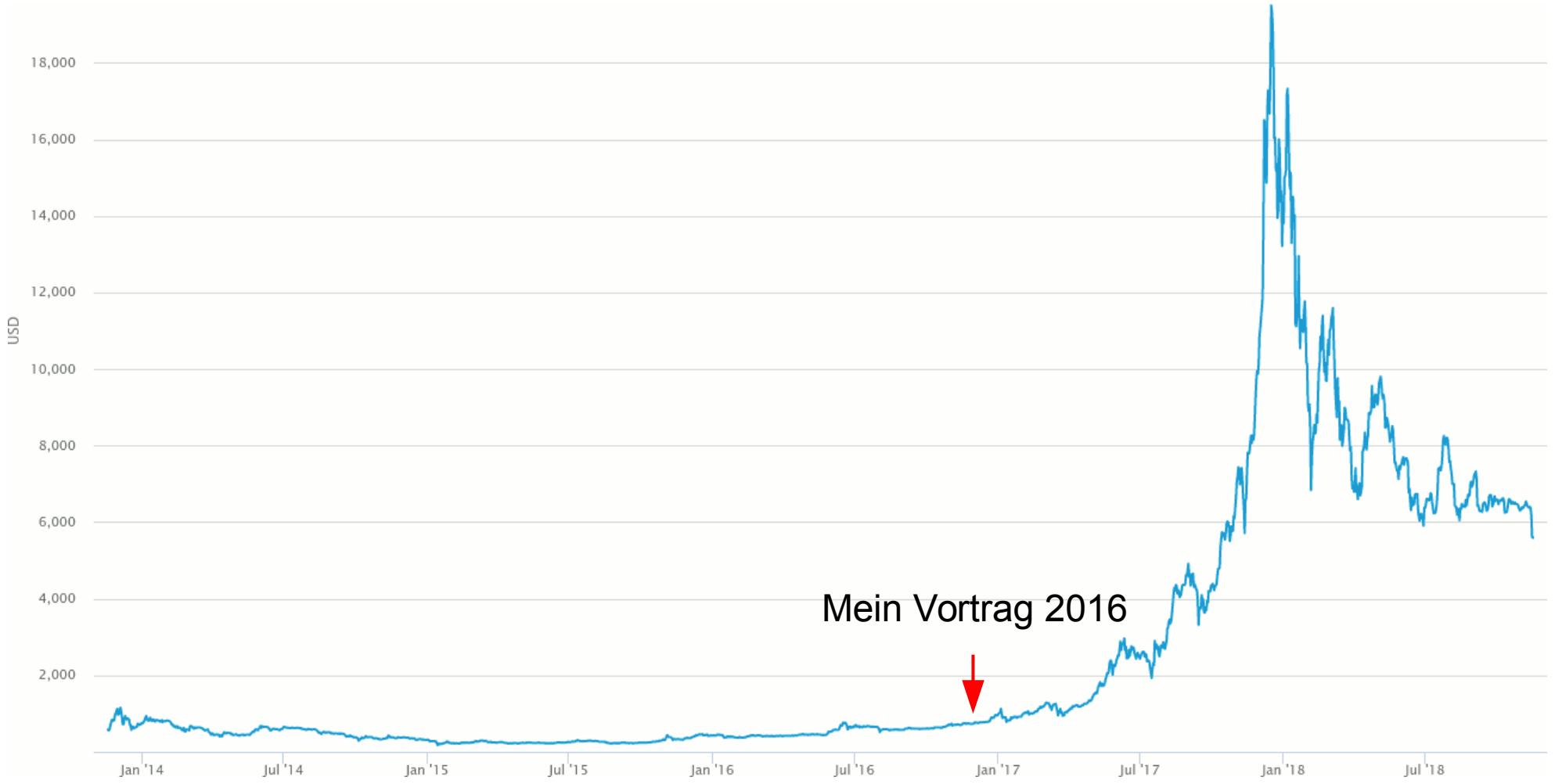
Blockchain-Anwendungen für Spiele und das Internet der Dinge:

CryptoKitty und IOTA

Matthias Brüstle

Nürnberg 2018-11-25

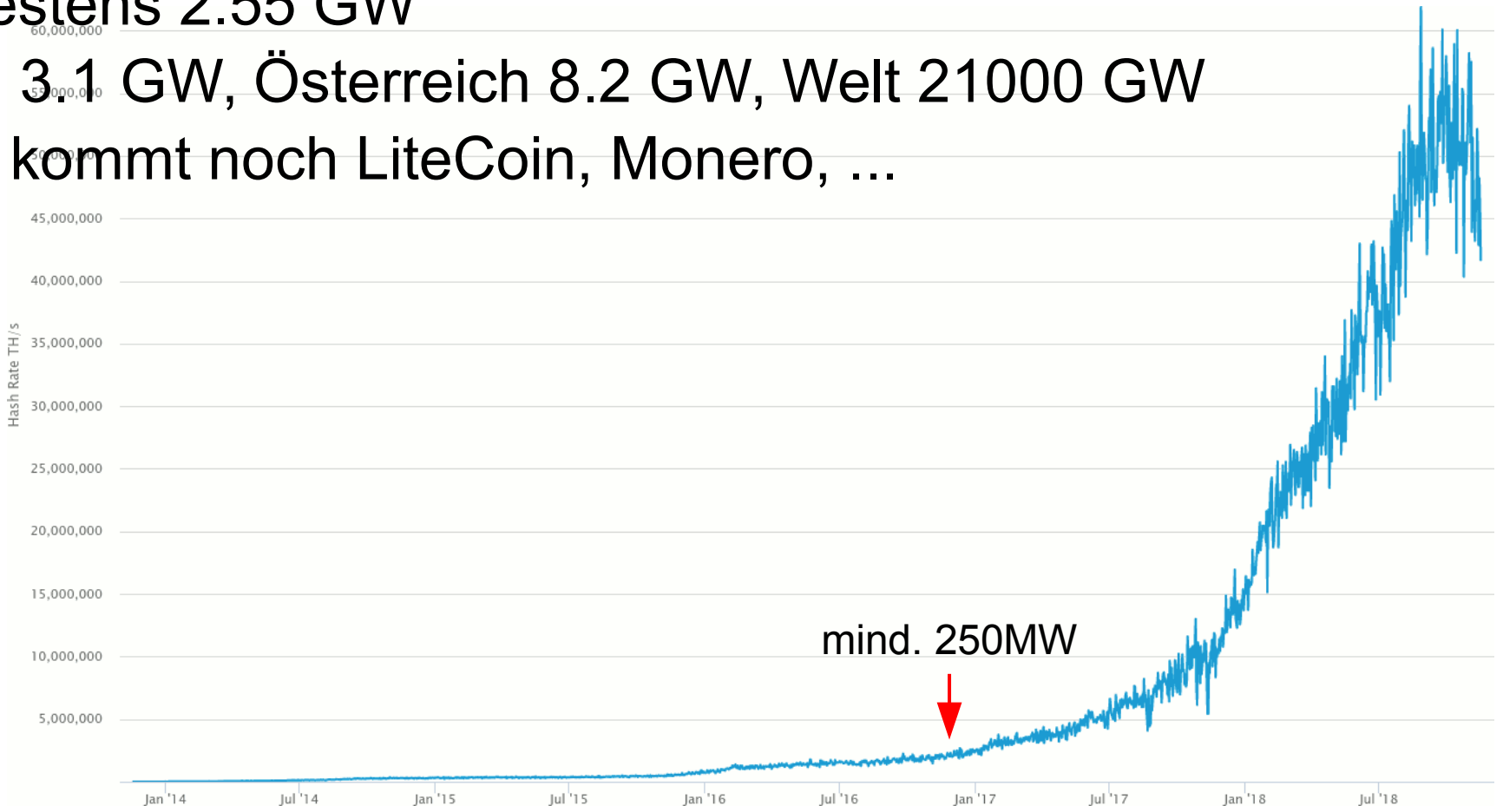
Aber erstmal wieder was zu BitCoin: Kurs in USD



https://www.blockchain.com/charts

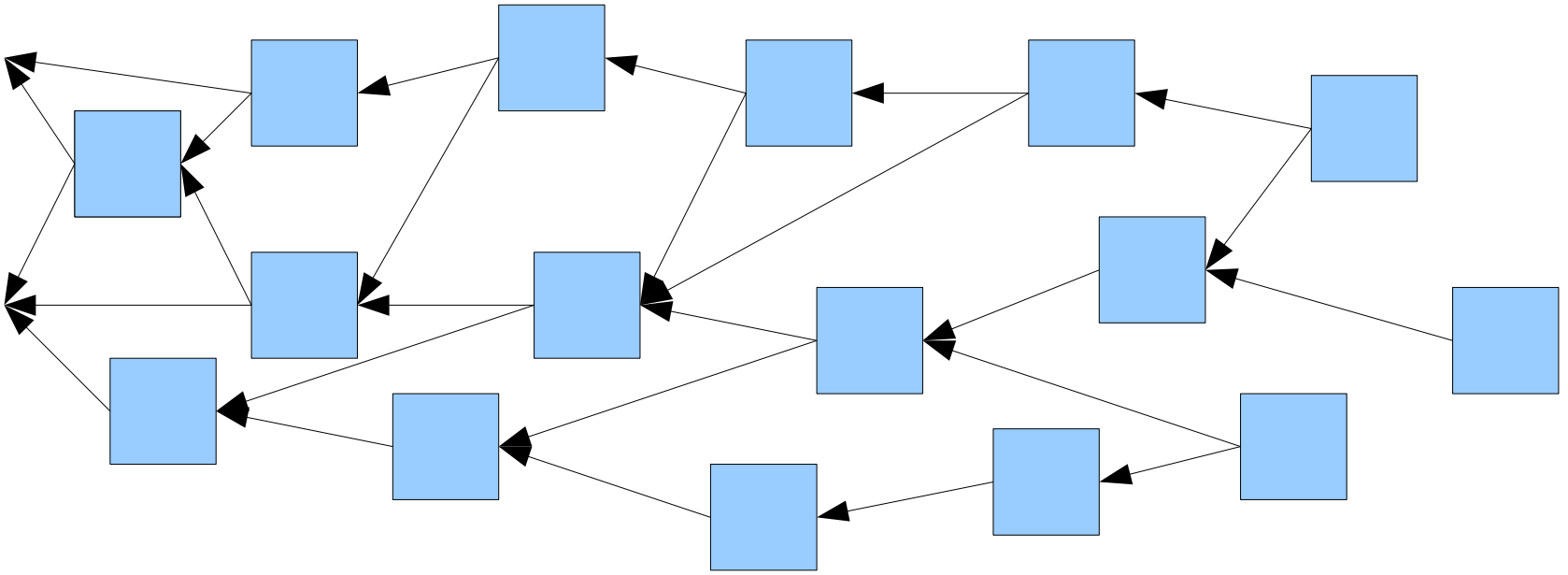
Hash Rate

- Über 60EH/s-Spitzenrate
- https://www.cell.com/joule/fulltext/S2542-4351 (April 2018): mindestens 2.55 GW
- Irland 3.1 GW, Österreich 8.2 GW, Welt 21000 GW
- Dazu kommt noch LiteCoin, Monero, ...



Miner-Einnahmen pro Transaktion

IOTA – The Tangle



The Tangle – Das Durcheinander

Was IOTA alles können soll

- IOTA wie IoT
- „Beseitigt das Skalierungsproblem durch Ersetzen der Blockchain durch The Tangle“
- „keine Miner“ -> keine Transaktionsgebühr
- „schnelle Transaktionen“
- „geringe CPU-Leistung nötig“
- „gegenseitige Bestätigung der Transaktionen im Transaktionsnetz“
- „Data First“ mit dem IOTA-Marketplace (so wie die Lindner-Wahlwerbung)

Pressestimmen zu IOTA

- DEUTSCHE TELEKOM & KRYPTOWÄHRUNGEN - Aktivitäten & Kooperationen mit IOTA (John Calian Blockchain-Experte der DT) (https://www.youtube.com/watch?v=knOKaDqxREQ)

- IOTA Co-Founder Dominik Schiener will be speaking to Germany's minister of the chancellery; Deutsche Telekom and Deutsche Bahn apparently into IOTA as well (https://helloiota.com/iota-co-founder-dominik-schiener-will-be-speaking-to-germanys-minister-of-the-chancellery/)

Probleme mit I(di)OTA: CURL

- IOTA verwendet(e) den selbstentwickelten, *trinären* Hash-Algorithmus CURL, weil trinäre Berechnungen effizienter wären
- Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks (weder kollisionssicher, noch pseudozufällig; mehrere gültige Transaktionen mit selbem CURL-Hashwert) (https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md)
- CURL teilweise ersetzt (Hard Fork) durch SHA-3/KECCAK-Variante obwohl es angeblich kein praktisches Problem ist (https://blog.iota.org/curl-disclosure-beyond-the-headline-1814048d08ef)
- Mehr Informationen: https://threadreaderapp.com/thread/976830315443507205.html
- Kein professioneller Umgang mit Kritik

Probleme mit I(di)OTA: Zentralisierung

- IOTA unsicher, wenn Angreifer 33% der Hashrechenleistung kontrolliert (https://forum.iota.org/t/iota-double-spending-masterclass/1311)
- „geringe CPU-Leistung nötig“ -> geringe Hashleistung des Systems -> leicht angreifbar
- Gegenmaßnahme: Bestätigungen („Milestones“) durch den „Coordinator“ (https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d)
- Dezentralisierung Light, aber eigentlich doch dezentral, weil der Coordinator nichts anders ist als Block 0 in Bitcoin
- „IOTA hat den Coordinator nie verschwiegen“ -> „Bitte link“ -> ...nüscht

Probleme mit I(di)OTA: Zentralisierung

- Keine Antwort auf Betrugsmöglichkeit durch den Coordinator (https://github.com/iotaledger/iri/issues/177)
- Auf Twitter: „not rational“, „doesn‘t need to be fixed“

„Redefining trust, value, and ownership“

Digital Collectibles

„Ethereum has recently created a new standard called the ERC721 token for tracking unique digital assets. One of the biggest use cases currently for such tokens are digital collectibles, as the infrastructure allows for people to prove ownership of scarce digital goods. Many games are currently being built using this technology, such as the overnight hit CryptoKitties, a game where you can collect and breed digital cats.“ (https://blockgeeks.com/guides/what-is-ethereum/)

„A new craze for virtual kittens is slowing down trade in one of the largest crypto-currencies. ... Etherscan has reported a sixfold increase in pending transactions on Ethereum since the game's release...“

Mein Hydrox

Hydrox

MartinHewitt
Owner

831207 Gen 0 Fast Cooldown

Bio

Yaya. I'm Hydrox. I'm alarming and gregarious, and sometimes even ghastly. Rita Ora wants me, but I'm more of a The Rolling Stones fan. I'll get started on our friendship bracelets.

Mewtations

impish
mouth

Cattributes

cashewmilk accent colour	dahlia eye colour	rorschach pattern	wiley eye shape
birman fur	bananacream base colour	coffee highlight colour	

43 Euro

CryptoKitties

- Virtuelle Katze, die kauf- und verkaufbar ist
- Zwitter
- Katzen zum Begatten „mietbar“
- Ein Bespringen erzeugt immer ein neues Cryptokätzchen
- Aussehen des Kindes wird durch Gene der Eltern und Mutation erzeugt
- Nach dem Paaren sind die Katzen eine Weile nicht mehr wuschig

Die Katz in Bit und Byte

- https://cryptokittydex.com/kitties/831207

Kitty #831207

Owner: 0xC32c054e8fBF20F661fF89bfa6DAD61e41E621a4
Born: July 3, 2018 at 6:11 AM UTC
Generation: 0
Block number: 0x59fa2b
Block hash: 0x7630126bae94049071af81250754ce524ade4fc349b476e043adb274da1e2863
Official profile: CryptoKitty #831207
Cattributes: wiley, bananacream, dahlia, impish, rorschach, cashewmilk, coffee, birman

Birman

- Dominant **Body** trait
- **~33.59%** chance of **Birman** being expressed in children
- Expressed in **~6.404%** of population
- Sells for **0.058 ETH** on average

Genes

Use the explorer below to browse this kitty's genes in different formats. The most useful format is named after @kaigani, th
genome.

kai hex binary

5gad 15gf b17c g966 626f eg16 72bd 9agg f2ff fefb 4937 7254

Sale history

Sold for 0.051 ETH	Jul. 3, 2018, 4:43 PM UTC
Sold for 0.078 ETH	Jul. 17, 2018, 9:09 PM UTC

Parents

This kitty has no parents!

Bebehs

This kitty has 0 bebehs

Immer noch jungfräulich

Noch biTiger und byTiger

- https://etherscan.io/tx/0x2108a6198cd6a951f19d4416fb576f49ddb5e173e44c68aad035731b672336c4

TxHash:	0x2108a6198cd6a951f19d4416fb576f49ddb5e173e44c68aad035731b672336c4
TxReceipt Status:	Success
Block Height:	5896747 (826474 Block Confirmations)
TimeStamp:	137 days 14 hrs ago (Jul-03-2018 06:11:47 AM +UTC)
From:	0xa21037849678af57f9865c6b9887f4e339f6377a
To:	Contract 0x06012c8cf97bead5deae237070f9587f8e7a266d (CryptoKitties_Core)
Tokens Transfered: (2 ERC-721 Transfers found)	From 0x0000000000000000.. To 0x06012c8cf97bead... For ERC-721 TokenID [831207] CK  From 0x06012c8cf97bead... To 0xb1690c08e213a35.. For ERC-721 TokenID [831207] CK 
Value:	0 Ether ($0.00)
Gas Limit:	400000
Gas Used By Transaction:	258359 (64.59%)
Gas Price:	0.000000075000000001 Ether (75.000000001 Gwei)
Actual Tx Cost/Fee:	0.01937692500025 Ether ($3.37)
Nonce & {Position}:	43902 | {59}
Input Data:	Function: createGen0Auction(uint256 _genes) MethodID: 0xc3bea9af [0]: 000023d2c011ee500cb7a0a5284ae6bc053054c425ef705ce735ca1a04630483 View Input As Decode Input Data

Noch biTiger und byTiger (2)

- https://etherscan.io/address/0x06012c8cf97bead5deae237070f9587f8e7a266d#code

```
contract KittyBase is KittyAccessControl {
  struct Kitty {
    // The Kitty's genetic code is packed into these 256-bits, the format is
    // sooper-sekret! A cat's genes never change.
    uint256 genes;

    uint32 matronId;
    uint32 sireId;

    // A non-zero value here is how we know a cat
    // is pregnant. Used to retrieve the genetic material for the new
    // kitten when the birth transpires.
    uint32 siringWithId;

    // The minimum timestamp after which this cat can engage in breeding
    // activities again. This same timestamp is used for the pregnancy
    // timer (for matrons) as well as the siring cooldown.
    uint64 cooldownEndBlock;

    uint16 generation;
  }
}
```

Noch biTiger und byTiger (3)

- https://etherscan.io/address/0x06012c8cf97bead5deae237070f9587f8e7a266d#code

```
contract ClockAuction is Pausable, ClockAuctionBase {
}

contract GeneScienceInterface {
  /// @dev given genes of kitten 1 & 2, return a genetic combination - may have a random factor
  /// @param genes1 genes of mom
  /// @param genes2 genes of sire
  /// @return the genes that are supposed to be passed down the child
  function mixGenes(uint256 genes1, uint256 genes2, uint256 targetBlock) public returns
(uint256);
}

contract KittyAccessControl {
  /// @dev Emited when contract is upgraded - See README.md for updgrade plan
  event ContractUpgrade(address newContract);
}
```

Was steht nicht im Smart Contract?

- Der Vertrag heisst „CryptoKitties“, aber das virtuelle Collectible könnte ein Nacktmull sein.
- Die Katzenbilder
- Die Bedeutung der Gene
- Teilweise die Spezialkatzen

Record!!!!!!!!!!

Für labbrige 600 ETH = 170000 USD (damals):

https://etherscan.io/tx/0x09bd9357d29bef46a68a6ffdc915304288d69ca089412a2edec0c8d370b3944b

Wahrscheinlich echte Rekorde

CryptoKitties Sales

~ Made by @nieldlr. (Psst... I'm building a decentralized Patreon. Read more here.) ~

Total Sales: 472103
Total Unique Kittens Sold: 374545
Total Ether Sold: 52581.59 ether
Total USD Sold: $26770381.81

Average Sale Price: $56.70
Median Sale Price: $9.03

Kitty Info	Pricing			Details
ID	Ether	USD (at time of sale)	USD (current value)	Sale Date
896775	Ξ 600.0000	$172625.79	$104400	9/4/2018, 6:21:26 AM
18	Ξ 253.3368	$110707.16	$44080.6	12/7/2017, 4:28:18 AM
4	Ξ 247.0000	$107816.49	$42978	12/6/2017, 8:41:57 PM
1	Ξ 246.9255	$114481.59	$42965.04	12/2/2017, 9:32:36 PM
21	Ξ 237.5228	$104404.35	$41328.97	12/8/2017, 10:31:03 AM
22	Ξ 225.0000	$98899.88	$39150	12/8/2017, 10:34:36 AM
5	Ξ 222.0000	$101600.52	$38628	12/5/2017, 5:45:01 PM
7	Ξ 190.0468	$87677.34	$33068.15	12/4/2017, 8:45:47 PM
35	Ξ 188.8897	$85000.53	$32866.8	12/6/2017, 8:18:02 AM
87	Ξ 179.0734	$79008.45	$31158.78	12/6/2017, 7:11:42 PM
101	Ξ 175.7532	$81993.25	$30581.05	12/4/2017, 4:28:4

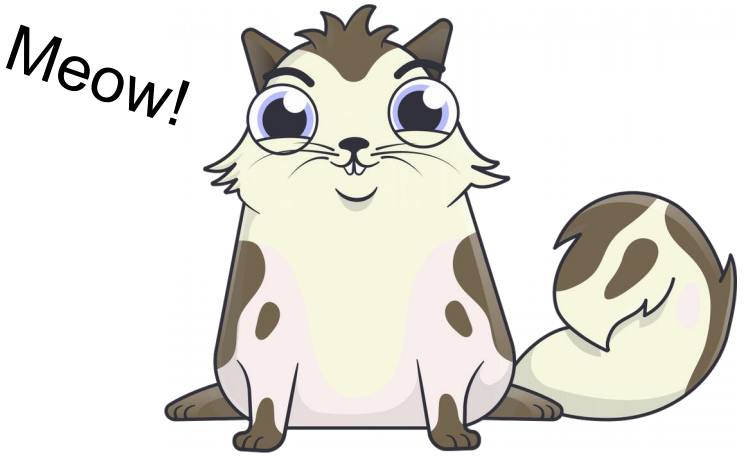
Smart Contracts, Dumb Bugs

- https://hackernoon.com/how-the-170-million-ethereum-bug-could-have-been-prevented-819053c3b2cb?gi=2d255e8bef17:
  Übersetzt: „Am 7. November ist der Ethereum-Nutzer Parity über einen Fehler gestolpert, der ihm erlaubt einen Vertrag, der Multisignatur-Börsen betrifft, in eine normale Börse umzuwandeln. Nach dem Umwandeln des Vertrages konnte der Nutzer sich selbst zum Eigentuemer machen. Verblüfft darüber was er machen konnte, hat der den Vertrag versehentlich gesperrt, was den Zugriff auf alle betreffenden Börsen unmöglich gemacht hat.“

  170 Millionen Dollar lösten sich in einem Wölkchen Logik auf.

- https://news.bitcoin.com/25-of-all-smart-contracts-contain-critical-bugs/:
  „In einem viertel der Projekte (gesamt 1 Milliarde USD), die Hosho auditiert hat, wurden kritische Fehler gefunden und in etwa 60$ alle Projekte war zumindest ein Sicherheitsproblem.“

- https://applicature.com/blog/smart-contract-mistakes-bugs-pitfalls:
  Übersetzt: „Dem GitHup-Nutzer Devops199 fror eine 285-Millionen-Dollar-Transaktion wegen einem verbreiteten Fehler ein.“



Saenks!

PS: https://github.com/ethereum/wiki/wiki/Ethereum-Virtual-Machine-(EVM)-Awesome-List

Matthias Brüstle

Nürnberg 2018-11-25