Keywords summary of recommended materials

1. Survey on Blockchain Networking: Context, State-of-the-Art, Challenges (Maya Dotan, Yvonne-Anne Pignolet, Stefan Schmid, Saar Tochner, and Aviv Zohar)
   State-of-the-art and call-to-arms to identify the unique requirements of blockchain networks and address the open issues; blockchain definition; main application of cryptocurrency; fully distributed manner, cutting out any middle man or trusted third party; disruptive innovation to many other sectors that traditionally rely on trusted third parties; tolerates Byzantine behaviour; run on top of P2P network; node bootstraps its operation with discovery protocol; two roles in in most cryptocurrencies - peer or miner; transaction and blocks are propagated using a flooding or gossip protocol; Bitcoin uses TCP and 3 way handshake informing of height and version; Ethereum defines TCP based DEVp2p protocol to support encryption and authentication; off-chain as additional payment protocol; difference with communication network cause importance of performance, security and incentives; depend on the network; cryptocurrency is recent and not well explored concept; incentive system to verify blocks and motivate to propagate information; miners get the fee; communication pattern; flooding based strategy in Bitcoin; difficult to design efficient route discovery process; Bitcoin and Ethereum rely on flat random graph topologies; off-chain capacities represent financial balances need to keep confidential and threats; importance of consensus layer for security; onion routing networks; DDOS gain advantages in mining, voting; store-and-forward propagation model ; performance; novel kinds of bottlenecks; main issue is scalability;
   block propagation;
   transaction propagation;
   topology of p2p network;
   sharding;
   off-chain payment channel;
   measurements;
   networking aspects of blockchain not yet received the attention they deserve;
2. Route Hijacking and DoS in Off-Chain Networks (Saar Tochner, Stefan Schmid, Aviv Zohar)
   Off-chain networks as mitigation of scalability issues in Bitcoin, novel type of DoS attack; attracting routes which exploits the way transaction are routed and executed along the channels of the network in order to attract nodes to route through the attacker; tradeoff for defender; real data collected; lnd, C-lightning, Eclair approach routing differently; small number of colluding nodes can deny service to a large fraction; lower fees; greedy strategy; five new links are enough to draw the majority of traffic; cost of creating these links is very low; suggestion to modify routing policy.
3. Video Bitcoin's Lightning Network: A Closer Look (Aviv Zohar)
   Bitcoin decentralized ledger scalability; transaction cost is slow and expensive; Lightning network as a solution (Off chain payment channels); Route hijacking attack (Stefan Schmid, Saar Tochner); Congestion attack (Ayelet Mizrahi), Flood & Loot attack (Jona Harris); privacy problem, disrupt gossip protocol, get victim to connect only to attacker by publishing only attacker nodes IP’s; filter channel announcements to victim; economic questions).
4. LightPIR: Privacy-Preserving Route Discovery for Payment Channel Networks (Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, and Michelle Yeo)
   Off-chain networks = payment channel networks; without requiring a consensus; privacy-preserving route discovery mechanisms for payment channel networks; LightPIR

approach discover a shortest path to its destination without revealing any information about endpoints of transaction; hub labeling heuristic; minimize storage and bandwidth overhead; more efficient than Lightning compared to a privacy preserved baseline.

5. Node Classification and Geographical Analysis of the Lightning Cryptocurrency Network (Philipp Zabka, Klaus-Tycho Foerster, Stefan Schmid, and Christian Decker)
   Performance improvements or the security of network, Lightning is leading off-chain network; classification of node types; geographical aspects of the Lightning network.
6. Toward Active and Passive Confidentiality Attacks On Cryptocurrency Off-Chain Networks (Utz Nisslmueller, Klaus-Tycho Foerster, Stefan Schmid, and Christian Decker)
   Lightning (Bitcoin) and Raiden (Ethereum) aim to increase scalability of on-chain transactions; exploit of off-chain networks; active and passive adversary; probing attack; timing attack; limitation and remediation.
7. Article tuwien.at New protocol makes Bitcoin transactions more secure and faster than Lightning (Lukas Aumayr)
   Protocol developed at TU Wien makes Bitcoin's transaction faster; Bitcoin's scalability problem; mathematical proof for protocol with formal methods, rule out specific security-critical attacks that were previously possible, and also to prevent long-term money blocking; the communication chain only has to be run through once; new protocol results in a factor of 4 to 33 fewer failed transactions than with the conventional Lightning network; deployment in a near future.

Keywords summary of materials I picked on my own

1. The Bitcoin Lightning Network (Joseph Poon, Thaddeus Dryja)
   Decentralized system whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels); transfer occurs off-blockchain; sighash; contracts which are enforceable via broadcast over the bitcoin blockchain in the event of uncooperative or hostile participants; The Bitcoin Blockchain Scalability Problem; Hashlocked Bidirectional Micropayment Channels; Hashed Timelock Contract (HTLC).
2. Blitz: Secure Multi-Hop Payments Without Two-Phase Commits (Lukas Aumayr, Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei) Paper from the website
   (PCN reduces the load on-chain by allow- ing arbitrarily many off-chain multi-hop payments (MHPs) between any two users connected through a path of payment channels; current MHP protocols are far from satisfactory; one round MHPs vs two round MHPs; Lightning follows 2 phase commit protocol; 2 phase commit brings other attacks, f.e. wormhole, staggered collateral and dependency on specific scripting language functionality (HTLC); Blitz is novel MHP protocol; achieve the best of the two worlds; no malicious intermediary can steal coins; not prone to the wormhole attack; using only digital signa- tures and a timelock functionality; cryptographic details of Blitz; formal proof of security.
3. Bitcoin: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto)
   Peer-to-peer version of electronic cash; without financial institution; digital signatures; solution to the double-spending; network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work; longest chain and outpace attackers; network itself requires minimal structure; messages are broadcast on a best effort basis; nodes can leave and rejoin the network at will; accepting the longest proof-of-work chain as proof of what happened while they were gone.

4. How the blockchain is changing money and business (Don Tapscott)

   Blockchain is next generation of the Internet; financial assets cannot be transferred as a copy; what we have no is centralized that means hackable; social inequality is growing; Bitcoin enabled people to establish trust and do transactions without a third party; blockchain is “trust” protocol; global ledger, using the highest level of cryptography; when a transaction is conducted, it's posted globally, across millions and millions of computers; first miner to find out the truth and to validate the block, is rewarded in digital currency; block is linked to the previous block and the previous block to create a chain of blocks; build smart contracts in Ethereum's blockchain; with a blockchain financial industry, there would be no settlement, because the payment and the settlement is the same activity, it's just a change in the ledger; good for prosperity cause it could be real share economy; biggest flow of funds is remittances; most powerful asset of the digital age is data.
5. Blockchain revolution (Don Tapscott, Alex Tapscott)

Important terms for understanding the main problem:

Ledger, HTLC, Lightning, 2nd layer protocol, sharding, P2P network (repeat), discovery protocol, peer, miner, SPV (simplified payment verification) wallet, lnd, C-lightning, Eclair, Payment-channel networks (PCN), One-round MHPs (e.g., Interledger), two-round MHPs (e.g., Lightning Network (LN), staggered collateral (i.e., funds are locked for a time proportional to the payment path length).