Philipp Lehwalder | September 14, 2020 Calculator (Party 1) Contract Verifier (Party 2) registerDispute() with collateral registerDispute() with collateral root_{calculator}, leaf₀, sig_{root} = sign(root), sig_{leaf} = sign(leaf₀) Initialization Check Signatures initDispute(root_{verifier}, root_{calculator}, leaf₀, sig_{root}, sig_{leaf}) Set root hash getIndexToSubmit() getIndexToSubmit() **Bisection Search** indexToSubmit indexToSubmit submitHash(nodeindexToSubmit) submitHash(node_{indexToSubmit}) emit FoundDeviatingLeafIndex(index) getIndexToSubmit() indexToSubmit = index - 1 getIndexToSubmit() indexToSubmit indexToSubmit Determine Guiltier getMerkleProofIndexes() $merkleProof = [node_0, ..., node_N]$ $reveal Preimage (preimage_{indexToSubmit}, \ merkle Proof)$ check merkleProof correctLeaf = makeStep(preimage) Any of the two parties need to check which party submitted the correct reveal the leaf (if any) preimage emit DetermindedGuiltier(partyIndex)