of-Band TX Ordering Attack



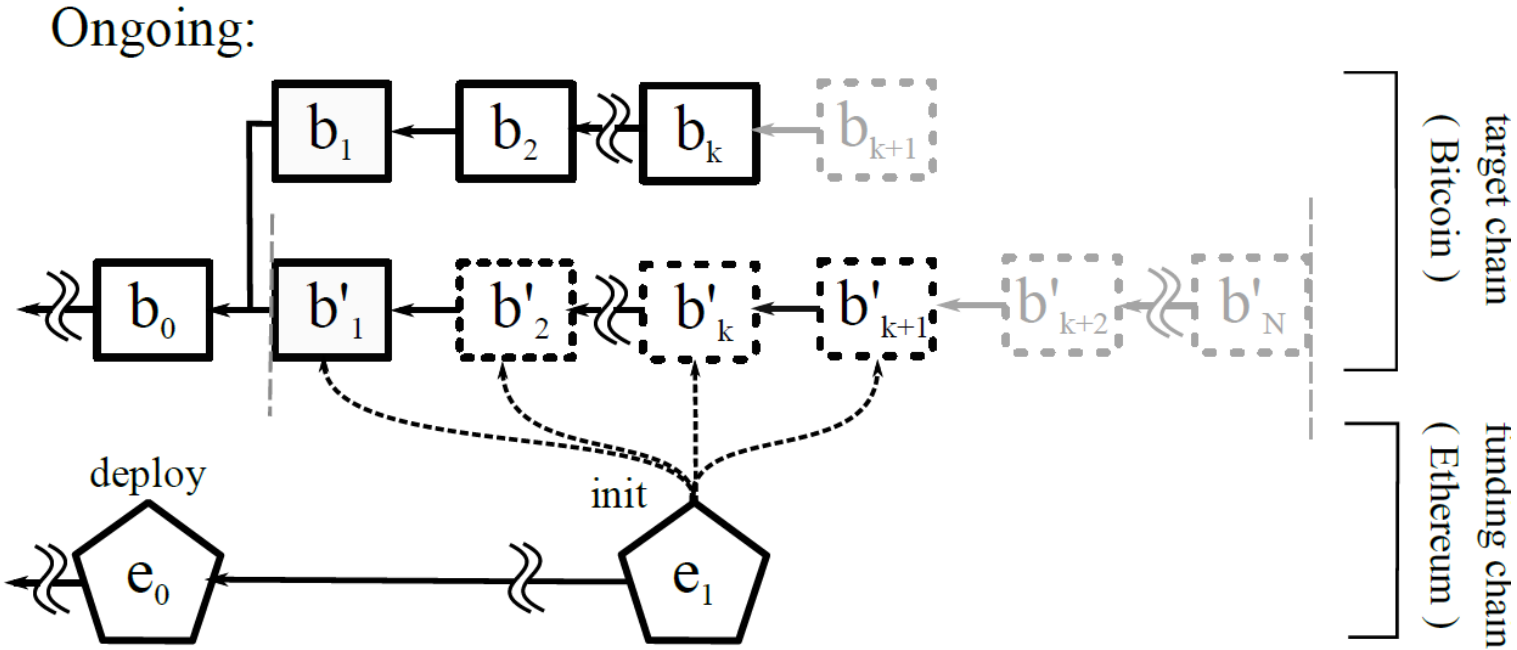
Out-of-Band TX Ordering Attack – Failed



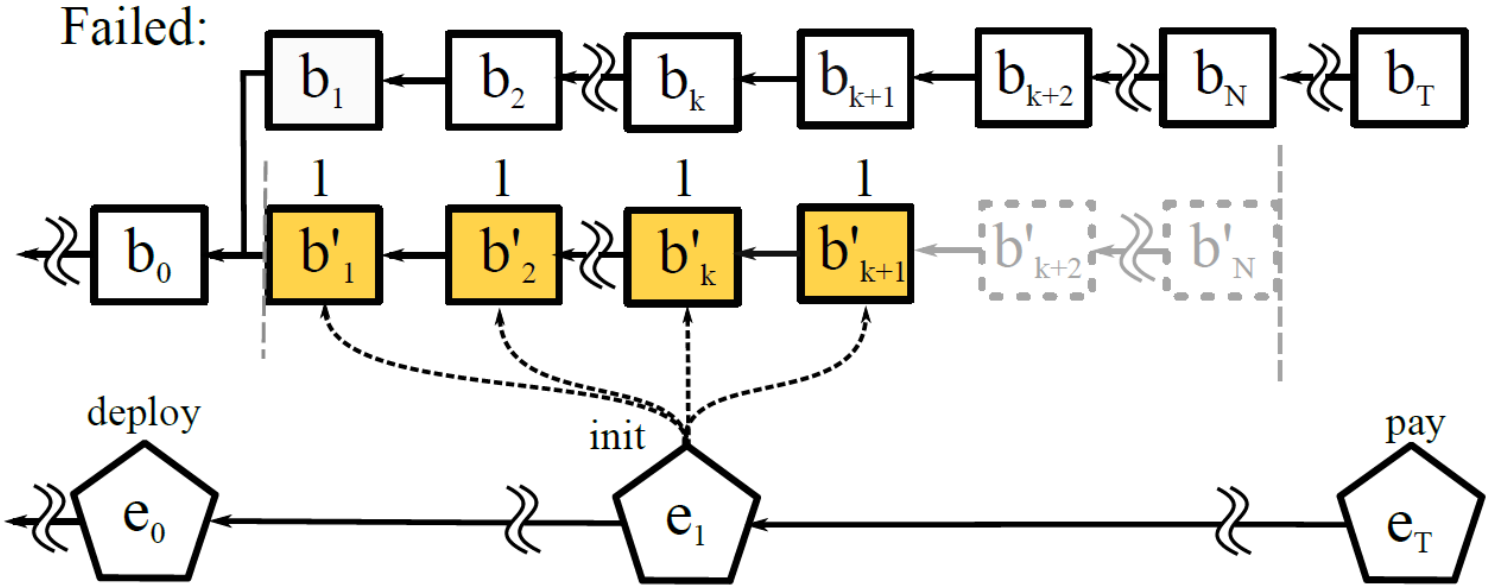
Out-of-Band TX Ordering Attack – Successful



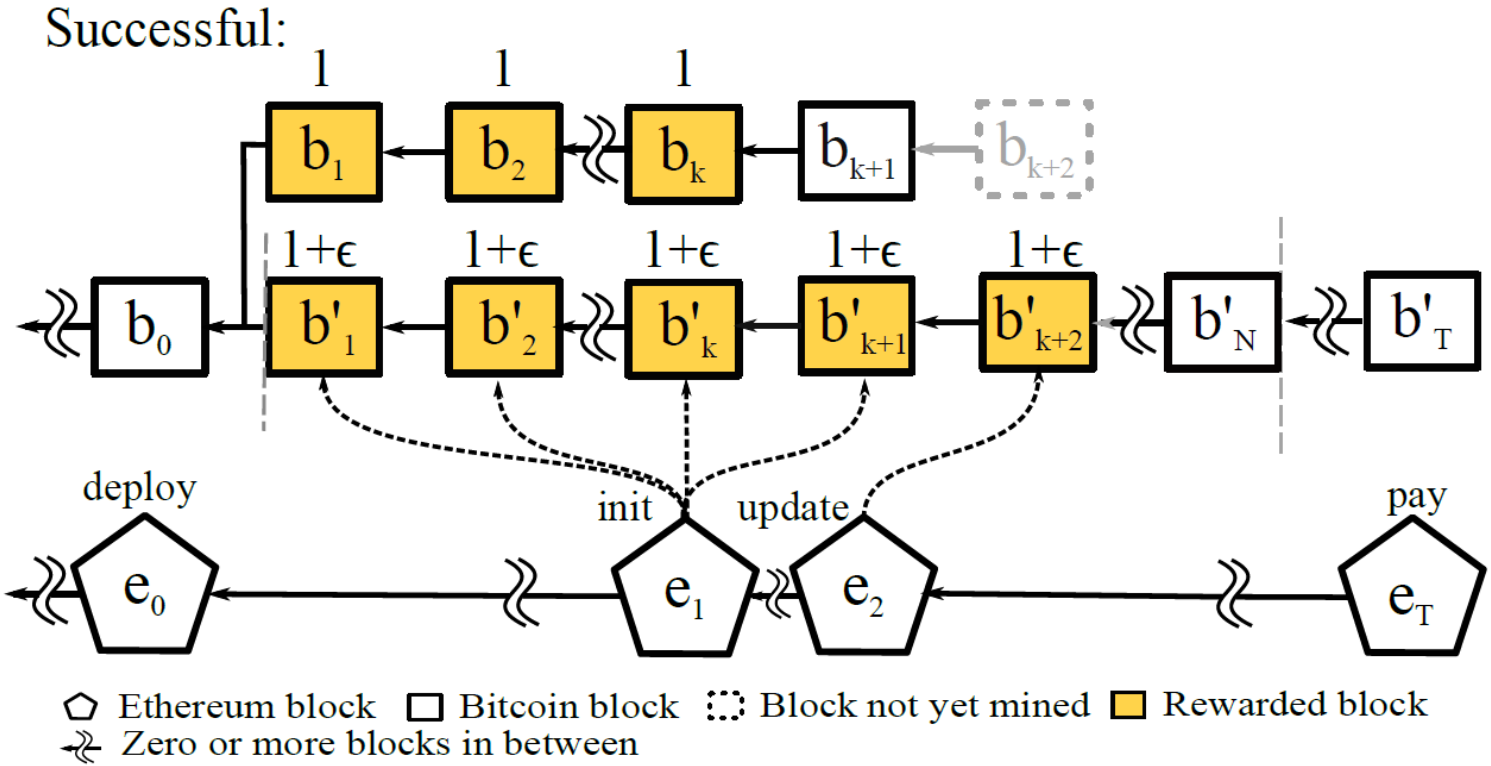
Out-of-Band TX Revision Attack



Out-of-Band TX Revision Attack – Failed



Out-of-Band TX Revision Attack – Successful




iCTF
2019
$> Scoreboard
$> Service List
$> Service Status
$> Service Exploits
$> Teams
Bushwhackers
Game ends in
00:23:48
current tick
121
Rank
Team
1
Bushwhacke
2
WE_OWN_YO
I am the one who
WeOwnYou
WE OWN YOU
二進CTF忍術


ACM
CCS
2016
23rd ACM Conference
on Computer and Communications Security
Hofburg Imperial Palace, Vienna, Austria
October 24-28, 2016
SBA
Research


EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Recent Top Publications

HydRand: Practical Continuous Distributed Randomness. IEEE S&P 2020.

Echoes of the past: Recovering blockchain metrics from merged mining. Financial Crypto 2019.

Proof-of-blackouts? how proof-of-work cryptocurrencies could affect power grids. RAID 2018.

Grid Shock: Coordinated Load-Changing Attacks on Power Grids, ACSAC 2017

I Have No Idea What I'm Doing - On the Usability of Deploying HTTPS, USENIX Security 2017

Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools, Euro S&P, 2017

The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection, RAID 2016

The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy, Financial Crypto 2016