## 15 Oct 2018

1. [Mike L] Remaining tests for ZKSnarks
2. [Mike L] Range proofs for anonymous payments
   1. Proof of solvency
3. [Mike L] Secure payment key management
   1. HD keys
   2. Syncing keys
4. [Mike L] Distributed point functions (DPF)
   1. <http://www.scs.stanford.edu/~dm/home/papers/corrigan-gibbs:riposte.pdf>

## 8 Oct 2018

1. Bank Notes
   1. Need Anonymous and Private Payments
2. [Dmitry K] - Mirror curves
   1. Commitments point multiplications
   2. Proofs of Signatures can be inefficient with bullet proofs
   3. Use another curve that *mirrors* where you can make efficient elliptic curve circuits vs arithmetic circuits
   4. <https://github.com/BlockchainCommons/secp256k1/issues/1>
   5. <https://mobile.twitter.com/pwuille/status/993572063389605889>
   6. <https://mathoverflow.net/questions/249982/elliptic-curve-related-equivalence-between-fields-of-different-characteristic>
3. Range Proofs in ECC
   1. Use BBS+ for all proofs but ranges
   2. Use RSA for ranges (commitments to values)
   3. Include RSA parameters in cred defs
4. <https://github.com/tjfoc/gmsm>

## 1 Oct 2018

1. [Mike L] - Bellman Curve
   1. Can we swap curve params? Yes
   2. Just need to adjust hash functions that map to points
   3. Adjust generators too
   4. Circuits could be longer
   5. Libsnark is faster and more predictable
      1. Time to generate proof
      2. SHA256 is very close to MIMC
2. [Mike L] - Heard back from GMP, low probability for license change
3. [Mike L] - Verifiable Credentials Working Group proposal
   1. Known Weaknesses
      1. Linkability
      2. No Selective Disclosure
4. [Mike L] - Mirror Symmetry for Elliptic Curves

## 24 Sept 2018

1. [Mike L] Bank notes
2. [Mike L] Zcash snark library
   1. Using libsnark, benmarked MiMC
      1. MiMC is 7 times faster than SHA-256 but not >20 times as expected.
   2. Potential [benchmarks](https://docs.google.com/document/d/1uCi1_Z-dYOt7ZV21XyqfD_RThbCXxvYlo21m_oEIeE8/edit?usp=sharing).
3. [Mike L] Set membership proofs
   1. Snarks merkle trees
   2. Accumulators
   3. Public - Managed by the ledger more generic
   4. Private - Managed by entities (revocation registries)
   5. Multiple parties involved
4. [Mike L] Range proofs Elliptic curve options
5. [Brent Z] Elixxir
   1. Secure Communications
   2. Anonymous payments
   3. Consensus every node is doing Secure MPC
   4. Claiming 10K/sec
6. [Mike L] Verifiable Random Functions (VRFs)
   1. The state root hash could do this, but not recommended
7. BigNumber libraries
   1. Extract OpenSSL BigNum to be a standalone

## 17 Sept 2018

1. [Mike L] Proposal to move all indy-sdk crypto code to crypto lib
   1. Ethereum adopting crypto-lib
   2. [TODO]: Read crypto-lib [proposal](https://docs.google.com/document/d/1JtFT5L-82egj6shgGXzTsNAg6_UHuMheKfsst6NS_Xo/edit?usp=sharing)
2. [Lovesh] Merge Z-mix and crypto-lib
3. [Mike L] Snarks update from Lovesh
4. Banknotes
   1. Brent to do a write up for Mike L and Nathan G to review
5. Agent Authorization Policy
   1. Hart and Dave will review
6. [Lovesh] Sovrin smart contract on EVM (it can be used with Ethereum, RSK, etc)
   1. Credential issuance and verification using Indy
   2. Ethereum would house the keys
   3. DAPP that can access Sovrin
   4. Sovrin Protocol can be used on any blockchain
   5. More info to come next week
7. Mike L to petition GMP authors to have third license: Apache 2.0
   1. We can offer them a logo, always display GMP
   2. Mass adoption with license change
8. Sawtooth is adjusting some items in their code base that Indy could utilize.
   1. Could they eventually merge into one project?
   2. Mike L to ask Nathan George
   3. CC Dave Huseby, Brent, Lovesh
9. Regional based crypto
   1. Chinese