Course Subjects List: A supplement

			Background or supplementary	
Cluster	Sub-Cluster	Work-in-progress Course Subject List	Readings	Online courses or Videos/Podcasts
Tools -> Economics	Economic Primitives –	Auction, Voting, Derivatives	[A], [B]	[1]
	Staking –	Slashing conditions	[C]	
	Token models –	kickstarter, access tokens, dividends	[D]	
Tools -> Cryptography	Cryptographic Primitives –	Hash functions & blockchains, signatures (public/private)	[E]	[2]
	Accumulators –	Merkle trees, sparse merkle trees, RSA accumulators	[F]	[3] , [3A]
	Additional Crypto –	Onion hashing, commit reveal		
	Fault Proofs			
Analysis	Synchrony assumptions –	synchronous, partially synchronous, asynchronous		
	Security models / honest assumptions –	honest majority, rational majority, bribing attacker, uncoordinated, coordinated choice	[G], [H],	[4], [5]
	Griefing Analysis		[H]	
	Block withholding		[I]	
	Formal verification		[J], [C1]	
Design Patterns -> Consensus	Proof-of-work		[K]	[3A]
	Proof-of-authority		[L]	
	Proof-of-stake		[M]	

Design Patterns -> Layer 2 Scaling	State Channels		[N]	[6]
	Plasma		[O]	[7]
General				
	Verification & Validation			
	The Future –	Prediction markets, DAOs, Voting	[P]	[8]
Additional Topics				
Tools -> Economic	Cryptoeconomic Primitives			
	Curation Markets	Token Curated Registries (TCRs) & Curve Bonding	[Q]	
	Mechanism Design		[R]	
	Economics (non-blockchain)	Adverse selection, moral hazard		
	Schelling Points		[S]	
	Token Valuation	Velocity sinks, burning, Supply of Money Eq (MV = PQ)?	[T]	
	Game Theory		[U]	
	Emergent Theory			
Tools -> Cryptography	homomorphic encryption		[V]	
	Zero knowledge		[W]	
	Threshold signatures (BLS vs ECDSA sig)			
	Organizing Principles			
	Random Beacons			
Analysis	Attacks	Selfish mining		
		Verifier's dilemma	[Z]	
		Fee-stealing attacks		
	Game Theory		[U]	
	Spore Framework			[X]

Design Patterns -> Consensus	Proof-of-Space			
	Proof-of-Custody			
	Proof-of-Work	Miner Games (i.e., selfish mining, fee sniping)		
Design Patterns -> Protocol Layer	Charging rent for blockchain resources			
Design Patterns -> Application Layer	Domain name registry pricing			
Design Patterns -> Layer 1	Sharding		[X]	
Design Patterns -> Layer 2	Truebit			
	HTLCs			
	Cross-chain atomic swaps			
General or (misc)	Mechanism Design in Dapps			
	Seignorage Shares			
	Analysis of Dpos protocols		[Y]	
	Filecoin / Storj			
	Distributed Systems	Byzantine Fault Tolerance vs Crash Fault	[AA]	
	Cost of Running Programs on a laptop			

References: Readings

[A] Klemperer, P. (2002). What really matters in auction design. *Journal of economic perspectives*, *16*(1), 169-189.

[B] Caplan, B. (2011). *The myth of the rational voter: Why democracies choose bad policies*. Princeton University Press.

Lewis-Beck, M. S., & Stegmaier, M. (2007). Economic models of voting. In *The Oxford handbook of political behavior*.

[C] Buterin, V. (Mar 2, 2017) Minimal Slashing Condition https://medium.com/@VitalikButerin/minimal-slashing-conditions-20f0b500fc6c

[C1] Hirai, Y. (Feb 26, 2017) Formal methods on some PoS Stuff https://medium.com/@pirapira/formal-methods-on-some-pos-stuff-e309775c2ab8

[D] Siegel, D. (Sep 13, 2017) The Token Handbook https://hackernoon.com/the-token-handbook-a80244a6aacb

Gnosis (Jan 31, 2017) What are Gnosis Tokens? – the New Access Based Token Model https://blog.gnosis.pm/what-are-gnosis-tokens-the-new-access-based-token-model-e59c5a490af6

Milev, A. (Apr 17, 2018) Dividend Tokens, Explained https://cointelegraph.com/explained/dividend-tokens-explained

[E] Boneh, D. & Shoup, V (Sep 2017) A Graduate Course in Applied Cryptography (Version 0.4)

[F] Clifton, M. (Mar 13, 2017) Understanding Merkle Trees – Why use them, who uses them, and how to use them https://www.codeproject.com/Articles/1176140/Understanding-Merkle-Trees-Why-use-them-who-uses-t

[G] Lopp, J, (Nov 13, 2016) Bitcoin's Security Model: A Deep Dive https://www.coindesk.com/bitcoins-security-model-deep-dive/

[H] Buterin, V. (Jul 16, 2017) The Triangle of Harm https://vitalik.ca/general/2017/07/16/triangle_of_harm.html

Buterin, V. (Jul 27, 2016) On inflation, transaction fees and cryptocurrency monetary policy https://blog.ethereum.org/2016/07/27/inflation-transaction-fees-cryptocurrency-monetary-policy/

Buterin, V. (Jan 28, 2015) The P + epsilon Attack (bribing) https://blog.ethereum.org/2015/01/28/p-epsilon-attack/

Buterin, V. (May 8, 2017) Engineering Security Through Coordination Problems https://vitalik.ca/general/2017/05/08/coordination_problems.html

[I] Buterin, V. (11.04.03) Selfish Mining: A 25% Attack Against the Bitcoin Network https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/

[J] Mueller, B. (Jan 29, 2018) How Formal Verification Can Ensure Flawless Smart Contracts https://media.consensys.net/how-formal-verification-can-ensure-flawless-smart-contracts-cbda8ad99bd1

[K] Eyal, I (July 2017) Proof of Work and Blockchains. The Initiative for Cryptocurrencies and Contracts (IC3), Distribute Cryptocurrencies and Consensus Ledger Conference(?)

Krawisz, D. (Jun 24, 2013) The Proof-of-Work Concept http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/

Greenfield, R. (Aug, 24, 2017) Vulnerability: Proof of Work vs. Proof of Stake https://medium.com/@robertgreenfieldiv/vulnerability-proof-of-work-vs-proof-of-stake-f0c44807d18c

[L] POA Network (Nov 12, 2017) Proof of Authority: Consensus model with Identity at Stake https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[M] Buterin, V. (Dec 31, 2016) A Proof-of-Stake Design Philosophy https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[N] Stark, J. (Feb 12, 2018) Making sense of Ethereum's Layer 2 Scaling Solutions: State channels, Plasma and Truebit https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

[O] Akentiev, A (Aug 10, 2017) Plasma in 10 minutes https://medium.com/chain-cloud-company-blog/plasma-in-10-minutes-c856da94e339

Poon, J. & Buterin, V. (White paper) https://plasma.io/

[P] Buterin, V (May 6, 2014) DAOs, DACs, DAs and More: An Incomplete Terminology Guide https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Bradbury, D (Jun 16, 2014) How blockchain technology could usher in Digital Democracy https://www.coindesk.com/block-chain-technology-digital-democracy/

[Q] Token Curated Registry (Feb 22, 2018) The Token Curated Registry Reading List https://medium.com/@tokencuratedregistry/the-token-curated-registry-whitepaper-bd2fb29299d6

De la Rouviere, S (Apr 2, 2018) Curation Markets & Curved Bonding Update: 02 April 2018 https://medium.com/@simondlr/curation-markets-curved-bonding-update-02-april-2018-87c593d629c2

[R] Blockchannel (Oct 17, 2017) A Crash Course in Mechanism Design for Cryptoeconomic Applications https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

[S] (Brief intro Schelling Points) http://wisdomofcrowds.blogspot.com.es/2010/02/chapter-five-part-iii.html

[T] Weber, W (Feb 27, 2018) The Quantity Theory of Money for Tokens https://blog.coinfund.io/the-quantity-theory-of-money-for-tokens-dbfbc5472423

Burniske, C (Sep 24, 2017) Cryptoasset Valuations https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7

[U] Rosic, A (2017) What is Cryptocurrency Game Theory: A Basic introduction https://blockgeeks.com/guides/cryptocurrency-game-theory/

[V] Green, M. (Jan 2, 2012) A very casual introduction to Fully Homomorphic Encryption https://blog.cryptographyengineering.com/2012/01/02/very-casual-introduction-to-fully/

[W] Green, M. (Nov 27, 2014) Zero Knowledge Proofs: An Illustrated primer https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/

[X] Jordan, R. (Jan 11, 2018) How to scale Ethereum: Sharding Explained https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce

Rosic, A (2017) What are Ethereum Nodes and Sharding? https://blockgeeks.com/guides/what-are-ethereum-nodes-and-sharding/

[Y] Tendermint Team (Sep 29, 2017) Consensus compare: Tendermint BFT vs EOS dPoS https://blog.cosmos.network/consensus-compare-tendermint-bft-vs-eos-dpos-46c5bca7204b

[Z] Luu, L., Teutsch, J., Kulkarni, R., & Saxena, P. (2015, October). Demystifying incentives in the consensus computer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 706-719). ACM.

[AA] Konstantopoulos (Dec 1, 2017) Understanding blockchain fundamentals, Part 1: Byzantine Fault Tolerance https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

References: Video / Online Courses

[1] Jackson, M.O., Leyton-Brown, K., & Shoham, Y. - Game Theory 1 (Coursera)

Jackson, M.O., Leyton-Brown, K., & Shoham, Y. - Game Theory 2: Advanced Applications (Coursera)

[2] Boneh, D. – Cryptogrpahy 1 (Coursera)

Boneh, D. – Cryptogrpahy 2 (forthing coming, Coursera)

Chang, S-Y., White, R., & Bahn W. – Introduction to Applied Cryptography Specialization (Coursera)

Chang, S-Y. – Applied Cryptography Specialization (Coursera)

[3] Chang, S-Y. – Cryptographic Hash and Integrity Protection (Coursera)

[3A] Narayanan, A. – Bitcoin and Cryptocurrency Technologies (Coursera)

[4] Blockchain at Berkeley – Lecture Series (Game Theory & Network Attacks: How to Destroy Bitcoin)

[5] Blockchain & Cryptography Courses (edX)

[6] L4 | Generalized State Channels https://www.youtube.com/watch?v=kZH_ty82jKY

[7] Ethereum Plasma MVP Overview https://www.youtube.com/watch?v=jTc_2tyT_lY

[8] Epicenter Videocast (EB98) Robin Hanson: Futarchy, Prediction Markets and the Challenge of Disruptive Technology https://www.youtube.com/watch?v=mUUk0jSndoc

[9] Spore Framework (Georgios Piliouras & Vlad Zamfir) https://youtu.be/OOJVpL9Nsx8?t=45m15s