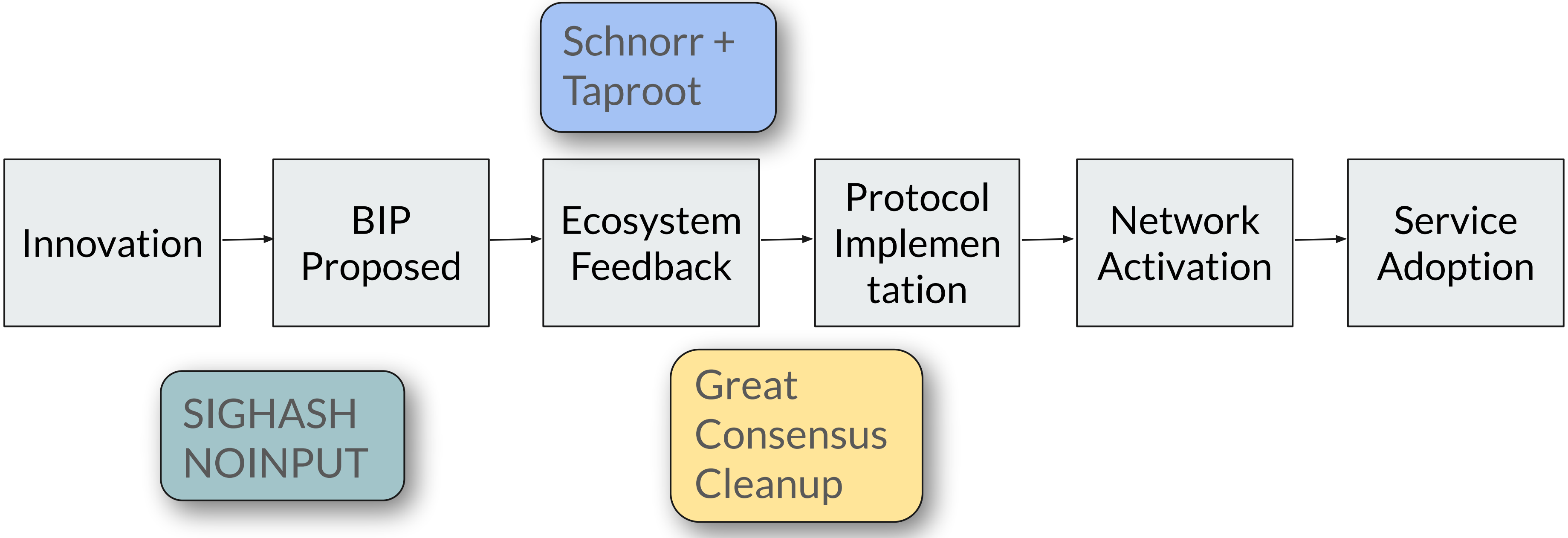
Optech Executive Briefing
The Next Softfork

"In our view, the benefits associated with this softfork are not likely to be controversial. This softfork appears to be a win-win-win for capability, scalability and privacy." - BitMEX Research

Steve Lee - Bitcoin Optech

May 14, 2019

Bitcoin Consensus Upgrade Lifecycle



Schnorr + Taproot

Innovation → BIP Proposed → Ecosystem Feedback → Protocol Implementation → Network Activation → Service Adoption

SIGHASH NOINPUT

Great Consensus Cleanup

Schnorr + Taproot

Motivation

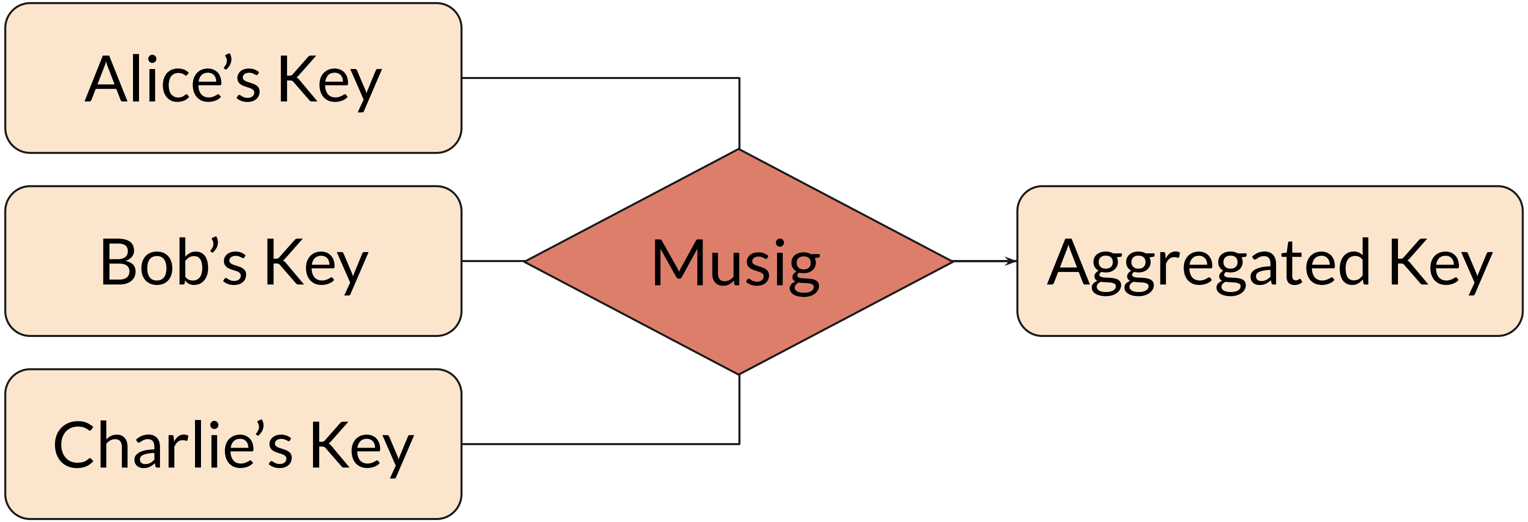
1	Scaling	● 30-75% savings on multisig ● 2.5x faster block validation
2	Fungibility	● All outputs and most spends indistinguishable
3	Script Innovation	● Very large k of n multisig ● Larger scripts, many scripts

Schnorr signatures

1. Better in every way than ECDSA
2. 11% smaller than existing signatures
3. Compatible with existing private keys
4. Same security assumption...with a theoretical proof

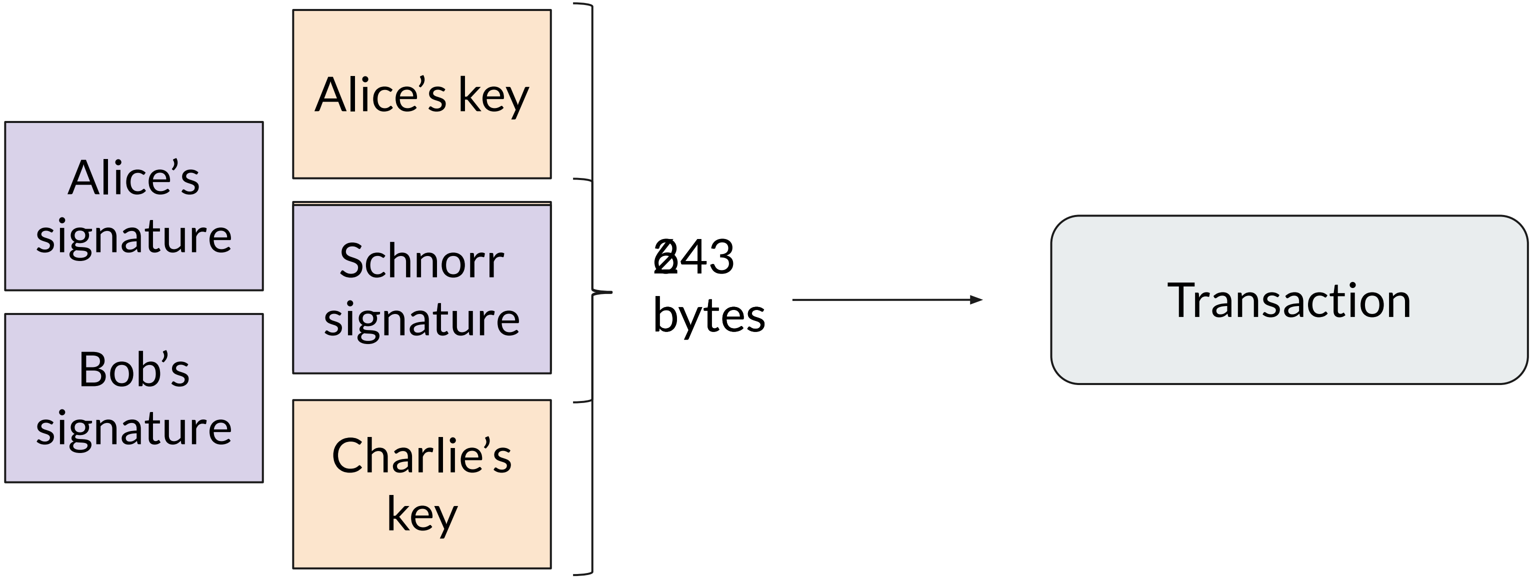
Schnorr + Taproot

Schnorr enables key aggregation



Schnorr + Taproot

Impact on a 2-of-3 multisig transaction



Alice's signature

Bob's signature

Alice's key

Schnorr signature

Charlie's key

243 bytes

Transaction

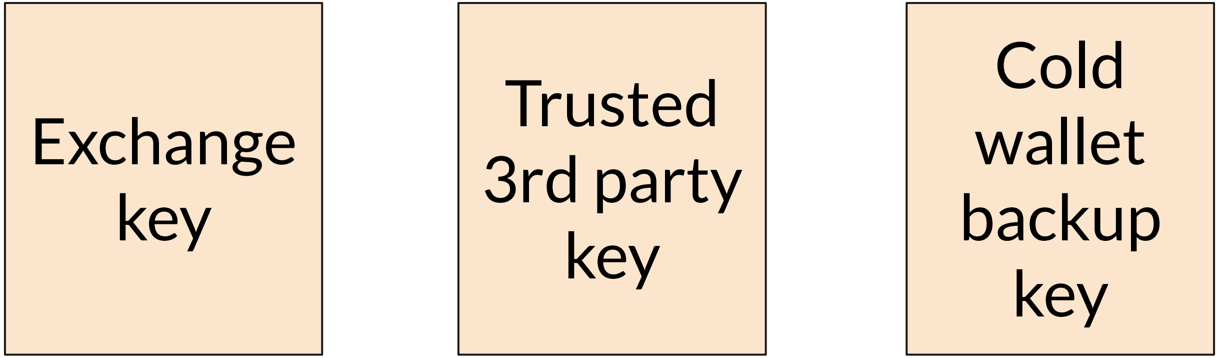
Schnorr + Taproot

Taproot

1. Pay-to-Taproot, or P2TR
2. New segwit v1 script
3. Used for any type of spend

Schnorr + Taproot

Exchange 2-of-3 hot wallet example



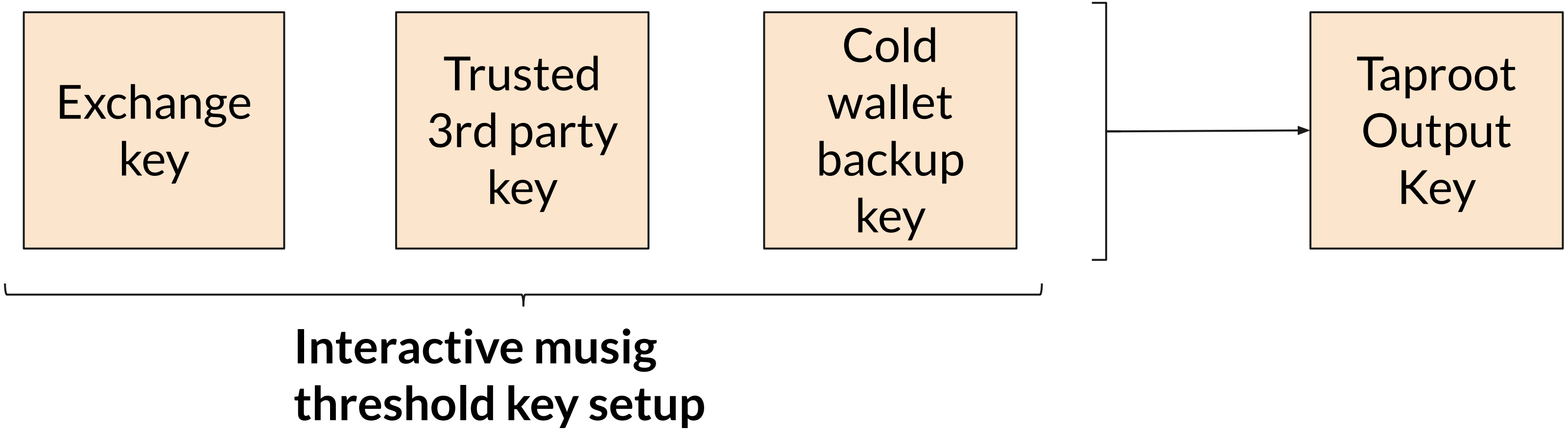
Exchange key

Trusted 3rd party key

Cold wallet backup key

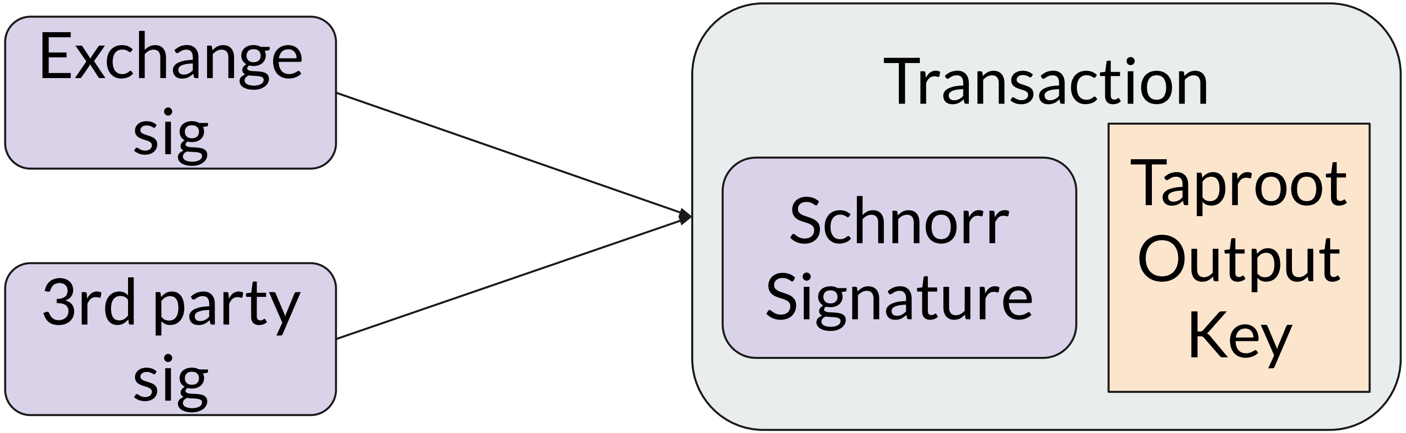
Schnorr + Taproot

Exchange 2-of-3 using threshold signatures



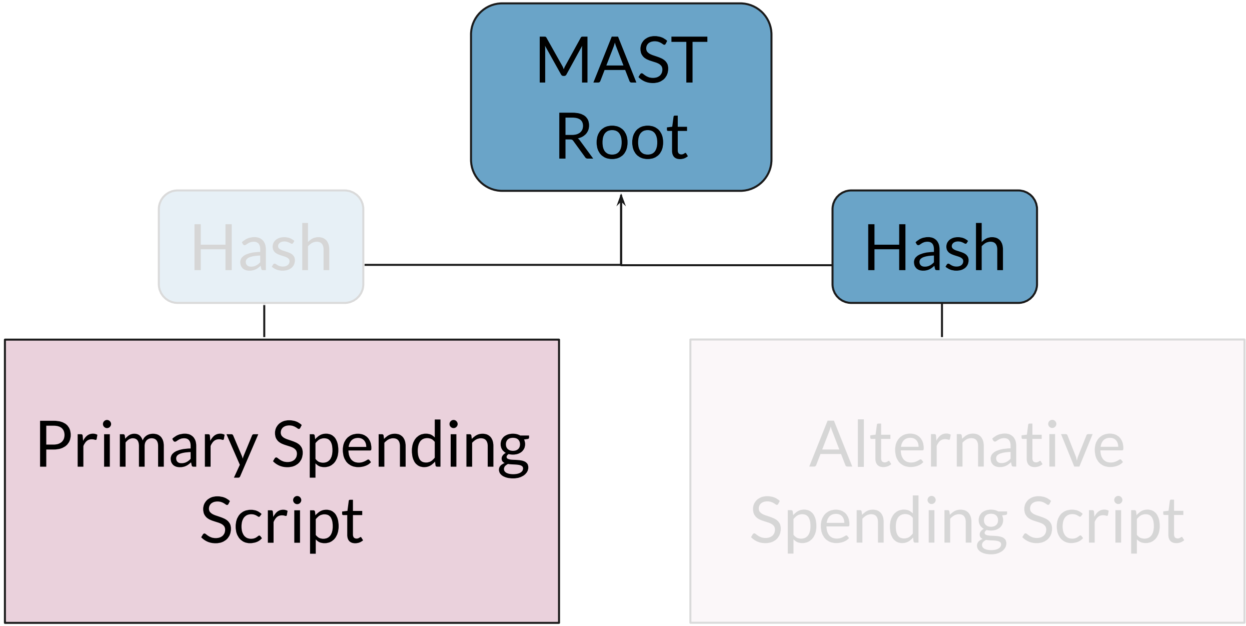
Schnorr + Taproot

Spending using Musig thresholds



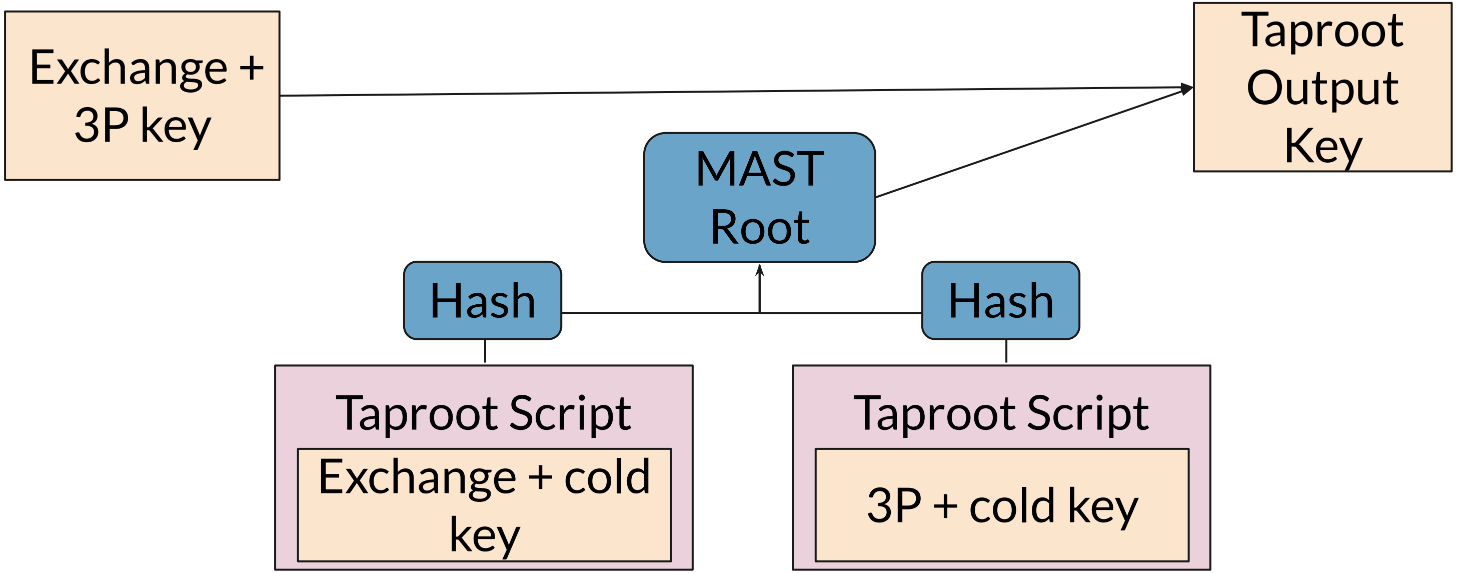
Schnorr + Taproot

MAST Concept



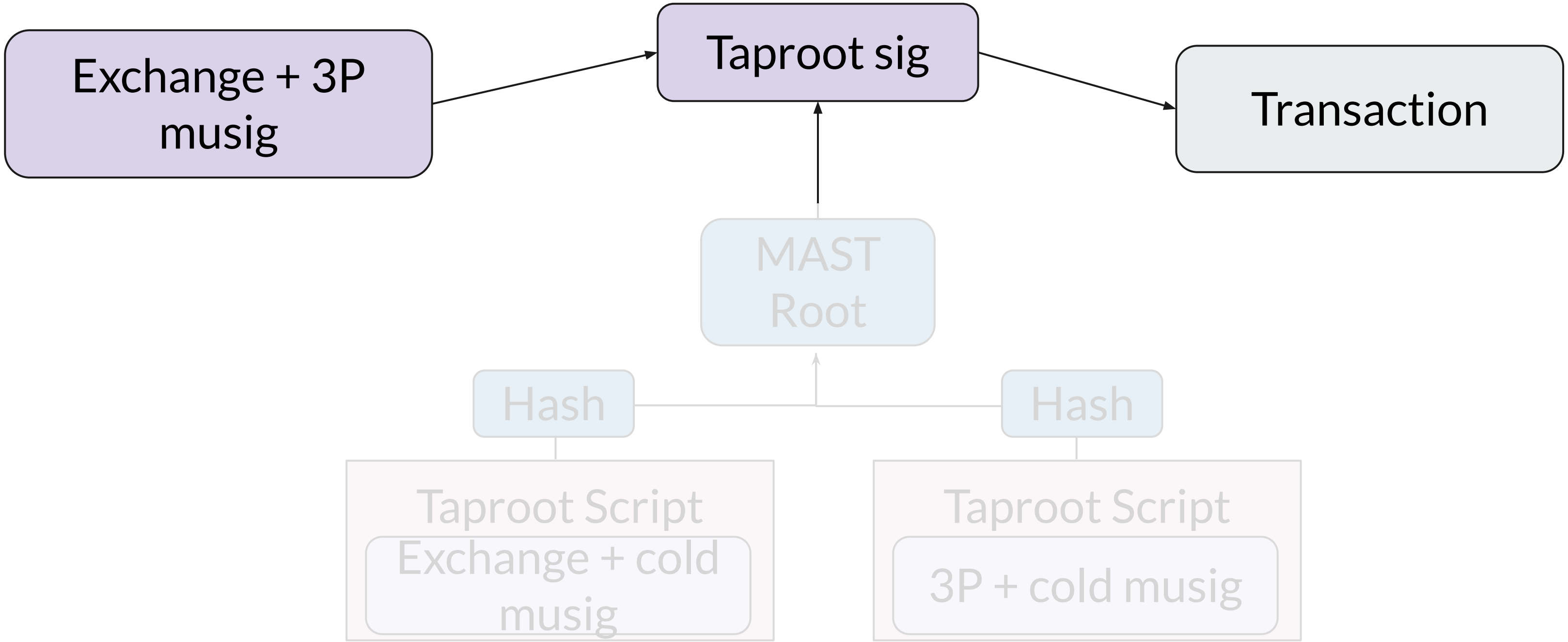
Schnorr + Taproot

Exchange 2-of-3 using Musig keytrees



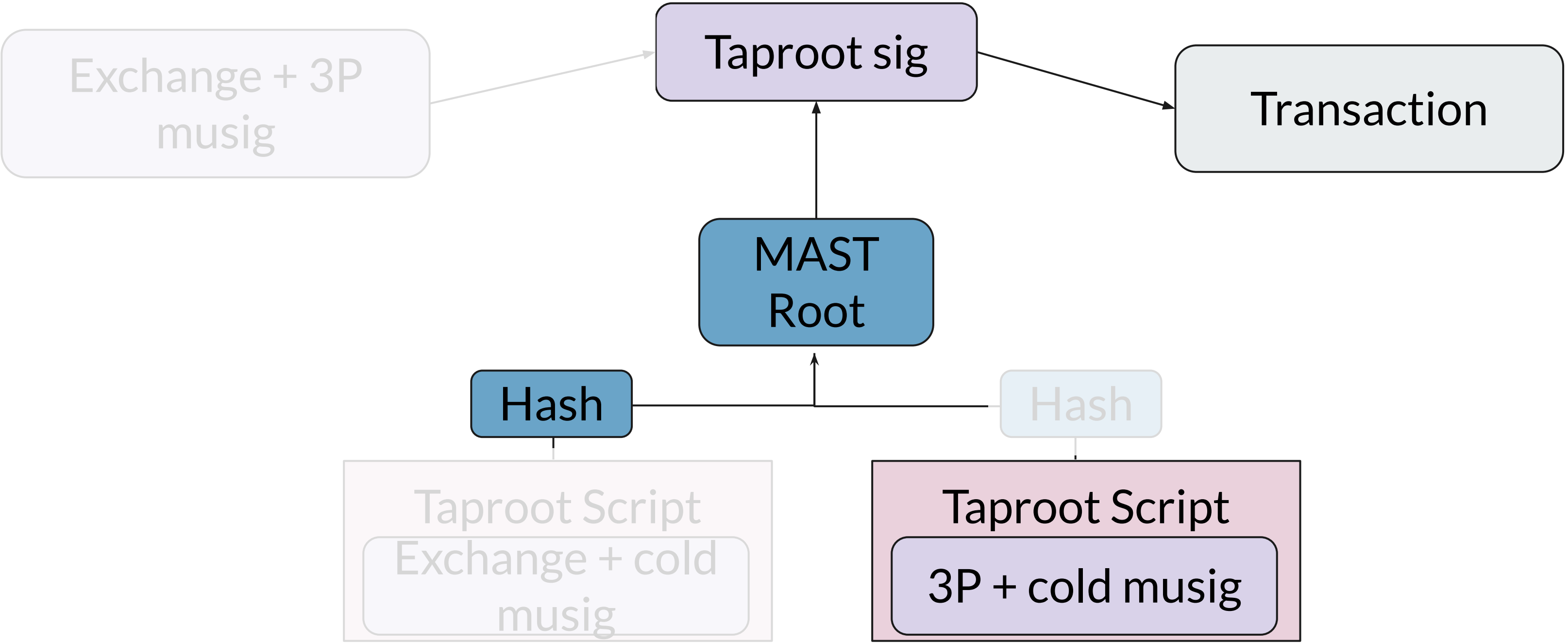
Schnorr + Taproot

Key path spending using Musig keytrees



Schnorr + Taproot

Script path spending using Musig keytrees



Schnorr + Taproot

Summary of multisig constructs

Construct	Fungiblity / Fees	Interactive key setup	Interactive signing	Account ability
Musig k-of-n threshold sigs	Great	Yes	Yes	No
Musig k-of-n keytree	Good	No	Yes	Internal
Musig n-of-n	Great	No	Yes	Internal
Traditional	Poor	No	No	Public

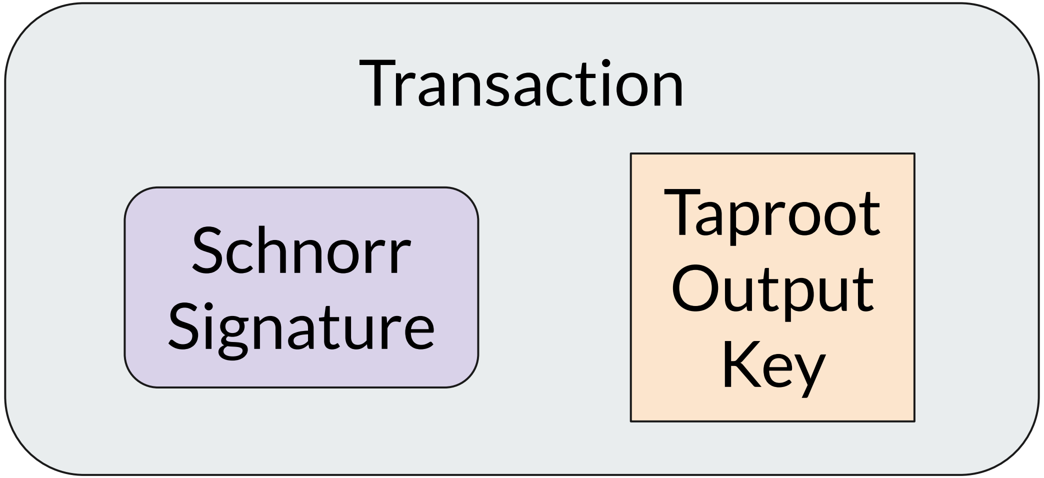
Schnorr + Taproot

Much more innovation ahead...

1. Alternatives to Musig
2. Very large k-of-n
3. Near limitless # of scripts, large script size
4. Adaptor signatures

Schnorr + Taproot

What type of transaction is this?



Motivation - improving layer 2 protocols

1 Improves UX

- No penalty for accidental broadcast of older states

2 More scalable

- Enables multiparty and channel factories
- Lighter, more economical LN nodes

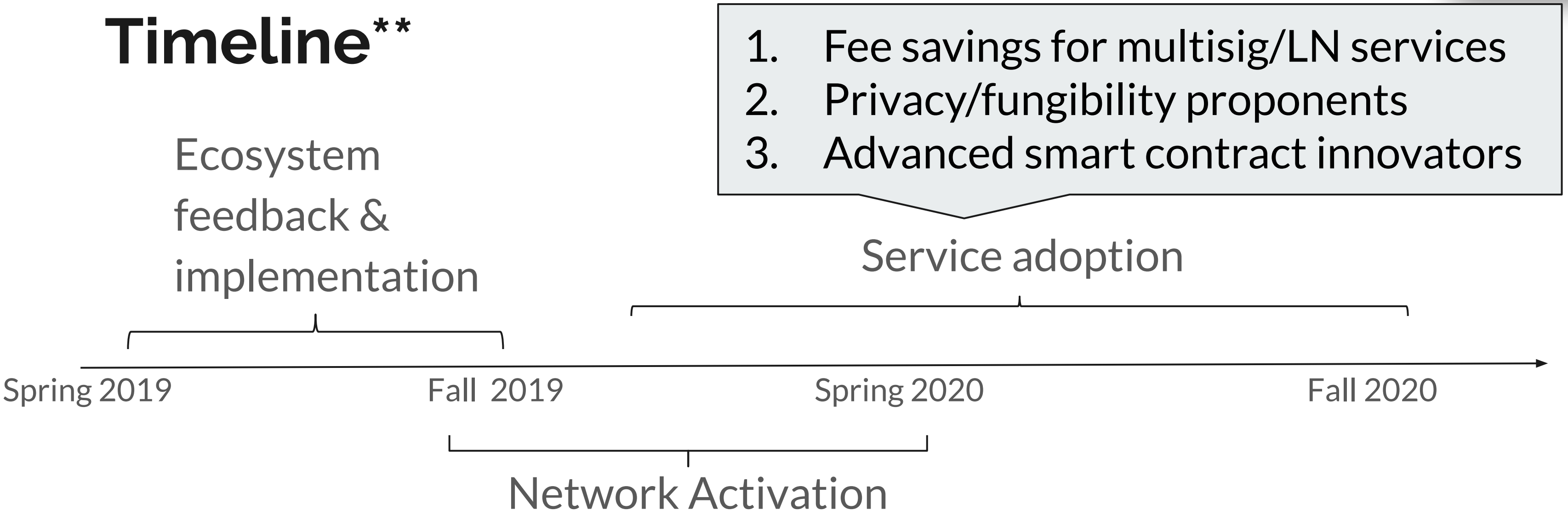
Great Consensus Cleanup

Motivation - harden Bitcoin

1	Reduce worst-case validation time	● Invalidate non-segwit CODESEP opcode ● Invalidate FindAndDelete
2	"Timewarp" inflation	● Restrict nTime fields on difficulty adj blocks
3	Malleation in the merkle tree construction	● Forbid transactions 64 bytes or smaller

Schnorr + Taproot

Timeline**



1. Fee savings for multisig/LN services
2. Privacy/fungibility proponents
3. Advanced smart contract innovators

Ecosystem feedback & implementation

Service adoption

Spring 2019

Fall 2019

Spring 2020

Fall 2020

Network Activation

** This is for illustrative purposes. Timing is a function of ecosystem feedback and the deployment process.

Next Steps

1. Utilize Optech (Slack, workshops, newsletter)

2. Engage and provide feedback

3. Experiment and implement

Questions?

http://bitcoinops.org