RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: CRYP-W12

CRYPTOGRAPHY PANEL
TOPIC: CRYPTOCURRENCIES

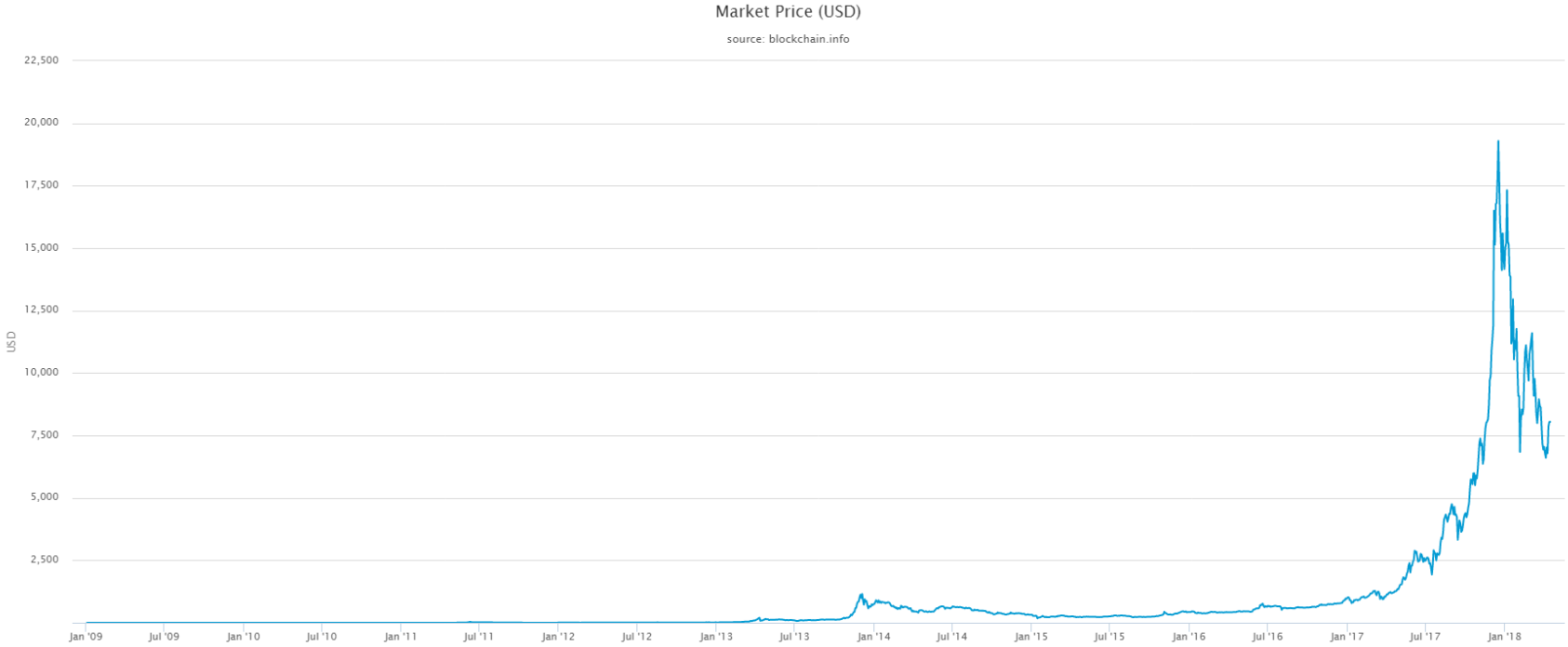
MODERATOR: **Bart Preneel**
Professor, KULeuven
@COSICbe

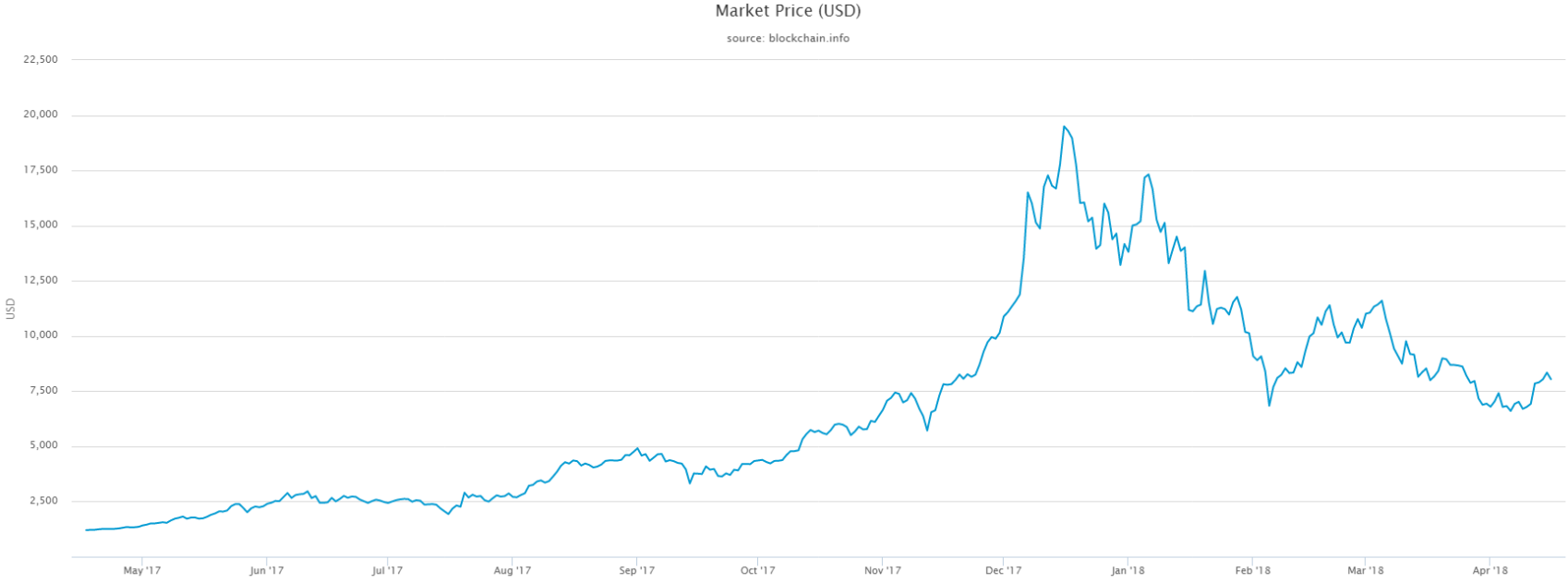
PANELISTS: **Matthew Green**
Assistant Professor, Johns Hopkins Information Security Institute
@matthew_d_green

Charles Hoskinson
CEO,
Input Output HK
@IOHK_Charles

Silvio Micali
Professor,
MIT Computer Science and Artificial Intelligence Laboratory

Adi Shamir
Borman Professor of Computer Science, The Weizmann Institute, Israel


Market Price (USD)
source: blockchain.info
USD
22,500
20,000
17,500
15,000
12,500
10,000
7,500
5,000
2,500
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18


Market Price (USD)
source: blockchain.info
USD
22,500
20,000
17,500
15,000
12,500
10,000
7,500
5,000
2,500
May '17
Jun '17
Jul '17
Aug '17
Sep '17
Oct '17
Nov '17
Dec '17
Jan '18
Feb '18
Mar '18
Apr '18

> 1500 Cryptocurrencies
Total Market Cap: B$331

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$137,152,142,247	$8,075.76	16,983,187	$6,524,180,000	-0.47%	0.72%	18.36%
2	Ethereum	ETH	$50,730,448,494	$513.05	98,879,740	$1,726,770,000	-0.41%	1.26%	25.84%
3	Ripple	XRP	$26,296,621,375	$0.672156	39,122,794,968 *	$407,726,000	-0.29%	2.57%	37.06%
4	Bitcoin Cash	BCH	$13,285,572,214	$777.91	17,078,613	$329,049,000	0.06%	2.52%	20.12%
5	Litecoin	LTC	$7,756,167,648	$138.19	56,125,213	$508,788,000	-0.53%	8.51%	21.09%
6	EOS	EOS	$7,010,268,415	$8.77	798,965,649 *	$773,136,000	-1.56%	8.41%	45.81%
7	Cardano	ADA	$6,587,420,447	$0.254075	25,927,070,538 *	$587,620,000	-0.05%	3.13%	63.91%
8	Stellar	XLM	$5,813,425,480	$0.313086	18,568,142,554 *	$97,656,200	1.60%	12.12%	56.93%
9	IOTA	MIOTA	$4,523,213,015	$1.63	2,779,530,283 *	$58,310,600	-0.33%	3.26%	62.10%
10	NEO	NEO	$4,422,054,000	$68.03	65,000,000 *	$103,024,000	-0.07%	3.27%	31.34%
11	Monero	XMR	$3,210,491,532	$201.41	15,939,764	$37,995,000	-0.17%	4.77%	21.48%
12	NEM	XEM	$3,070,800,000	$0.341200	8,999,999,999 *	$45,240,500	0.47%	3.01%	47.51%

Algorand

A **Unique** Foundational Blockchain
Development from **First Principles**
A Deep Roadmap of **Innovations**

Main Idea: Message-passing *Byzantine Agreement*
Main Approach: *PURE* PoS ~~Delegated~~ ~~Bonded~~
Main Assumption: Honest Majority of Money

’s Two Magic Phases

(Magic replaced by Mathematics)

PHASE 1

A random user is selected among **all** users
(with prob. proportional to the amount of money he/she has in the system)
His/her public key become known to all users
He/She proposes, signs, and propagates a new block

PHASE 2

1,000 users are randomly selected among all users
Their keys magically become known to all users
They reach agreement on (and sign) the block proposed by the first user.

's Technical Advancements

- VRFs and **Cryptographic Self-Selection** to Blockchains
  (allow users to secretly, fairly, and provably select themselves)

- A **New** and **Super Fast** Byzantine agreement
  (allows to agree on a new block while the block propagates)

- **Player Replaceability**
  (prevents a honest user to be corrupted in the middle of a protocol)

- AND MUCH MORE…
  (Stay tuned!)

's Basic Properties

- No Forks, No Miners, No Proof of Work
- Trivial Computation, Perfect Scalability, Transaction Finality
- Great Security against protocol and network attacks

Plus:

- Security against arbitrary partitions
- Flexible Governance without hard forks
- Secure Incentives
- Deep Roadmap

What a blockchain always wanted to be….

Thank
You!