The 83rd IFIP WG 10.4 Workshop (Winter 2023)

Workshop Chairs:

Jiangshan Yu (Monash University, AU)
Paulo Verissimo (KAUST, KSA)
Matti Hiltunen (AT&T Labs, USA)

Meeting Hosts:

Jiangshan Yu (Monash University, AU)
Dan Kim (University of Queensland, AU)
Gernot Heiser (UNSW, AU)

13 January 2023
Melbourne, Australia

MONASH University

Workshop Theme

The Future of Blockchains

CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

MARKETING MEDIA·MONEY

MEET THE WORLD-CLASS MAR

FUELING THE EVOLUTION OF ADVERT

FIND OUT MORE

BITCOIN

Bitcoin is the 'mother of all scams' and blockchain is most hyped tech ever, Roubini tells Congress

- One of the few economists who predicted the 2008 fi

CryptoLocker

Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send 2 BTC to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

<< Back

Next >>

THE TIMES | Today's sections | Past six days | Explore | Times Radio | Log in | Subscribe | Search

FTX 'is one of the biggest financial frauds in history'

Exchange's former chief Sam Bankman-Fried faces e

Katie Prescott, Callum Jones

Wednesday December 14 2022, 12.01am GMT, The Times

Sam Bankman-Fried is escorted out of a court building
DANTE CARRER/REUTERS

A US prosecutor in New York last night described the collapse of FTX, the failed crypto exchange, as "one of the biggest financial frauds in US history".

The US Department of Justice has charged Sam Bankman-Fried, founder and

CoinDesk

Policy | Technology | Web3 | Learn

Binance USD $1.00 +0.00% | Cardano $0.32719000 +1.61% | Dogecoin $0.07907942 +2.06% | Stellar $0.08169000 +2.70% | Polygon $0.37348851 +6.48%

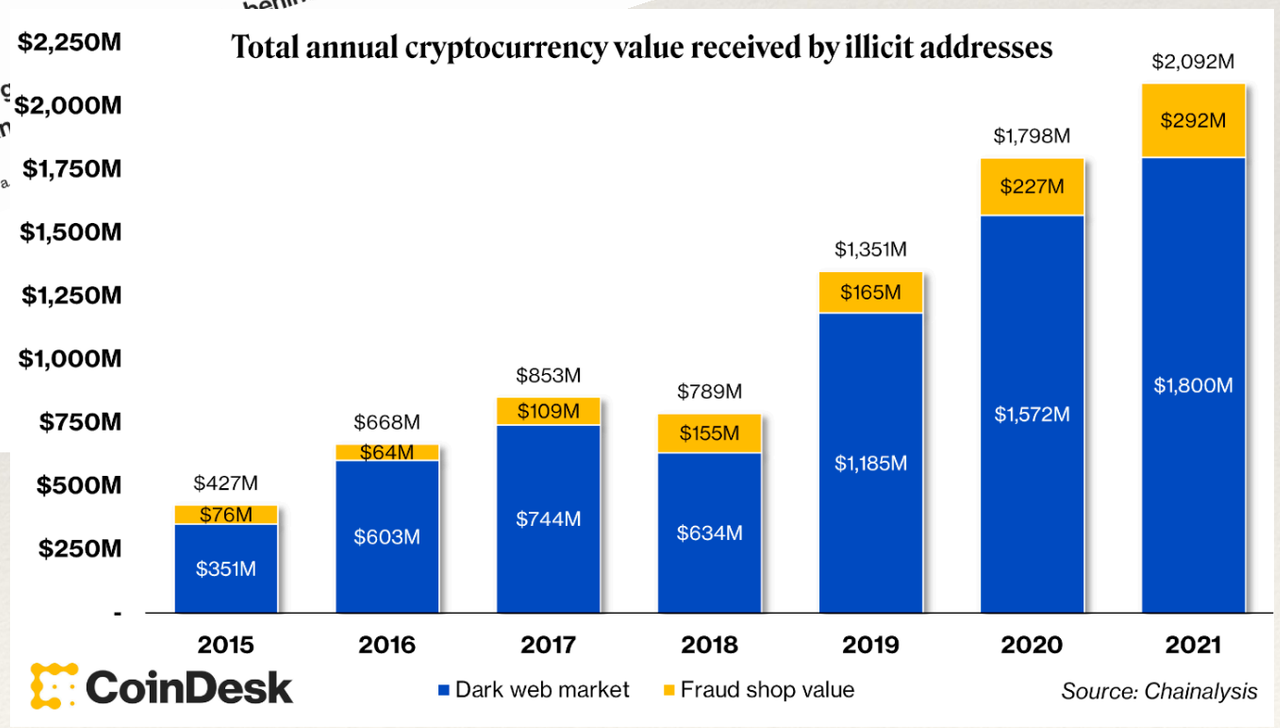
Policy

SEC Pursues $45M Scam Based in Fake Blockchain Technology

The U.S. securities agency is s
stealing from tens of thousan

By Jesse Hamilton Jan 5, 2023 at 10:18 a

behind what it says was a massive fraud



MONASH University

The Evolution of Trust

Uncertainty

Local

Institution

Technology

Scalability and Efficiency

MONASH University

National Transformation Program 2020

Saudi Vision 2030

By Marie Huillet

MAR 18, 2019

Australia Announces National Blockchain Roadmap and Further Boost to Government Funding

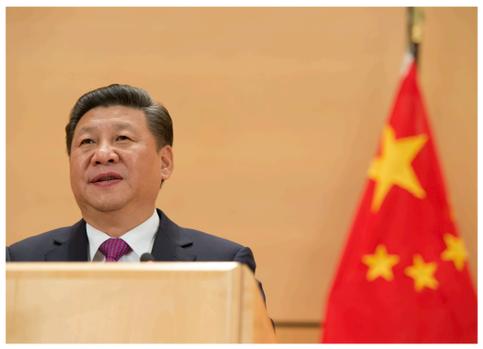
7293 Total views 489 Total shares Listen to article

www.news.cn 新华网 NEWS www.xinhuanet.com XINHUANET

Thursday, Sept

China's digital currency may be world's first: newspaper

Source: Xinhua | 2019-09-04 13:04:11 | Editor: Liu



Hard National Security Choices

LAWFARE

TOPICS HOME FOB BLOG JAN. 6 PROJECT REVIEWS AND ESSAYS AEGIS RESOURCE PAGES MORE

SINOTECH

China Sharpens Its Vision for the Digital Economy

By Brian Liu, Raquel Leslie Friday, January 21, 2022, 10:28 AM

ld's first central bank digital currency

ic wallets to support direct and peer-
a smartphone, but the final design
g Mu Changchun, deputy director of

e central ban
at commerc

certain payn
utions, said

Major Banks Sign Up for New EU Commission Blockchain App Association

Yogita Khatri

Nov 22, 2018 at 13:00 UTC

NEWS

Homeland Security

US Government Offering Up to $800K for Anti-Forgery Blockchain Solutions

CoinDesk

Terra $64.10 -2.38% Solana $93.90 -16.47% Cardano $0.988063 -13.91% Polkadot $18.16 -8.36% Stellar

Policy

China to Release National Blockchain Standard Next Year, Says Official: Report

While cracking down on on the cryptocurrency industry, Beijing is pouring resources into blockchain for governmental and enterprise use.

By Eliza Gkritsi · Oct 28, 2021 at 5:20 p.m. · Updated Oct 29, 2021 at 1:12 a.m.

NEWS

ions from

Anshun covered bridges in Chengdu, Sichuan. (Zain Lee/Unsplash)

European Commis

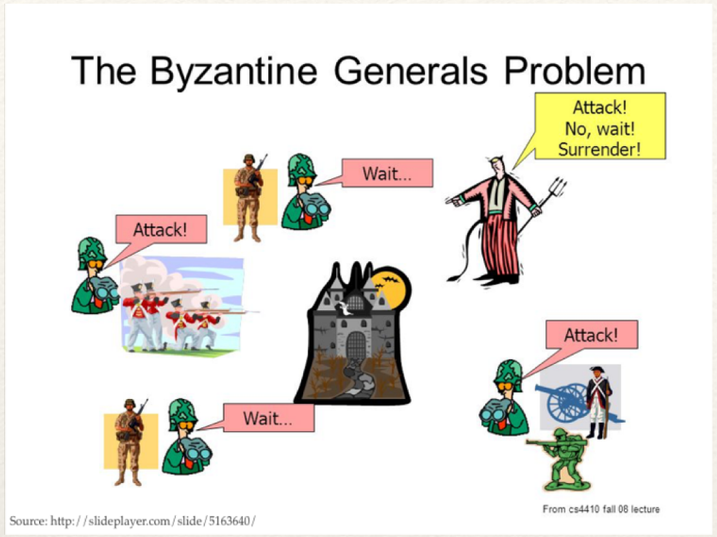
Digital Single

DIGIBYTE | 20 November 2018

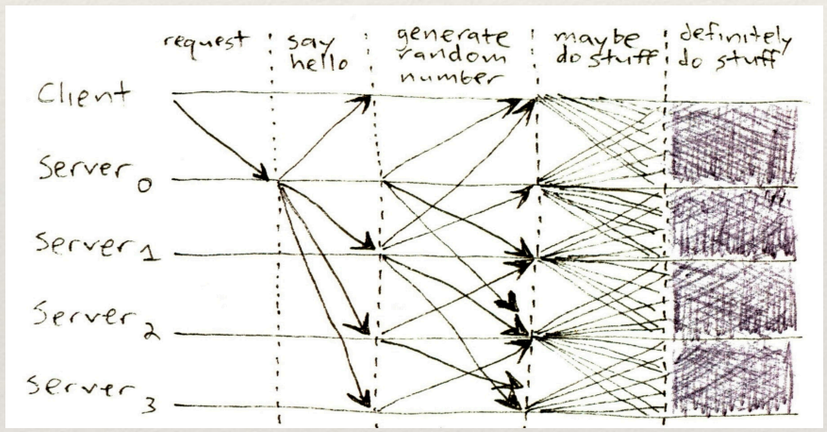
EU Blockchain Roundtable paves the way for Europe to lead in blockchain technologies

MONASH University

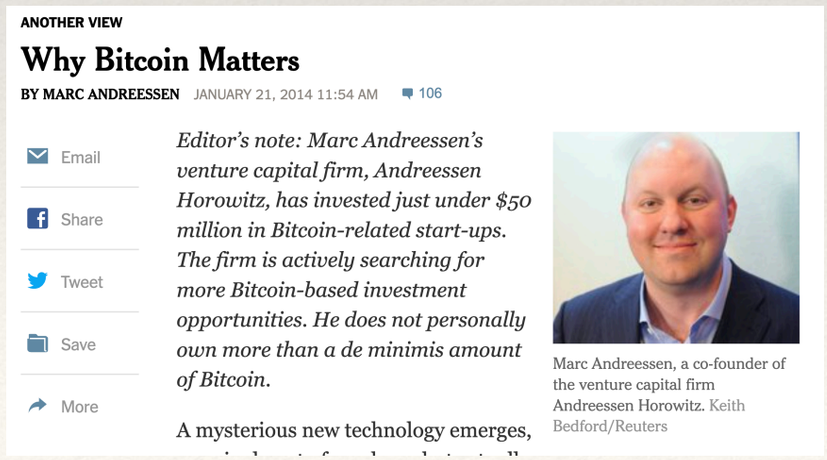
Dependability: 40 years of BFT research



Leslie Lamport, Robert E. Shostak, Marshall C. Pease. (1982)
"The Byzantine Generals Problem".
ACM Transactions on Programming Languages and Systems. 4 (3): 382–401.



"The Saddest Moment"
James Mickens, login Usenix Mag. 2014


ANOTHER VIEW

Why Bitcoin Matters

BY MARC ANDREESSEN JANUARY 21, 2014 11:54 AM 106

Email
Share
Tweet
Save
More

Editor's note: Marc Andreessen's venture capital firm, Andreessen Horowitz, has invested just under $50 million in Bitcoin-related start-ups. The firm is actively searching for more Bitcoin-based investment opportunities. He does not personally own more than a de minimis amount of Bitcoin.

A mysterious new technology emerges,

Marc Andreessen, a co-founder of the venture capital firm Andreessen Horowitz. Keith Bedford/Reuters

"Bitcoin is the first practical solution to a longstanding problem in computer science called the *Byzantine Generals Problem*"

Marc Andreesen, NYTimes, 2014

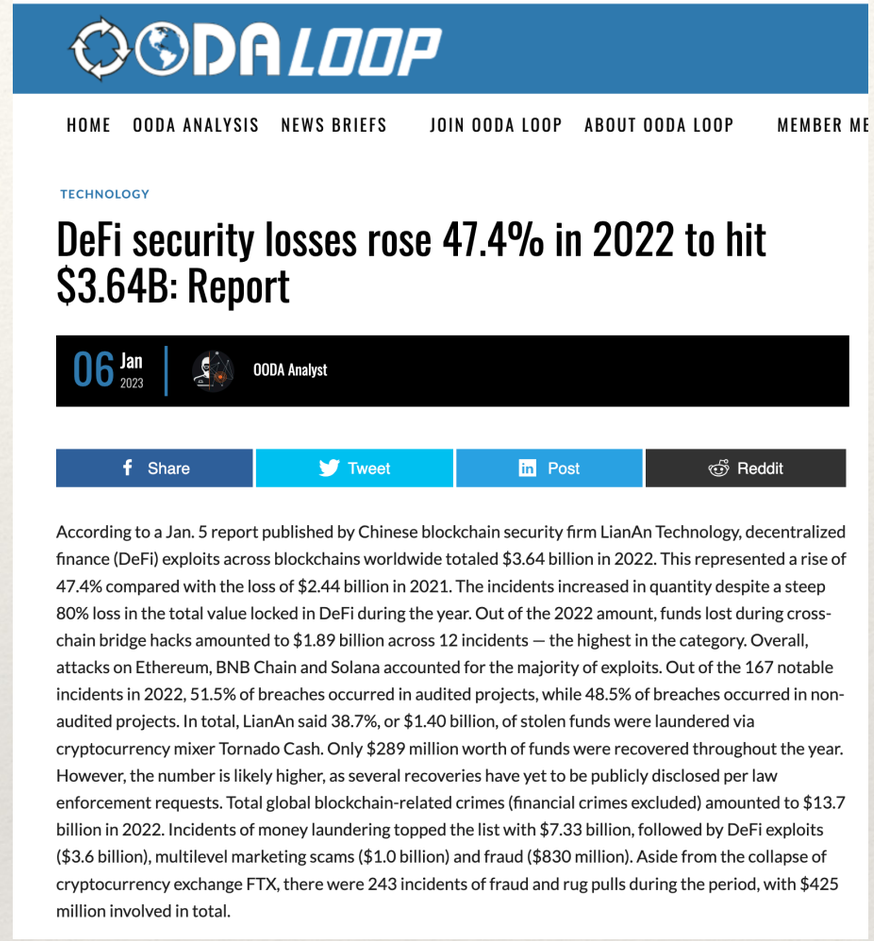
Investor of Mosaic
co-funder of Netscape
Co-funder of Silicon Valley VC firm Andreessen Horowitz

MONASH University

Some socio-technical dependability challenges

1. Smart contract security
2. Diversity of devices in permissionless networks
3. Authenticated data feed
4. Finance ecosystem and application systems
   (NFT, DeFi, DAO, DApp, GameFi, Metaverse, etc.)
5. Many more challenges:

- wallet security and key management
- Responsible and dependable law and regulation
- usability
- privacy
- deployment challenges
- post-quantum security
- human factor and culture impact
- …



OODA LOOP

HOME OODA ANALYSIS NEWS BRIEFS JOIN OODA LOOP ABOUT OODA LOOP MEMBER ME

TECHNOLOGY

DeFi security losses rose 47.4% in 2022 to hit $3.64B: Report

06 Jan 2023 | OODA Analyst

Share Tweet Post Reddit

According to a Jan. 5 report published by Chinese blockchain security firm LianAn Technology, decentralized finance (DeFi) exploits across blockchains worldwide totaled $3.64 billion in 2022. This represented a rise of 47.4% compared with the loss of $2.44 billion in 2021. The incidents increased in quantity despite a steep 80% loss in the total value locked in DeFi during the year. Out of the 2022 amount, funds lost during cross-chain bridge hacks amounted to $1.89 billion across 12 incidents — the highest in the category. Overall, attacks on Ethereum, BNB Chain and Solana accounted for the majority of exploits. Out of the 167 notable incidents in 2022, 51.5% of breaches occurred in audited projects, while 48.5% of breaches occurred in non-audited projects. In total, LianAn said 38.7%, or $1.40 billion, of stolen funds were laundered via cryptocurrency mixer Tornado Cash. Only $289 million worth of funds were recovered throughout the year. However, the number is likely higher, as several recoveries have yet to be publicly disclosed per law enforcement requests. Total global blockchain-related crimes (financial crimes excluded) amounted to $13.7 billion in 2022. Incidents of money laundering topped the list with $7.33 billion, followed by DeFi exploits ($3.6 billion), multilevel marketing scams ($1.0 billion) and fraud ($830 million). Aside from the collapse of cryptocurrency exchange FTX, there were 243 incidents of fraud and rug pulls during the period, with $425 million involved in total.

Workshop sessions

Session 1 – Blockchain for Critical Infrastructure (Chair: Dan Kim)

- Blockchain for Cyber-Physical Systems (Salil Kanhere, UNSW)
- Blockchain and database - a match made in the cloud (Anh Dinh, Deakin University)

Session 2 – Future Applications and Regulations (Chair: Sushmita Ruj)

- Blockchain in Action – Data61 Blockchain R&D (Shiping Chen, Data61-CSIRO)
- Know-Your-Transactions: Crypto Compliance and Transaction Monitoring (Lihong Tang, HyperLab)

Session 3 – Dependability and Security Aspects of Blockchain (Chair: Marcus Völp)

- Securing Blockchain Systems: Codes and Human (Yang Xiang, Swinburne University of Technology)
- Blockchain Replication: The Whys and The Hows (Miguel Correia, INESC-ID/IST)

Session 4 – Performance and Scalability Aspects of Blockchain (Chair: Anh Dinh, Deakin University)

- Coloring Smart Contracts and Other Musings About Efficient Blockchain Execution (Roy Friedman, Technion)
- Dumbo Protocols: Making Asynchronous Consensus Real (Qiang Tang, University of Sydney)