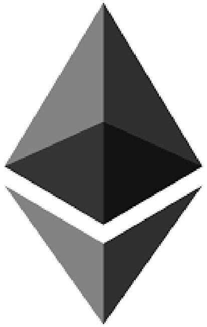
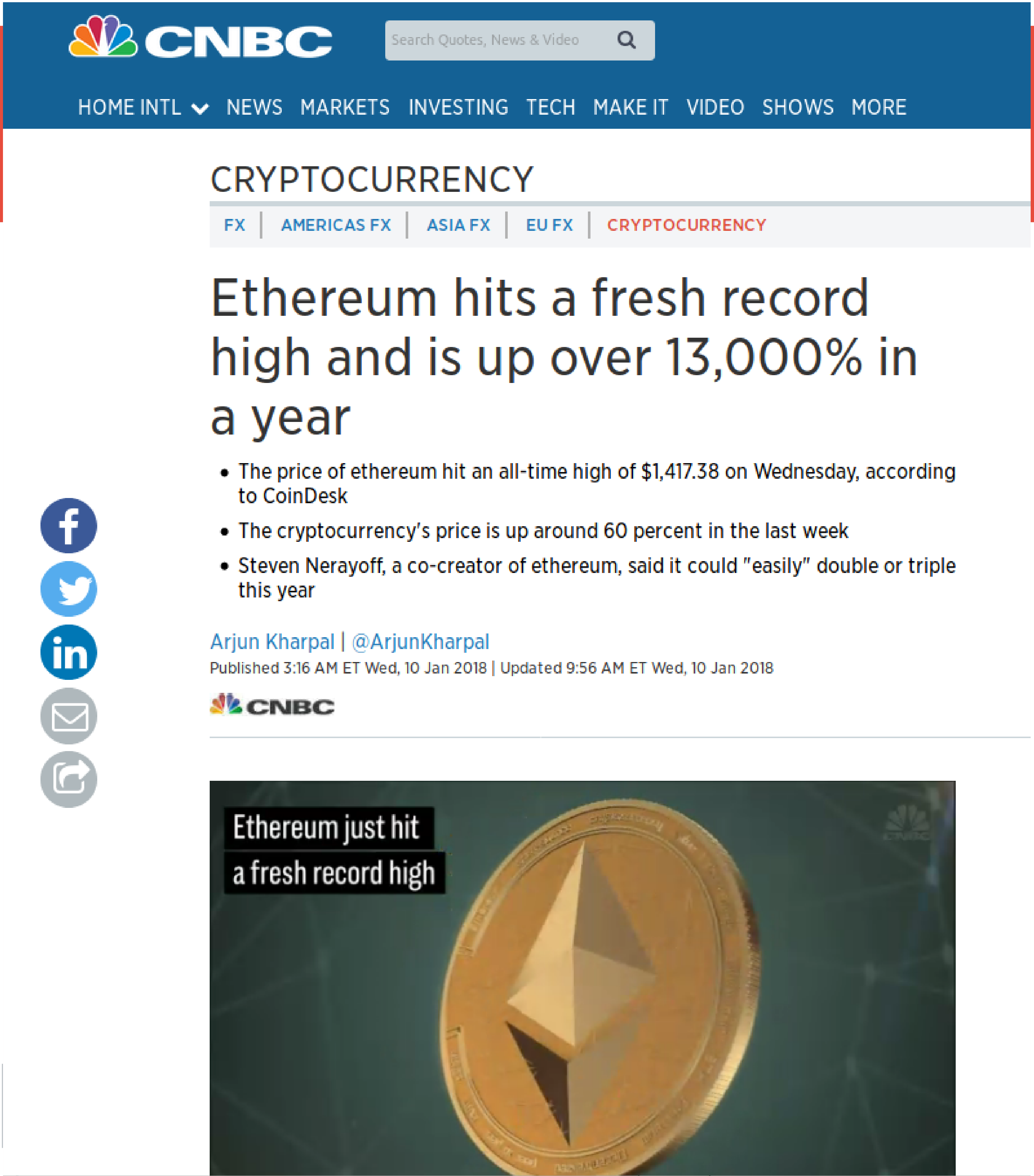
Blockchain and Cryptocurrencies Background



Cryptocoins

Virtual money

- money = something that I believe has value because I believe that others believe has value
  - no inherent value, only ability to exchange
- usually this collective hallucination (“consensus”) starts from a trusted authority
- in cryptocurrencies: decentralized consensus, possible without trusted authority

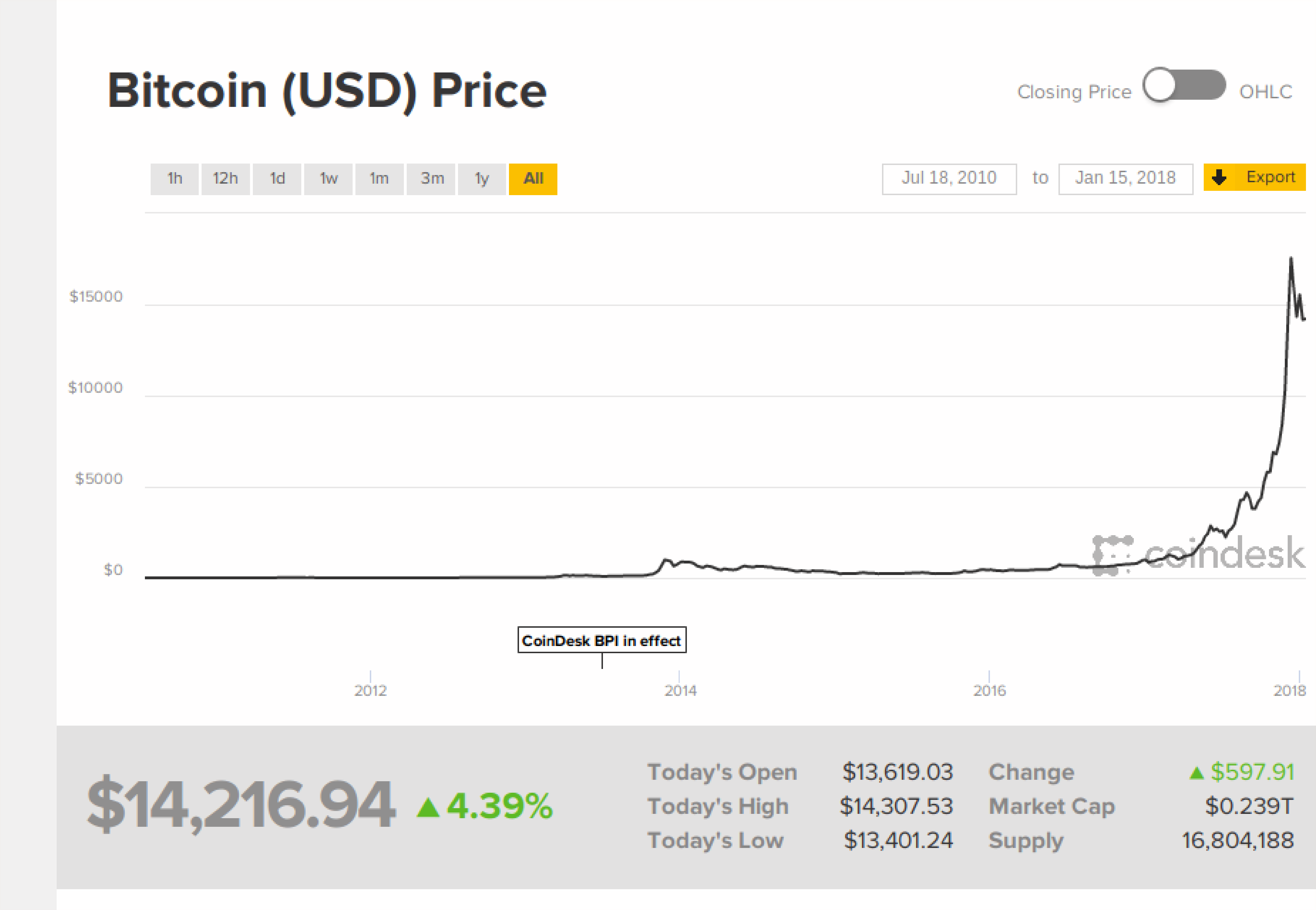


CRYPTOCURRENCY

Ethereum hits a fresh record high and is up over 13,000% in a year

- The price of ethereum hit an all-time high of $1,417.38 on Wednesday, according to CoinDesk
- The cryptocurrency's price is up around 60 percent in the last week
- Steven Nerayoff, a co-creator of ethereum, said it could "easily" double or triple this year

Arjun Kharpal | @ArjunKharpal
Published 3:16 AM ET Wed, 10 Jan 2018 | Updated 9:56 AM ET Wed, 10 Jan 2018



Bitcoin (USD) Price

Closing Price ○ OHLC

Jul 18, 2010 to Jan 15, 2018

$14,216.94 ▲4.39%

Today's Open	$13,619.03	Change	▲ $597.91
Today's High	$14,307.53	Market Cap	$0.239T
Today's Low	$13,401.24	Supply	16,804,188

Cryptography for our Purposes

Two main functions:

- unforgeable signatures, identification
- publication of boxes with locks that only I can open
  - an infinite number of boxes, of all possible sizes, can fit other boxes inside

“Have” = “Know”

Blockchain

A decentralized ledger of transactions

- maintained by untrusted peers

Continuously expanding chain of blocks

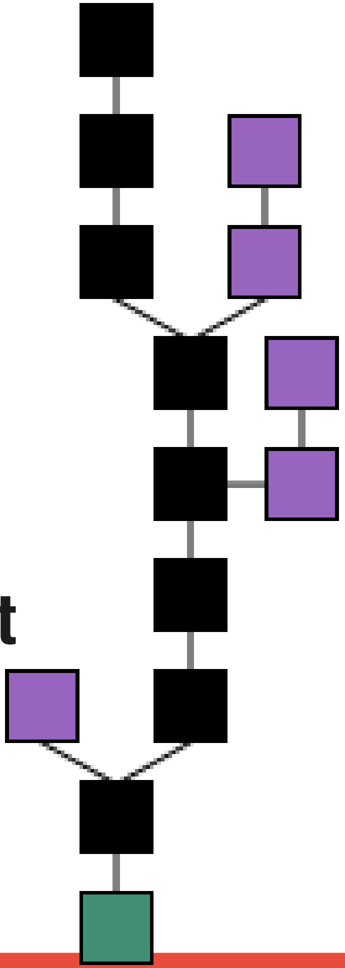
- longest chain is accepted as valid

Peers collect transactions, try to form new block

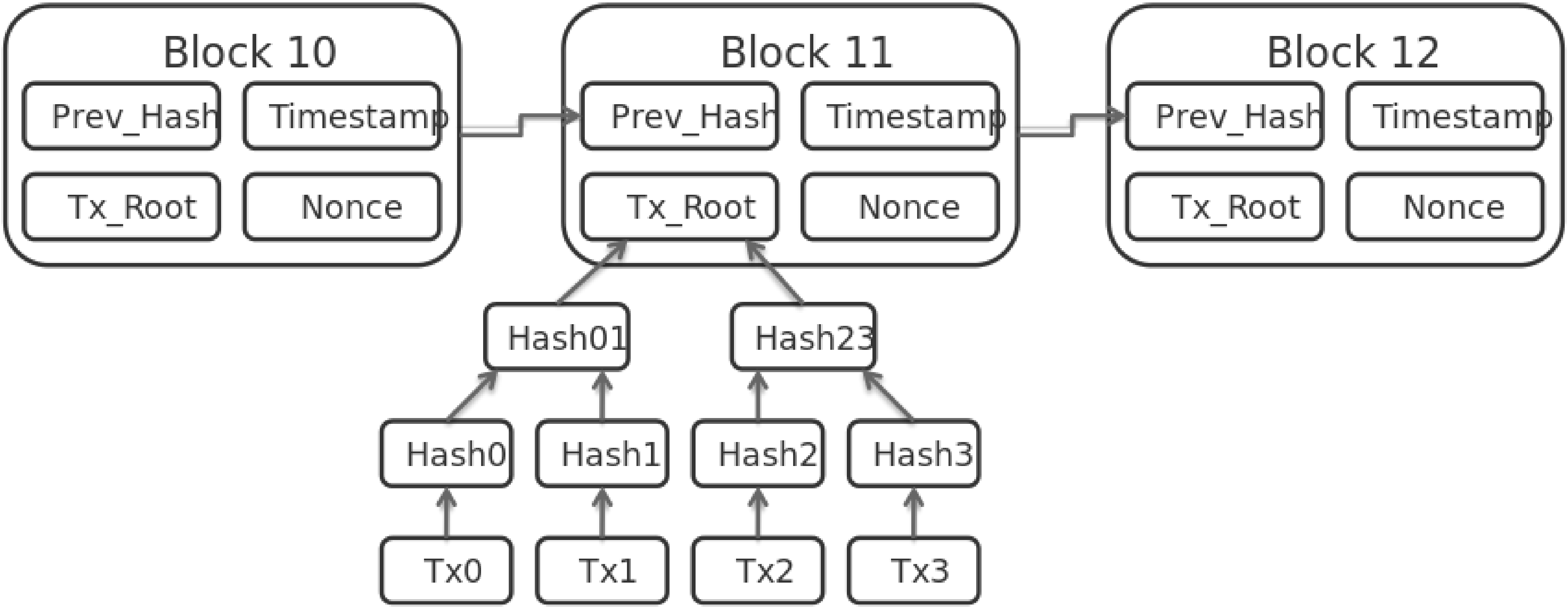
- by mining: solving a crypto-puzzle (proof of work)
- reward for solver ("miner")

Peers accept the block if transactions consistent

Blocks sign previous ones



Example Structure



Ethereum Blockchain

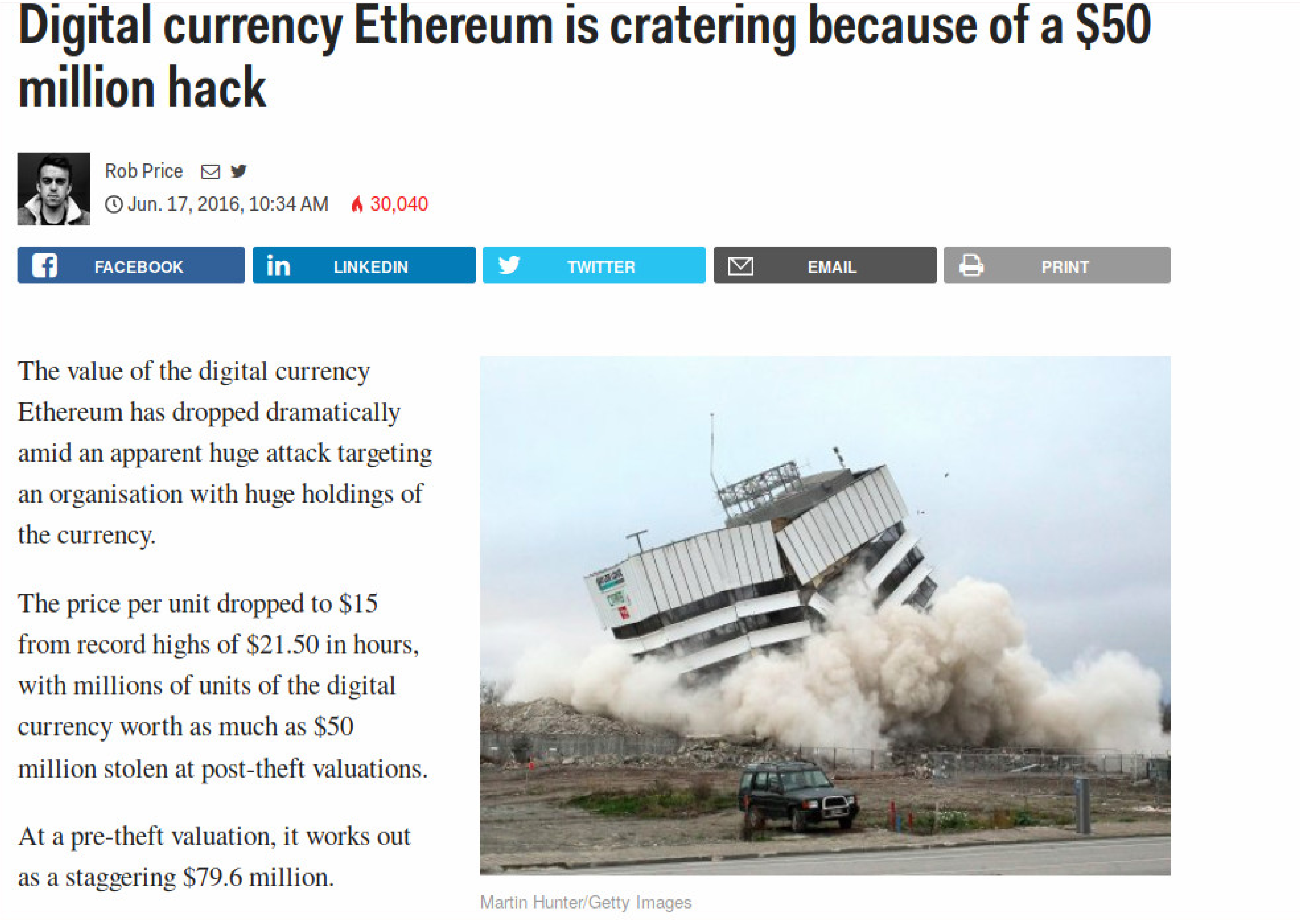
Main novelty: smart contracts

- complete programs, persistently on the blockchain
- accounts managed by smart contracts
- can call into them, starts a transaction

Gas: fee paid for running them

- translated in Ether (the Ethereum currency)
- bounded/hard coded

Security Threats



Digital currency Ethereum is cratering because of a $50 million hack

Rob Price

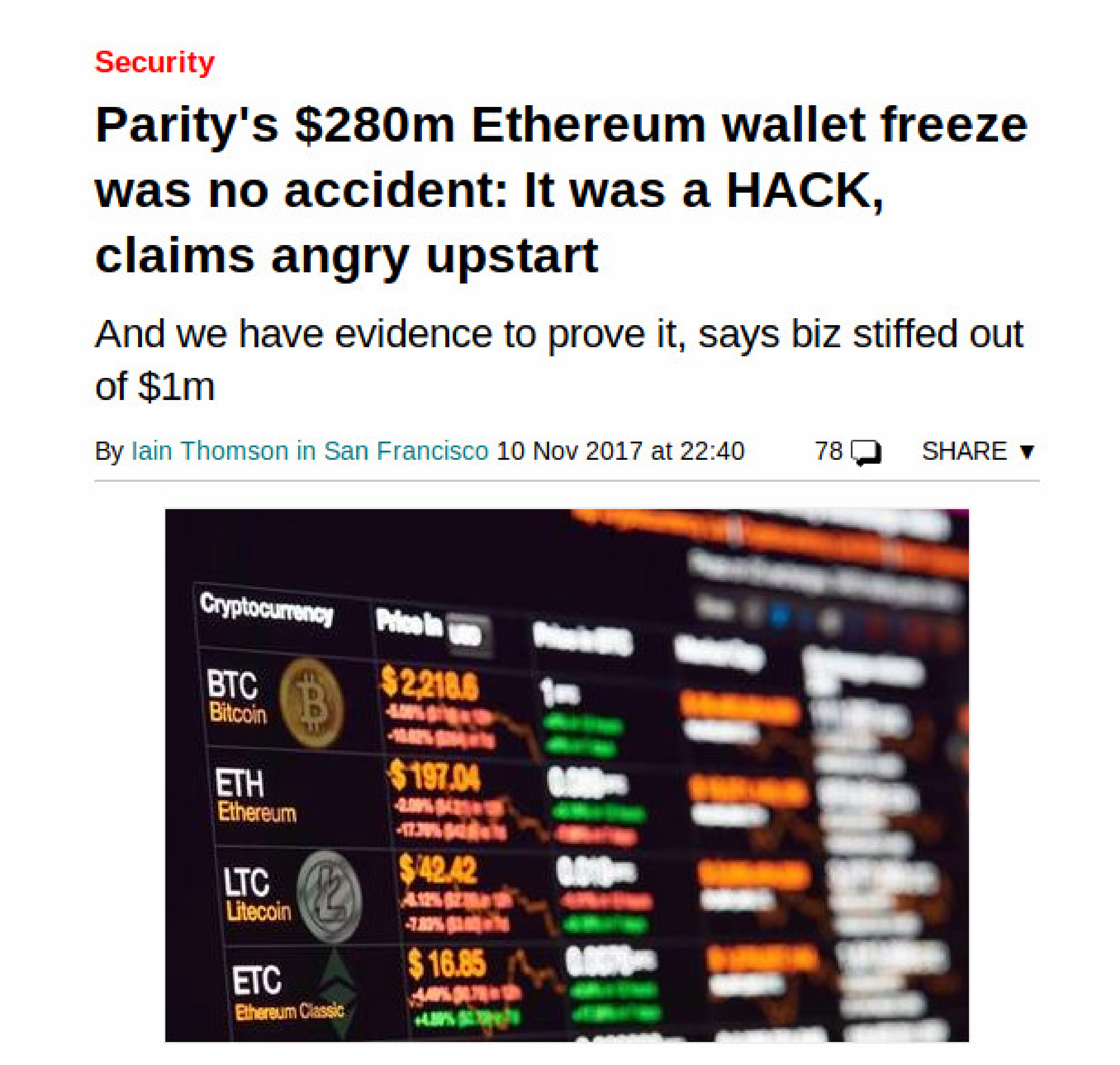
Jun. 17, 2016, 10:34 AM 30,040

The value of the digital currency Ethereum has dropped dramatically amid an apparent huge attack targeting an organisation with huge holdings of the currency.

The price per unit dropped to $15 from record highs of $21.50 in hours, with millions of units of the digital currency worth as much as $50 million stolen at post-theft valuations.

At a pre-theft valuation, it works out as a staggering $79.6 million.

Martin Hunter/Getty Images



Security

Parity's $280m Ethereum wallet freeze was no accident: It was a HACK, claims angry upstart

And we have evidence to prove it, says biz stiffed out of $1m

By Iain Thomson in San Francisco 10 Nov 2017 at 22:40   78   SHARE ▼

DAO Hack

```
contract SimpleDAO { ...
  function withdraw(uint amount) {
    if (credit[msg.sender] >= amount) {
      msg.sender.call.value(amount)();
      credit[msg.sender] -= amount;
} } }
```

DAO Hack

```
contract SimpleDAO { ...
  function withdraw(uint amount) {
    if (credit[msg.sender] >= amount) {
      msg.sender.call.value(amount)();
      credit[msg.sender] -= amount;
} } }

contract Attack {
  ... function() { dao.withdraw(10); } ...
}
```

Gigahorse Decompiler

Go to http://contract-library.com

EVM Bytecode Decompilation is Hard!

- Ethereum vs. JVM/CIL bytecode
  - No data structures, objects, methods or types
  - Stack depth can be different under different control flow paths
  - All control-flow edges (jumps) are variables, not constants
  - All functions of a contract are fused in one (jumps transfer control)

Decompilation: Stratification Points

Original Bytecode

1. Whole contract ctx & flow sensitive analysis

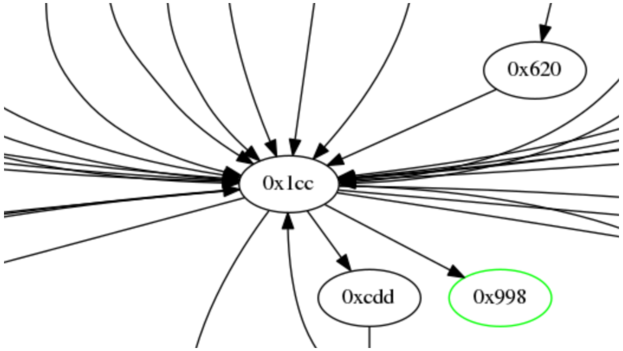
Whole program 3 address IR + CFG

2. Function extraction algorithms

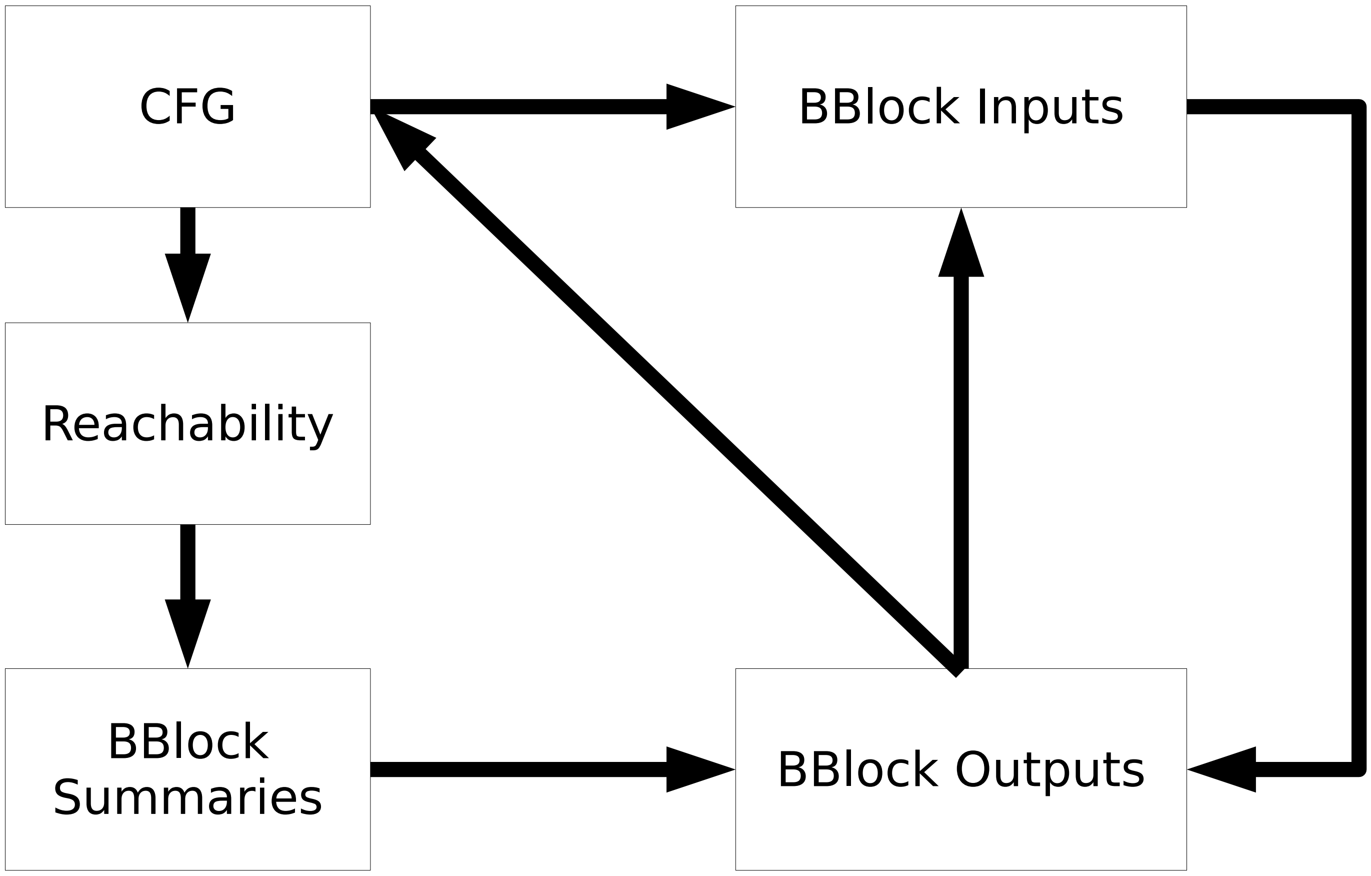
3. Function argument inference with flow sensitive analysis

3 address IR + function bounds + local CFGs

Functional 3-address code



Large-Scale Recursion



Heuristics: Functions That Return

```
         PUSH4 <return>  // return address
         PUSH4 0xFF      // push data
         PUSH4 <foo>     // function address
         JUMP            // jumps to ‘foo’
return:  JUMPDEST
         ...
         ...
foo:     JUMPDEST
         POP             // pops data
         JUMP            // jumps to ‘return’
```

Heuristics: Functions That Return

```
         PUSH4 <return>  // return address
         PUSH4 0xFF      // push data
         PUSH4 <foo>     // fu cti          ss
         JUMP            // j
return:  JUMPDEST
         ...
         ...
foo:     JUMPDEST
         POP             // pops data
         JUMP            // jumps to ‘return’
```

Detect flows of Return addresses

Heuristics: Finding More Functions

```
i = 1.
do {
  InFunction$_i$(block, block) ←  FunctionEntry$_{i-1}$(block).
  InFunction$_i$(next, func) ←
    InFunction$_i$(block, func),BlockEdge(block, next),
    !FunctionCall$_{i-1}$(block, next), !Function_Exit(block).

  FunctionCall$_i$(prev, block), FunctionEntry$_i$(block) ←
    InFunction$_i$(block, f1), InFunction$_i$(block, f2), f1 != f2,
    BlockEdge(prev, block), !FunctionExit(prev),
    !InFunction$_i$(prev, f1), !InFunction$_i$(prev, f2).

  i = i + 1.
} until fixpoint(FunctionEntry)
```

Output IR After Function Arg Inference

```
private 0xa3b (va1, va2, va3) → (int4, int16)
   f1 := CONST 0xa4b
   ret := CONST 0x3f
   v1, v2 := CALLPRIVATE(f1, ret, va2)
   r1 := SHA3(va2, va3)
   RETURNPRIVATE va1, r1, v1;
}
private 0xa4b(va1, va2) → (int4, int16)
...
}
```

Implementation

- A few (<5) KLoC of Datalog
- Decompiles 99.9% of entire Ethereum blockchain in 2 hours