BLOCKCHAIN & CRYPTOCURRENCIES

Crypto Canon

by Sonal Chokshi, Chris Dixon, Denis Nazarov, Jesse Walden, and Ali Yahya

Here's a list — building on and including Chris' last roundup — of crypto readings and resources. It's organized from building blocks and basics; foundations (& history); and key concepts and beginners' guides — followed by specific topics such as governance; privacy and security; scaling; consensus; cryptoeconomics and investing; fundraising and token distribution; decentralized exchanges; stablecoins; and cryptoeconomic primitives (crytocollectibles, curation markets, games). We also included a section with developer tutorials and practical guides, as well as other resources, such as newsletters and courses, at the end.

We'll soon be updating this regularly at crypto.a16z.com, for now we'll keep it updated here. You can also find most of a16z's writings, posts, and videos on the topic at a16z.com/crypto.

* * *

Building Blocks and Basics

WTF is the blockchain? — understanding the problem it solves before defining it

by Mohit Mamoria

https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348

Ever wonder how bitcoin (and other cryptocurrencies) actually work?

from 3Blue1Brown

https://youtu.be/bBC-nXj3Ng4

How the bitcoin protocol actually works

by Michael Nielsen

http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

Ethereum in 25 minutes

by Vitalik Buterin

https://youtu.be/66SaEDzlmP4

How does Ethereum work, anyway? — how it functions at a technical level, without complex math

by Preethi Kasireddy

https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369

Decrypting crypto, from bitcoin and blockchain to ICOs

by Alex Rampell

https://a16z.com/2017/12/08/summit-crypto-alex-rampell/

Cryptographic hash function — what they are, properties of, etc.

by Khan Academy

https://youtu.be/0WiTaBI82Mc

basic primer on blockchain — ledger basics, why it matters

Chris Berg, Sinclair Davidson, and Jason Potts

https://medium.com/@cryptoeconomics/the-blockchain-economy-a-beginners-guide-to-institutional-cryptoeconomics-64bf2f2beec4

basic terminology for Ethereum — from gas to dapps (distributed apps)

by Matt Condon

https://medium.com/@mattcondon/getting-up-to-speed-on-ethereum-63ed28821bbe

a basic glossary of terms — a few short and simple definitions

https://tangelo.co/insights/blog/techs-must-have-reference-guide-to-blockchain-and-cryptocurrency

Foundations (& History)

Bitcoin whitepaper (2009): A Peer-to-Peer Electronic Cash System

by Satoshi Nakamoto

https://bitcoin.org/bitcoin.pdf

Ethereum whitepaper (2013+): A Next-Generation Smart Contract and Decentralized Application Platform

by Vitalik Buterin et al

https://github.com/ethereum/wiki/wiki/White-Paper

The Byzantine Generals Problem (1982)

by Leslie Lamport, Robert Shostak, and Marshall Pease

https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

The Agoric papers series (1988)

by Mark Miller and K. Eric Drexler

https://e-drexler.com/d/09/00/AgoricsPapers/agoricpapers.html

The idea of smart contracts (1997)

by Nick Szabo

http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Why bitcoin matters (2014)

by Marc Andreessen

https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Bitcoin's academic pedigree (2017)

by Arvind Narayanan and Jeremy Clark

https://queue.acm.org/detail.cfm?id=3136559

Key Concepts and Beginners' Guides

Beyond the bitcoin bubble

by Steven Johnson

https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html

Crypto tokens: A breakthrough in open network design

by Chris Dixon

https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef

Crypto tokens and the coming age of protocol innovation

by Albert Wenger

http://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol

Fat protocols

by Joel Monegro

https://www.usv.com/blog/fat-protocols

Cryptocurrencies, app coins, and investing in protocols

Olaf Carson-Wee, Chris Dixon, and Sonal Chokshi

https://a16z.com/2017/04/03/cryptocurrencies-protocols-appcoins/

Getting applications into people's hands

Juan Benet and Chris Dixon

https://a16z.com/2017/09/14/networks-protocols-labs-tokens/

How the U.S. government used blockchain to fight fraud

by Kathryn Haun

https://youtu.be/507wn9VcSAE

Bitcoin network effects

by Elad Gil

http://blog.eladgil.com/2017/12/bitcoin-network-effects_11.html

Keepers: workers that maintain blockchain networks — when designed correctly, tokens can act like rocket-fuel for driving network effects by incentivizing desired behaviors

by Ryan Zurrer

https://medium.com/@rzurrer/keepers-workers-that-maintain-blockchain-networks-a40182615b66

The quiet master of cryptocurrency — Nick Szabo in conversation with Naval Ravikant

by Tim Ferris

https://tim.blog/2017/06/04/nick-szabo/

Beginner's guide series on cryptoassets (series) — from ethereum to litecoin

by Linda Xie

https://medium.com/@linda.xie/beginners-guide-series-on-cryptoassets-d897535d887

Why crypto tokens matter

Fred Ehrsam and Chris Dixon

https://a16z.com/2017/09/28/cryptocurrencies-networks-tokens/

Why it's hard to "get" bitcoin: the blockchain spectrum

by Dhruv Bansal

https://blog.unchained-capital.com/blockchain-spectrum-806847e1c575

What do we mean by "blockchains are trustless"?

by Preethi Kasireddy

https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6

The meaning of decentralization — but what does that actually mean? nuances, depth

by Vitalik Buterin

https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

The truth about blockchain — framework for adoption to help big company executives understand state of development; strategic investments; challenges, resources, processes to facilitate adoption

by Marco Iansiti and Karim Lakhani

https://hbr.org/2017/01/the-truth-about-blockchain

The slow death of the firm

by Nick Tomaino

https://thecontrol.co/the-slow-death-of-the-firm-1bd6cc81286b

Vitalik Buterin, creator of Ethereum — Unchained: big ideas from the worlds of blockchain and cryptocurrency
by Laura Shin
https://itunes.apple.com/us/podcast/unchained-big-ideas-from-worlds-blockchain-cryptocurrency/id1123922160

Mental models for understanding tokens
Nick Tomaino and Chris Dixon
https://a16z.com/2018/01/21/mental-models-tokens-crypto-trends/

Governance

The myth of the irrational token holder — why blockchain governance doesn't fit squarely into any existing model
by Kathleen Breitman
https://medium.com/@kathleenbreit/the-myth-of-the-irrational-token-holder-c12438709afd

Blockchain governance — design components, approaches, suggestions
by Fred Ehrsam
https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74

Against on-chain governance — refuting (and rebuking) the above post
by Vlad Zamfir

https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

Notes on blockchain governance

by Vitalik Buterin

http://vitalik.ca/general/2017/12/17/voting.html

A self-amending crypto-ledger — Tezos position paper

by Arthur and Kathleen Breitman

https://www.tezos.com/static/papers/position_paper.pdf

Privacy and Security

Privacy on the blockchain

by Vitalik Buterin

https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Securing smart contracts (series) — 6 Solidity vulnerabilities and how to avoid them from Loom

https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-1-c33048d4d17d

https://medium.com/loom-network/how-to-secure-your-smart-contracts-6-solidity-vulnerabilities-and-how-to-avoid-them-part-2-730db0aa4834

Ethereum smart contract best practices

by ConsenSys Diligence

https://consensys.github.io/smart-contract-best-practices/

Town Crier: an authenticated data feed for smart contracts

by Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi

https://eprint.iacr.org/2016/168.pdf

Devcon3 panel on formal verification

Phil Daian, Everett Hildenbrandt, Yoichi Hirai, and Loi Luu, moderated by Reto Trinkler

https://youtu.be/DrDIcirrhWM

STARKs, part I: proofs with polynomials — general-purpose technology that can be used for all sorts of use cases ranging from verifiable computation to privacy-preserving cryptocurrency

by Vitalik Buterin

https://vitalik.ca/general/2017/11/09/starks_part_1.html

Zk-SNARKs: under the hood — assumes basic knowledge (and requires reading up on quadratic arithmetic programs and elliptic curve pairings, linked within)

https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6

Scalable, transparent, and post-quantum secure computational integrity

by Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev

https://eprint.iacr.org/2018/046.pdf

Succinct non-interactive zero knowledge for a von Neumann Architecture — zK-SNARKs proofs

by Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza

https://eprint.iacr.org/2013/879.pdf

Scaling

Blockchains don't scale — not today, at least… but there's hope
by Preethi Kasireddy
https://hackernoon.com/blockchains-dont-scale-not-today-at-least-but-there-s-hope-2cb43946551a

Platform currencies may soon be obsolete — here is my claim: within 5 years the biggest cryptocurrency by market cap will be an application token
by Aleksandr Bulkin
https://blog.coinfund.io/platform-currencies-may-soon-be-obsolete-78d9b263d902

The importance of layer two — an HTTP of bitcoin and blockchains
by Elizabeth Stark
https://youtu.be/3PcR4HWJnkY

What is the Lightning Network and how can it help bitcoin scale?
by Elizabeth Stark
https://coincenter.org/entry/what-is-the-lightning-network

Scaling Tezos — scaling with recursive SNARKs (succinct non-interactive zero-knowledge proofs of knowledge)
by Arthur Breitman
https://hackernoon.com/scaling-tezo-8de241dd91bd

Ethereum Foundation research initiatives — primary topics in both pure and applied

research

by Ethereum Foundation

http://notes.eth.sg

/CwIwZgbAjADAxgUwLQEMUIKxOCsWCcIEwShAHCgEwJj4qyVA

Ethereum scalability research and development subsidy programs

by Vitalik Buterin

https://blog.ethereum.org/2018/01/02/ethereum-scalability-research-development-subsidy-programs/

A beginner's guide to Ethermint

by Tendermint

https://blog.cosmos.network/a-beginners-guide-to-ethermint-38ee15f8a6f4

Construction of a plasma chain 0x1

by David Knott

https://blog.omisego.network/construction-of-a-plasma-chain-0x1-614f6ebd1612

Accounts, transactions, gas, and block gas limits in Ethereum

by Hudson Jameson

https://hudsonjameson.com/2017-06-27-accounts-transactions-gas-ethereum/

Interplanetary linked computing: separating Merkle Computing from blockchain computational courts

by Simon de la Rouviere

https://media.consensys.net/interplanetary-linked-computing-separating-merkle

computing-from-blockchain-computational-courts-1ade201ecf8a

Ethereum sharding: overview and finality

by Hsiao-Wei Wang

https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649

Consensus

Consensus Compare: Casper vs. Tendermint; Tendermint BFT vs. EOS dPoS

from Tendermint

https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae

https://blog.cosmos.network/consensus-compare-tendermint-bft-vs-eos-dpos-46c5bca7204b

Ethereum Casper 101

by Jon Choi

https://medium.com/@jonchoi/ethereum-casper-101-7a851a4f1eb0

The history of Casper (series)

by Vlad Zamfir

https://medium.com/@Vlad_Zamfir/the-history-of-casper-part-1-59233819c9a9

Decentralization in bitcoin and ethereum

by Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gi

Sirer

http://hackingdistributed.com/2018/01/15/decentralization-bitcoin-ethereum/

Seeking consensus on consensus — DPOS (delegated proof of stake) and the Two Generals' problem

by Ian Grigg

https://steemit.com/eos/@iang/seeking-consensus-on-consensus-dpos-or-delegated-proof-of-stake-and-the-two-generals-problem

A proof of stake design philosophy

by Vitalik Buterin

https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

Inflation and participation in stake based token protocols

by Doug Petkanics

https://medium.com/@petkanics/inflation-and-participation-in-stake-based-token-protocols-1593688612bf

Cryptoeconomics and Investing

A crash course in mechanism design for cryptoeconomic applications — understanding the basic fundamentals of cryptoeconomics

from BlockChannel

https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-

cryptoeconomic-applications-a9f06ab6a976

Cryptoasset valuations — a theory and framework for evaluating
by Chris Burniske
https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7

An (institutional) investor's take on cryptoassets
by John Pfeffer
https://s3.eu-west-2.amazonaws.com/john-pfeffer
/An+Investor%27s+Take+on+Cryptoassets+v6.pdf

Comments on the above (tweetstorm) — network effects?; programmability as feature of money
by Kyle Samani
https://twitter.com/KyleSamani/status/943277077037506560

On value, velocity, and monetary theory — a new approach to cryptoasset valuations
by Alex Evans
https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f

On medium-of-exchange token valuations
by Vitalik Buterin
http://vitalik.ca/general/2017/10/17/moe.html

Understanding token velocity

by Kyle Samani

https://multicoin.capital/2017/12/08/understanding-token-velocity/

A process for evaluating new tokens

by Nick Tomaino

https://thecontrol.co/our-process-for-evaluating-new-tokens-4627ed97f500

Fat protocols are not an investment thesis

by Jake Brukhman

https://blog.coinfund.io/fat-protocols-are-not-an-investment-thesis-17c8837c2734

Skin-in-the-game coins

by Ryan Selkis

https://medium.com/tbis-weekly-bits/skin-in-the-game-coins-da0afdfdc650

Fundraising and Token Distribution

Thoughts on tokens

by Balaji Srinivasan

https://news.earn.com/thoughts-on-tokens-436109aabcbe

Funding the evolution of blockchains

by Fred Ehrsam

https://medium.com/@FEhrsam/funding-the-evolution-of-blockchains-87d160988481

The bitcoin model for crowdfunding

by Naval Ravikant

https://startupboy.com/2014/03/09/the-bitcoin-model-for-crowdfunding/

How to make bonding curves for the economic web — a novel token distribution mechanism for building healthy communities, a technical primer

by Slava Balasanov

https://hackernoon.com/how-to-make-bonding-curves-for-continuous-token-models-3784653f8b17

Separating the staking token from the fee token — introducing the Photon (the Hard Spoon explained)

by Tendermint

https://blog.cosmos.network/cosmos-fee-token-introducing-the-photon-8a62b2f51aa

Explanation of DAICOs

by Vitalik Buterin

https://ethresear.ch/t/explanation-of-daicos/465

The SAFT Project

https://saftproject.com/

Regulatory environment and considerations — updates and explainers from Coin Center

https://coincenter.org/our-work

Decentralized Exchanges

State of decentralized exchanges, 2018

by Nathan Sexer

https://media.consensys.net/state-of-decentralized-exchanges-2018-276dad340c79

Networked liquidity — projects solving the chicken and egg problem

by Radar Relay

https://medium.com/radarrelay/networked-liquidity-2030d85af897

List of decentralized exchanges — of cryptocurrencies and tokens (does not yet include column for degree of decentralization)

https://github.com/PYMERVAL/decentradexchange

Stablecoins

Stablecoins: A holy grail in digital currency

by Nick Tomaino

https://thecontrol.co/stablecoins-a-holy-grail-in-digital-currency-b64f3371e111

An overview of stablecoins

by Myles Snider

https://multicoin.capital/2018/01/17/an-overview-of-stablecoins/

The search for a stable cryptocurrency

by Vitalik Buterin

https://blog.ethereum.org/2014/11/11/search-stable-cryptocurrency/

Maker for dummies: a plain English explanation of the Dai stablecoin

by Gregory DiPrisco

https://medium.com/cryptolinks/maker-for-dummies-a-plain-english-explanation-of-the-dai-stablecoin-e4481d79b90

Cryptoeconomic Primitives: Curation Markets, Cryptocollectibles, Games

Introducing curation markets — trade popularity of memes and information (with code!)

by Simon de la Rouviere

https://medium.com/@simondlr/introducing-curation-markets-trade-popularity-of-memes-information-with-code-70bf6fed9881

Curation markets (tweetstorm) — summary and implications of

by Fred Ehrsam

https://twitter.com/FEhrsam/status/958388803655184386

Early UIs for curation markets (tweetstorm) — categories and some projects using markets to curate human readable information

by Jesse Walden

https://twitter.com/jessewldn/status/958733889643696128

Token-curated registries — a more formal but less-than-mathematical view of token-curated registries

by Mike Goldin

https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7

Building 'Google for the economic web' on the Ethereum blockchain

by Maciej Olpinski

https://blog.userfeeds.io/building-google-for-the-economic-web-on-the-ethereum-blockchain-de27cb3d23b

Smart media tokens

from Steemit

https://smt.steem.io/smt-whitepaper.pdf

Digital pets that don't die

by Elaine Ou

https://elaineou.com/2017/12/03/digital-pets-that-dont-die/

Will cryptocurrencies be the art market's next big thing?

by Scott Reyburn

https://www.nytimes.com/2018/01/13/arts/cryptocurrency-art-market.html

Digital collectibles and the weird future of "digibles"

by Josh Stark

https://hackernoon.com/digital-collectibles-and-the-weird-future-of-digibles-f75f4bf0f9aa

Cryptocollectibles are XLNT, but nobody knows what's next

by Matt Condon

https://medium.com/xlnt-art/cryptocollectibles-are-xlnt-but-nobody-knows-whats-next-a7892b311637

Rare pepe — what happens when you combine a crypto-asset with a meme and a trading card

by Fred Wilson

http://avc.com/2017/05/rare-pepe/

Developer Tutorials and Practical Guides

Learn to code Ethereum dapps by building your own game — designed for beginners to Solidity (even if you've never coded with Solidity before)

https://cryptozombies.io/

How to code your own cryptokitties-style game on Ethereum

by James Martin Duffy

https://medium.com/loom-network/how-to-code-your-own-cryptokitties-style-game-on-ethereum-7c8ac86a4eb3

Learning Solidity — commit-reveal voting

by Karl Floersch

https://karl.tech/learning-solidity-part-2-voting/

The hitchhiker's guide to smart contracts in Ethereum

by Manuel Araoz
https://blog.zeppelin.solutions/the-hitchhikers-guide-to-smart-contracts-in-ethereum-848f08001f05

Introduction to zk-SNARKs with examples — an overview of zk-SNARKs from a practical viewpoint
Christian Lundkvist
https://media.consensys.net/introduction-to-zksnarks-with-examples-3283b554fc3b

zkSNARKs: driver's ed — practical beginner's guide to creating, proving, verifying in contracts
by Joseph Stockermans
https://github.com/jstoxrocky/zksnarks_example

Epicenter — a trove of interviews with many different blockchain project leads
https://epicenter.tv/episodes/

Other Resources – Newsletters

Week in Ethereum News — tracking developments in the Ethereum ecosystem
by Evan Van Ness
http://www.weekinethereum.com/

The Control — on the entrepreneurs, projects and protocols that are putting control of power in the hands of the people
by 1confirmation

https://www.getrevue.co/profile/control

Token Economy — tracking new developments in distributed ledger tech

by Stefano Bernardi and Yannick Roux

https://tokeneconomy.co/

Proof of Work — projects and progress in crypto, also a view from China

by Eric Meltzer

https://tinyletter.com/proofofwork/archive

Other Resources – Courses

Cryptocurrency (2018)

by Susan Athey and Kathryn Haun

http://explorecourses.stanford.edu/search?view=catalog&filter-coursestatus-Active=on&q=MGTECON%20515:%20Cryptocurrency&academicYear=20172018

Bitcoin and Cryptocurrency Technologies (2015)

by Arvind Narayan, Joseph Bonneau, Edward Felten, Andrew Miller

https://piazza.com/princeton/spring2015/btctech/home

Advanced topics in computer science: Bitcoin and cryptocurrency technologies (2014)

by Arvind Narayan

http://randomwalker.info/teaching/fall-2014-bitcoin/

A graduate course in applied cryptography (2017)

by Dan Boneh and Victor Shoup

http://toc.cryptobook.us/

RELATED STORIES

a16z Field Notes: Devcon3 – Ethereum Developer's Conference

By Michael Wee

a16z Podcast: Ethereum, App Coins, and Beyond

By Vitalik Buterin, Fred Ehrsam and Chris Dixon

Why I'm Interested in Bitcoin

By Chris Dixon

blockchain & cryptocurrencies · coding literacy · online communities · open source · listicles · what we're reading

February 10, 2018