The Evolution of Blockchain: from Lit to Dark

Agostino Capponi

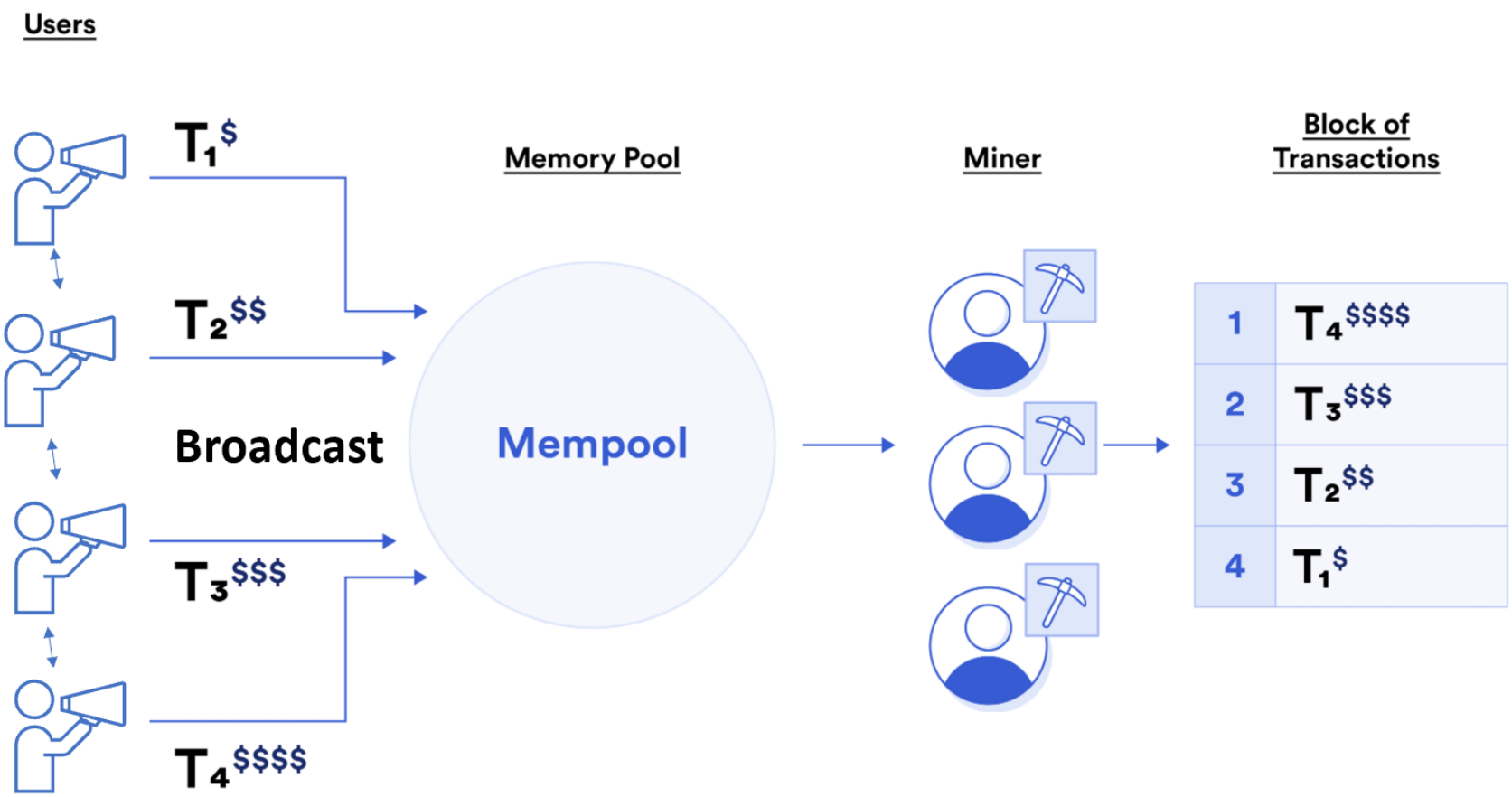
Columbia University

CUHK Distinguished Lectures in Quantitative Finance

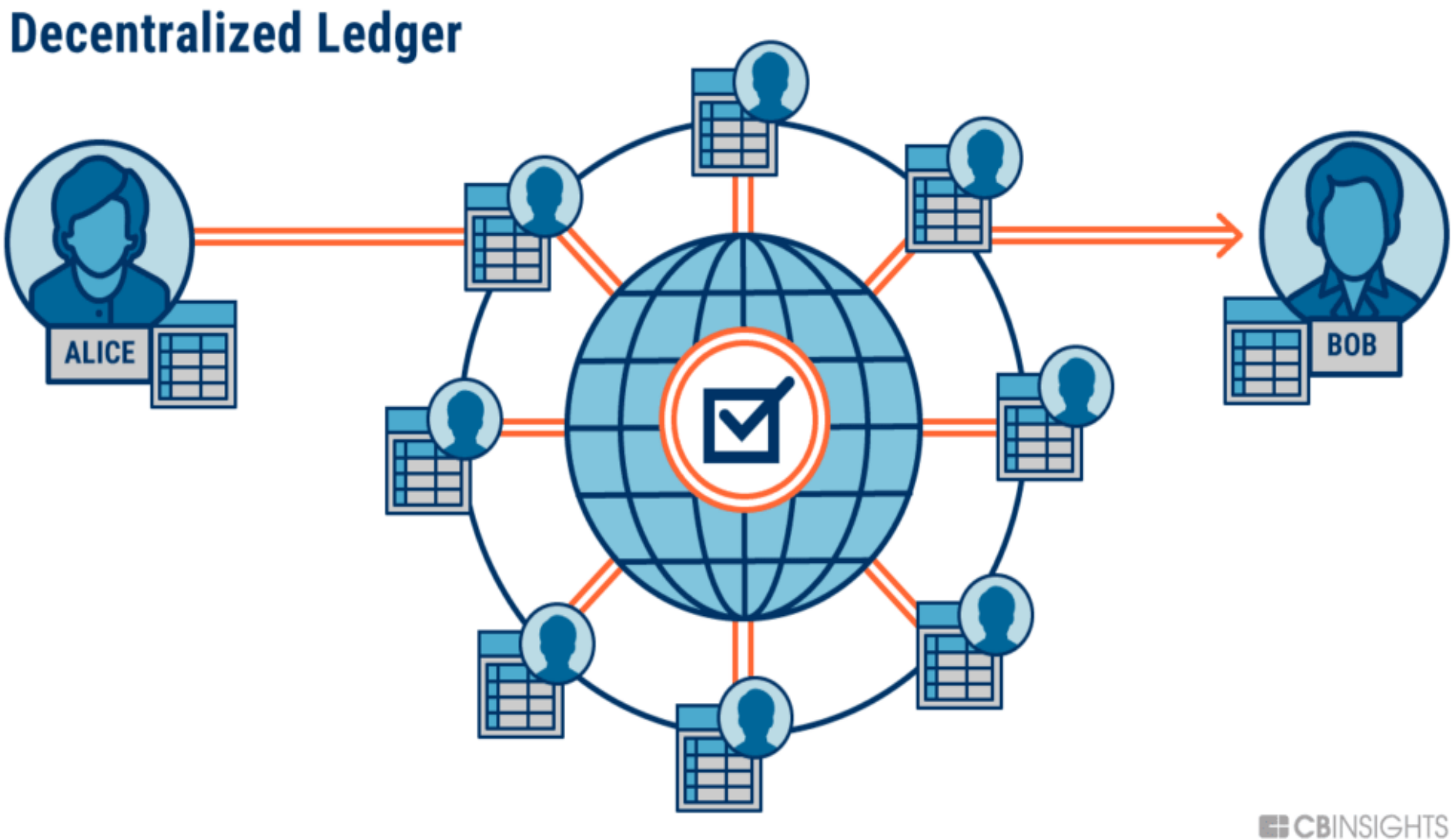
joint work with Ruizhe Jia (Columbia) and Ye Wang (ETH Zurich)

Outline

Blockchain Architecture

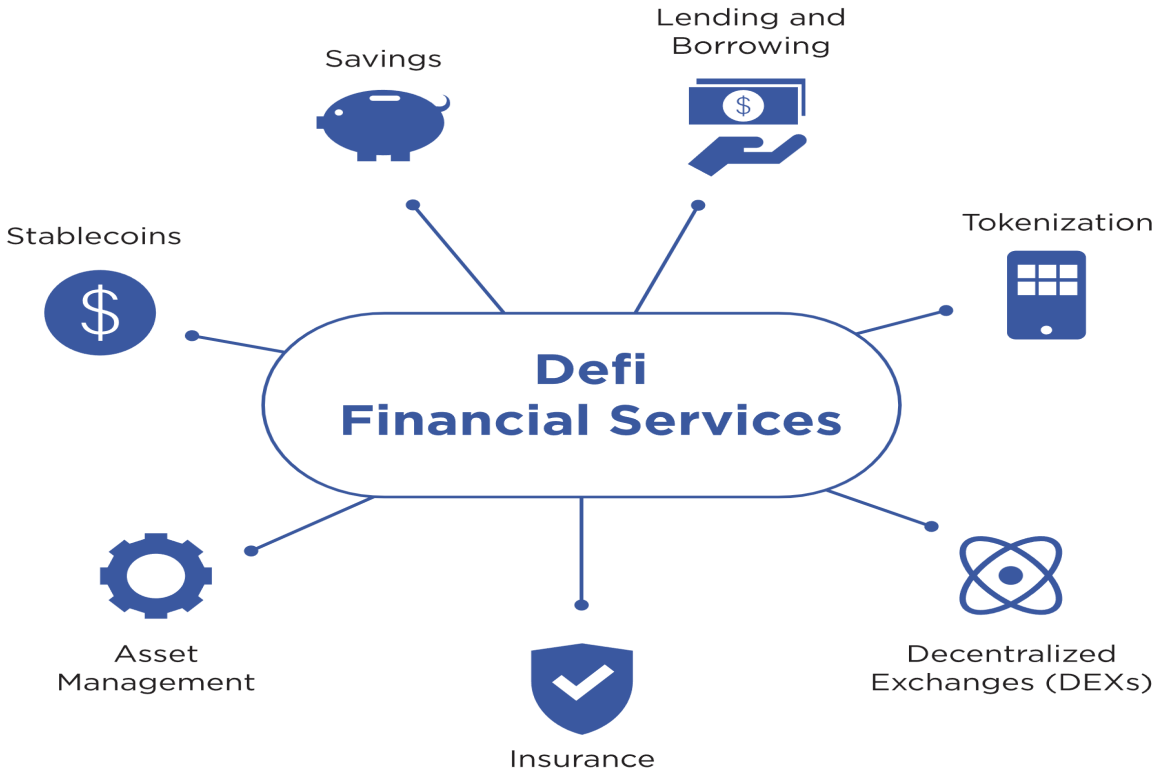


First Generation Blockchain: Payment Systems



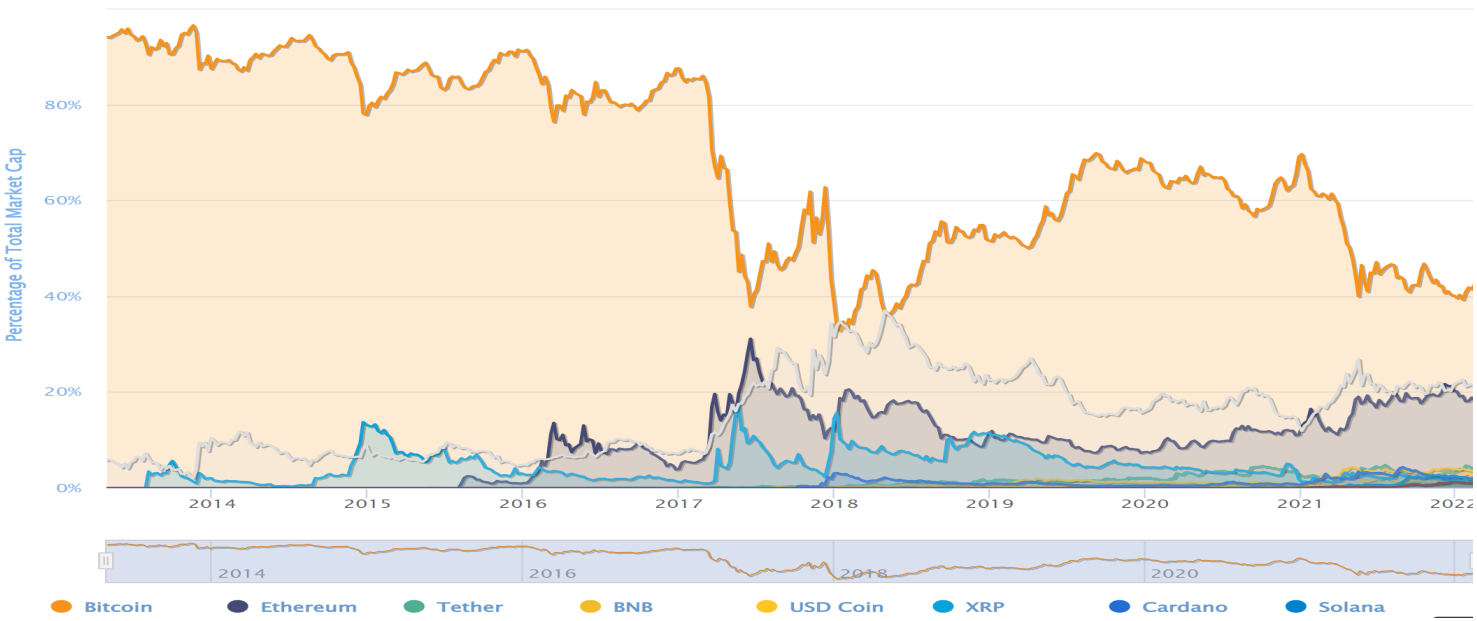
Second Generation Blockchain: Smart Contracts

- Second-generation blockchains (e.g. Etherum, Solana, ...) support smart contracts
- Smart contracts are computer programs running on a blockchain in accordance with predefined conditions agreed by contracting parties
- Smart contracts create protocols that implement financial services



From First to Second Generation Blockchain

- The services provided by blockchain systems shifted
  - from payment system: Bitcoin, Ripple XRP
  - to broader financial services: decentralized finance (Etherum, Solana), stable coins (Tether, Dai).



Transparency of Pending Transactions

A total of 235,292 pending txns found

(Showing the last 10000 records)

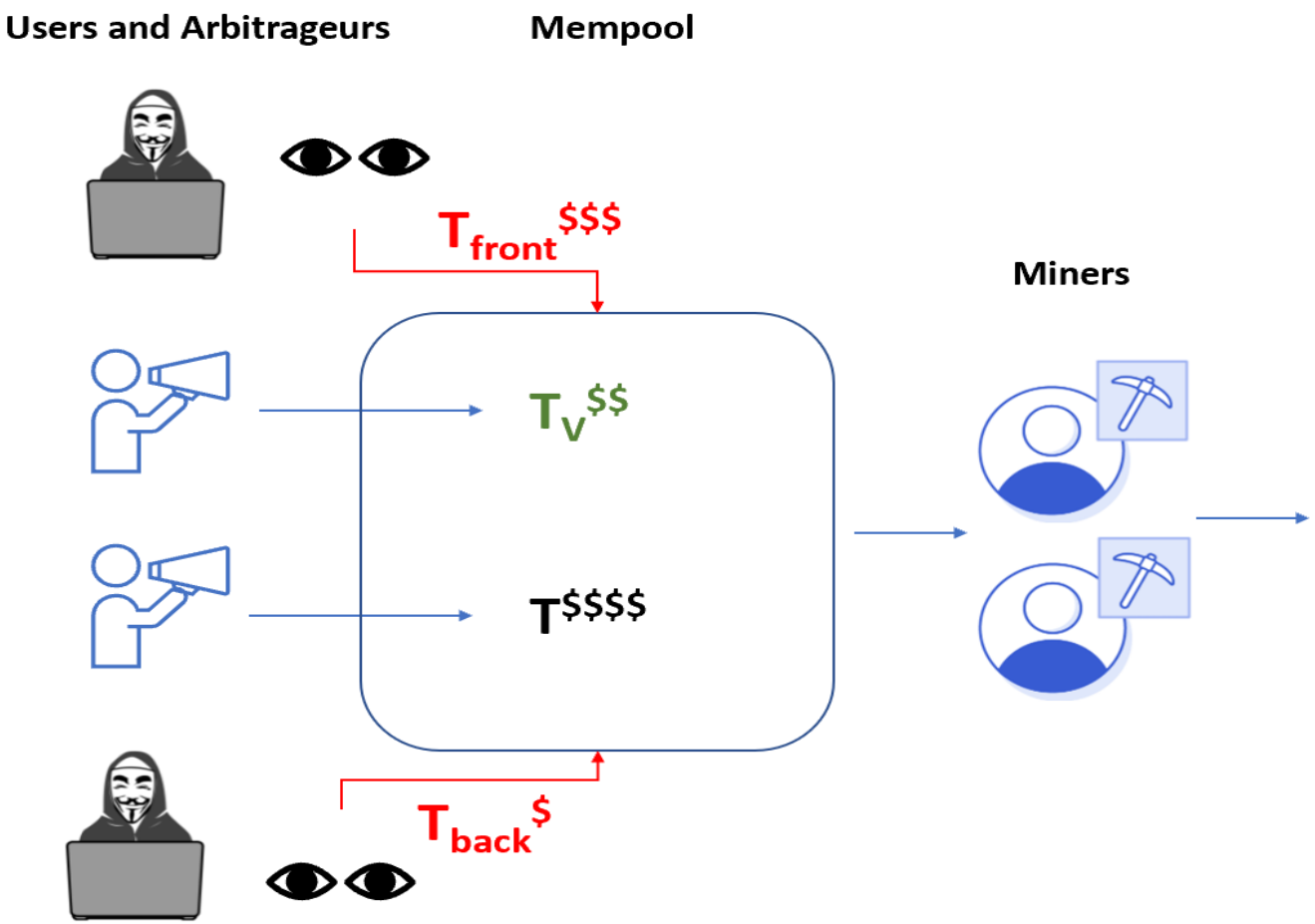
First ‹ Page 1 of 200 ›

Txn Hash	Nonce	Method ⓘ	Last Seen	Gas Limit	Gas Price ⓘ	From	To	Value
0x424b6f1f5098b573bf8...	31	0xc04b8d59	4 secs ago	296716	105.3884 | 1.5 Gwei	0x04729689f219cbd549...	Uniswap V3: Router	1.15 Ether
0x1f1a68ce3dd59685ed...	4164316	Transfer	4 secs ago	21000	185 | 2 Gwei	Coinbase 5	0xbcbd01a53140e26947...	0.05020473 E
0x9df4927481afc763d74...	13	Deposit	4 secs ago	45038	121.5063 | 1.5 Gwei	0x433db84f88f1944f3a5...	Wrapped Ether	0.5 Ether
0x18059111e7b412f3f55f...	475	Set Approval For...	4 secs ago	46747	110.2918 | 1.5 Gwei	0xf31fc1a5bfa83452184...	Based Fish Mafia: BFM T...	0 Ether
0xc733658c0a63c45c5f1...	73	Swap Exact Token...	4 secs ago	213798	105.3884 | 1.5 Gwei	0xc4f565416a9034ed52...	SushiSwap: Router	0 Ether

Blockchain Transparency

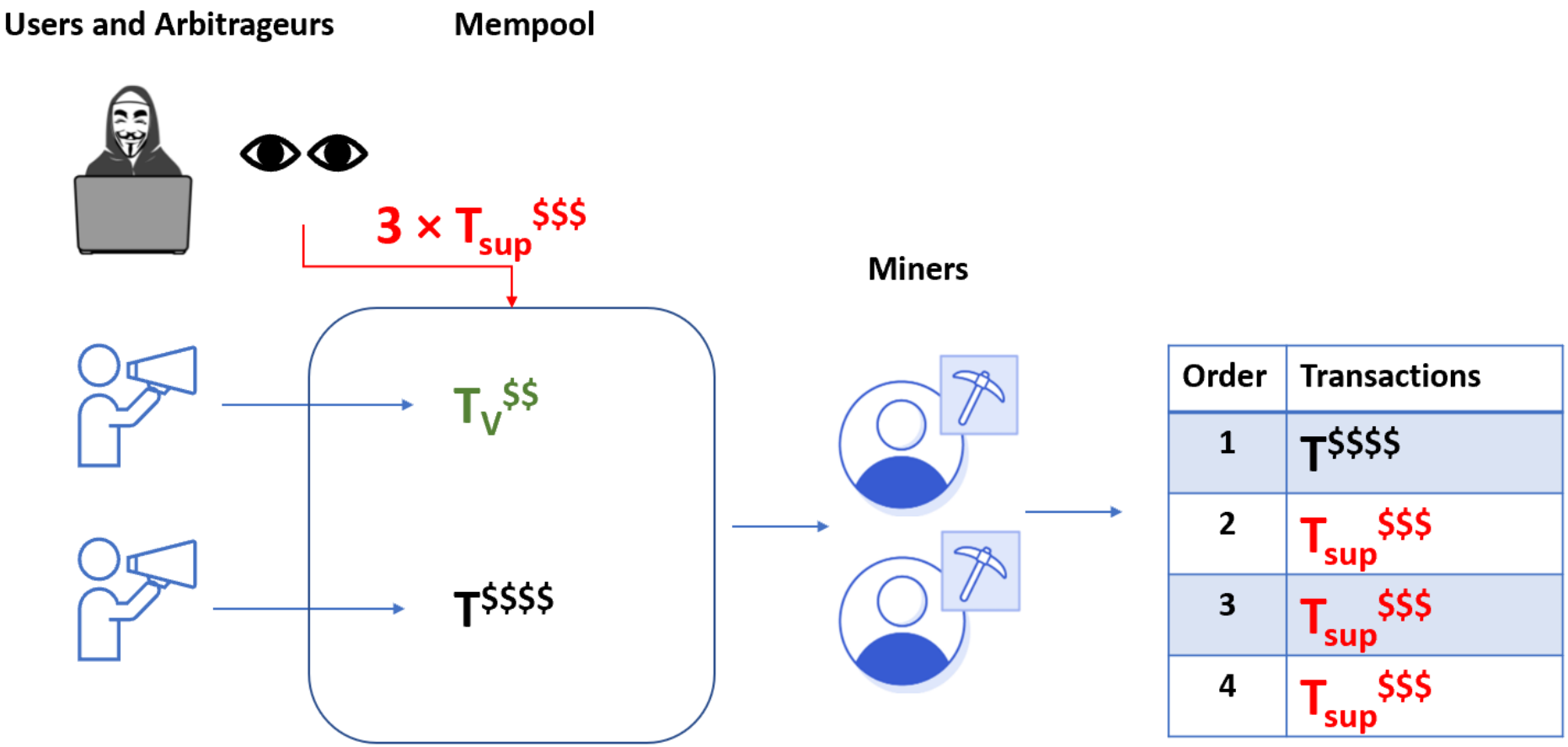
- Blockchain transparency can have unintended consequences
- Information on settled and pending transactions can be exploited by malicious attackers
- Pending transactions are revealed in the mem-pool before settlement, which leads to risk of frontrunning:
  - sandwich attack: frontrun + backrun
  - suppression attack: prevents certain transactions from getting on chain
  - displacement attack: creates identical transaction and frontrun
- Blockchain as a payment system: no frontrunning risk

Sandwich Attack

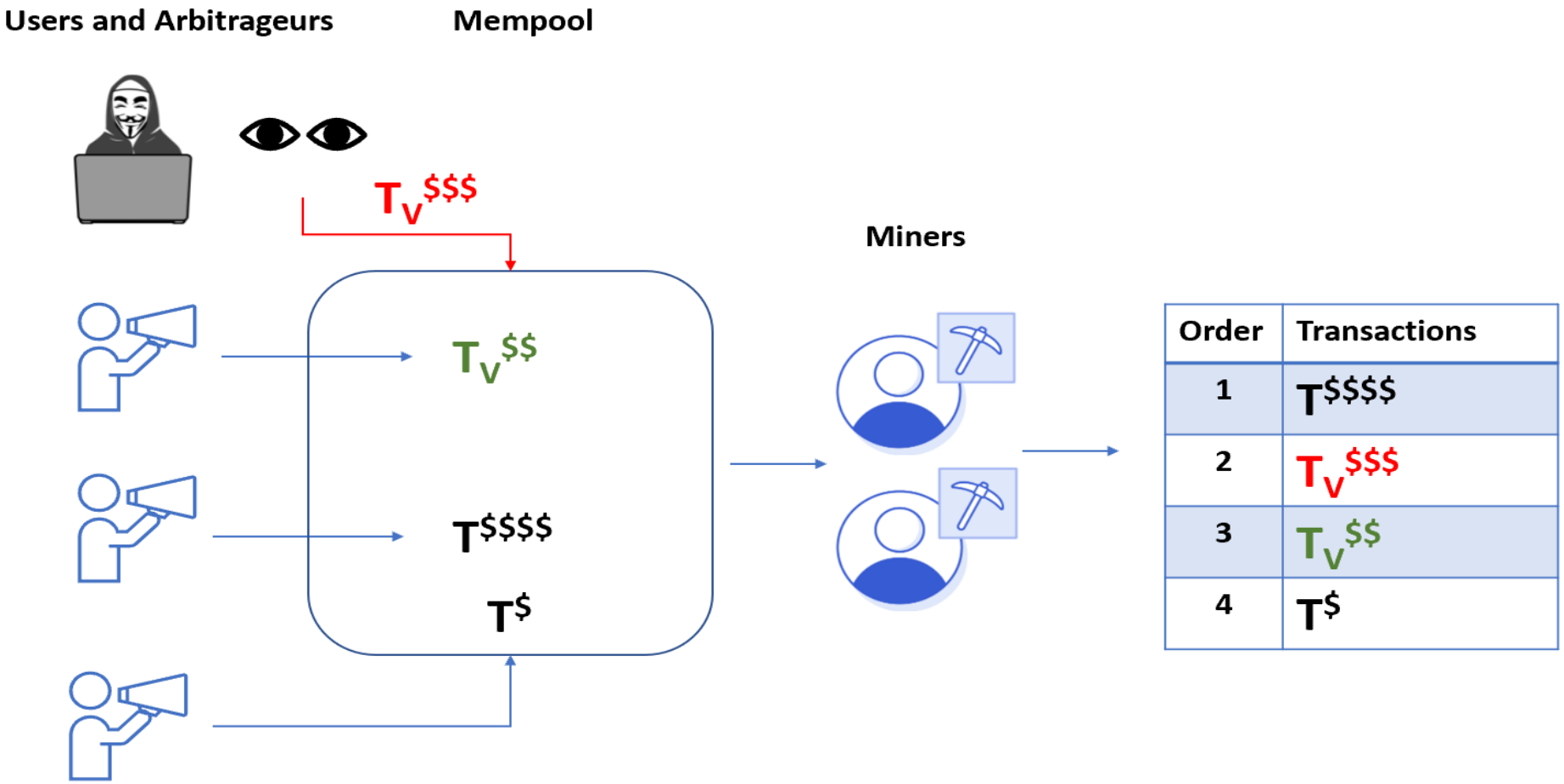


Order	Transactions
1	$T^{\$\$\$\$}$
2	$T_{front}^{\$\$\$}$
3	$T_V^{\$\$}$
4	$T_{back}^{\$}$

Suppression Attack



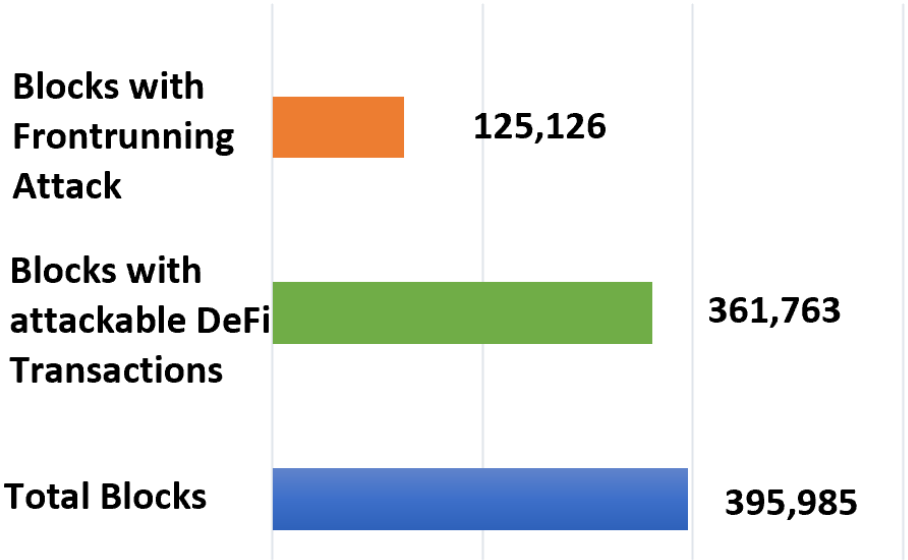
Displacement Attack

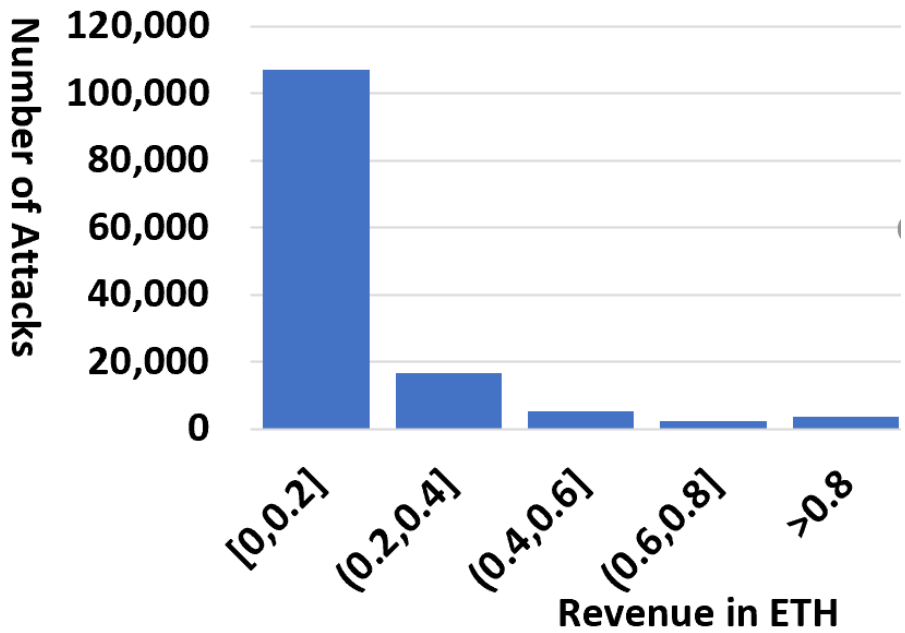


Order	Transactions
1	$T^{\$\$\$\$}$
2	$T_V^{\$\$\$}$
3	$T_V^{\$\$}$
4	$T^{\$}$

Is Frontrunning Material?

A third of blocks contain frontrunning attacks:



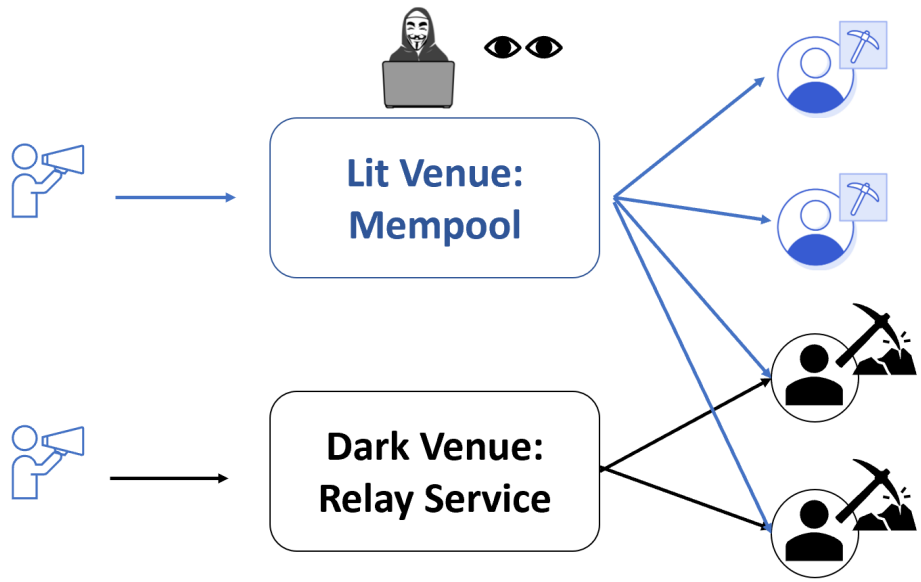


Private Submission Channels

- Relay Services create private channels:
  - Users can submit their transactions directly to miners without broadcasting.
  - Miners need to join the private channels to observe transactions submitted through these venues.
  - Miners must not disclose any transaction they observe.
- Flashbot and Eden Network are the two biggest relay service providers.
- Goal: reduce frontrunning and transaction cost externalities imposed by arbitrage bots.

Lit vs Dark Blockchain

- Relay Services (e.g. Flashbots) create private channels:
  - Users can submit their transactions directly to miners without broadcasting.
  - Miners need to join the private channels to observe transactions submitted through these venues.
  - Miners must not disclose any transaction they observe.
- Goal: reduce frontrunning and transaction cost externalities imposed by arbitrage bots.



Research Questions

- **Adoption:** Will the dark venue be adopted by participants of the blockchain ecosystem?
- **Mitigation of Frontrunning:** Will adoption achieve the intended purpose of reducing frontrunning arbitrage and transaction costs?
- **Welfare Implications:** Is the introduction of a dark venue welfare enhancing?

Research Findings

- Adoption: the dark venue is **at least partially adopted** by miners and utilized by at least one arbitrageur.
- Mitigation of Frontrunning: neither eliminates frontrunning arbitrage nor reduces transaction costs.
- Welfare Implications of a Dark Venue: Payoff of
  - Dark Venue Miners: strictly increases
  - Lit Venue Miners: weakly decreases
  - Frontrunnable users: increases
  - Arbitrageurs: decreases
  - Aggregate welfare: higher but not necessarily maximized.

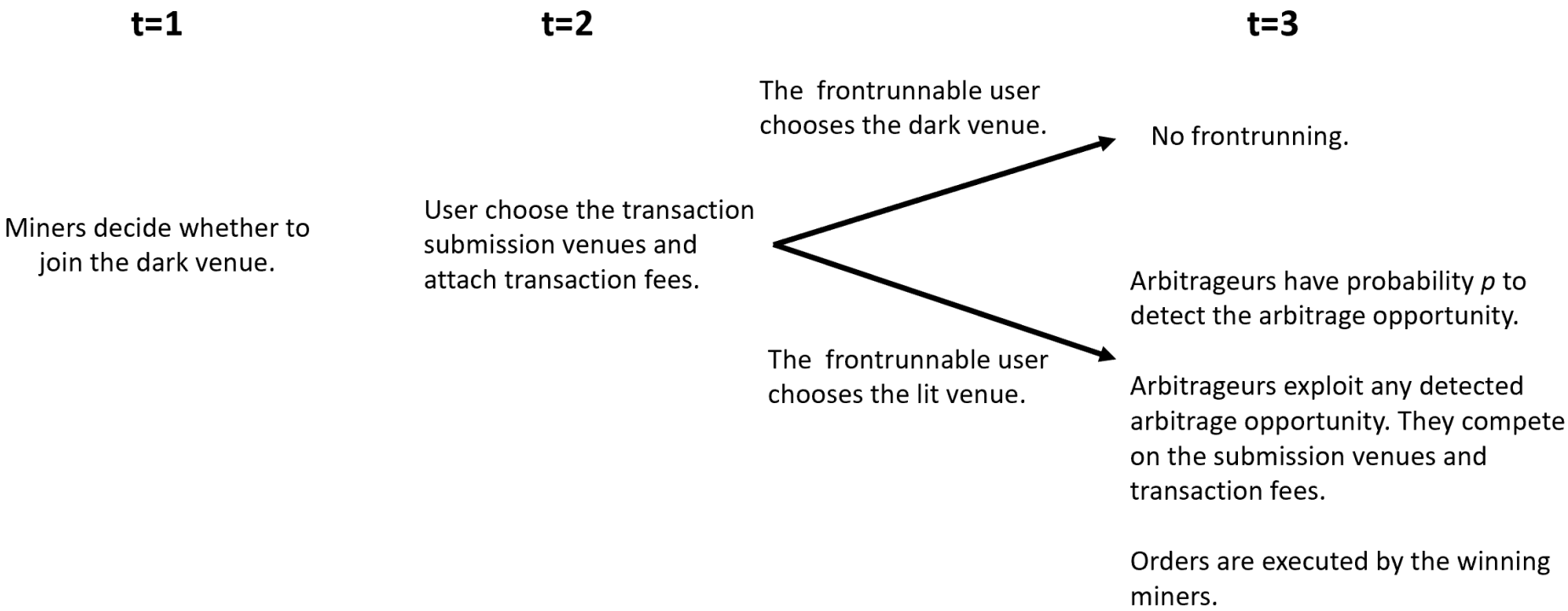
Related Literature

- Impact of frontrunning on DEX: Park (2021)
- Economic analysis of blockchain systems:
  - Consensus protocols (e.g., Biais et al. (2019); Saleh (2020); John et al. (2020); Roșu and Saleh (2021); Bakos and Halaburda (2021)).
  - Mining (e.g., Capponi et al. (2019); Cong et al. (2020); Prat and Walter (2021)).
  - Transactions fees (e.g., Huberman et al. (2021); Easley et al. (2019); Chung and Shi (2021); Roughgarden (2021)).
- Market microstructure literature on dark pools (e.g., Zhu (2014), Buti et al. (2017), Degryse et al. (2009))

Model Setup

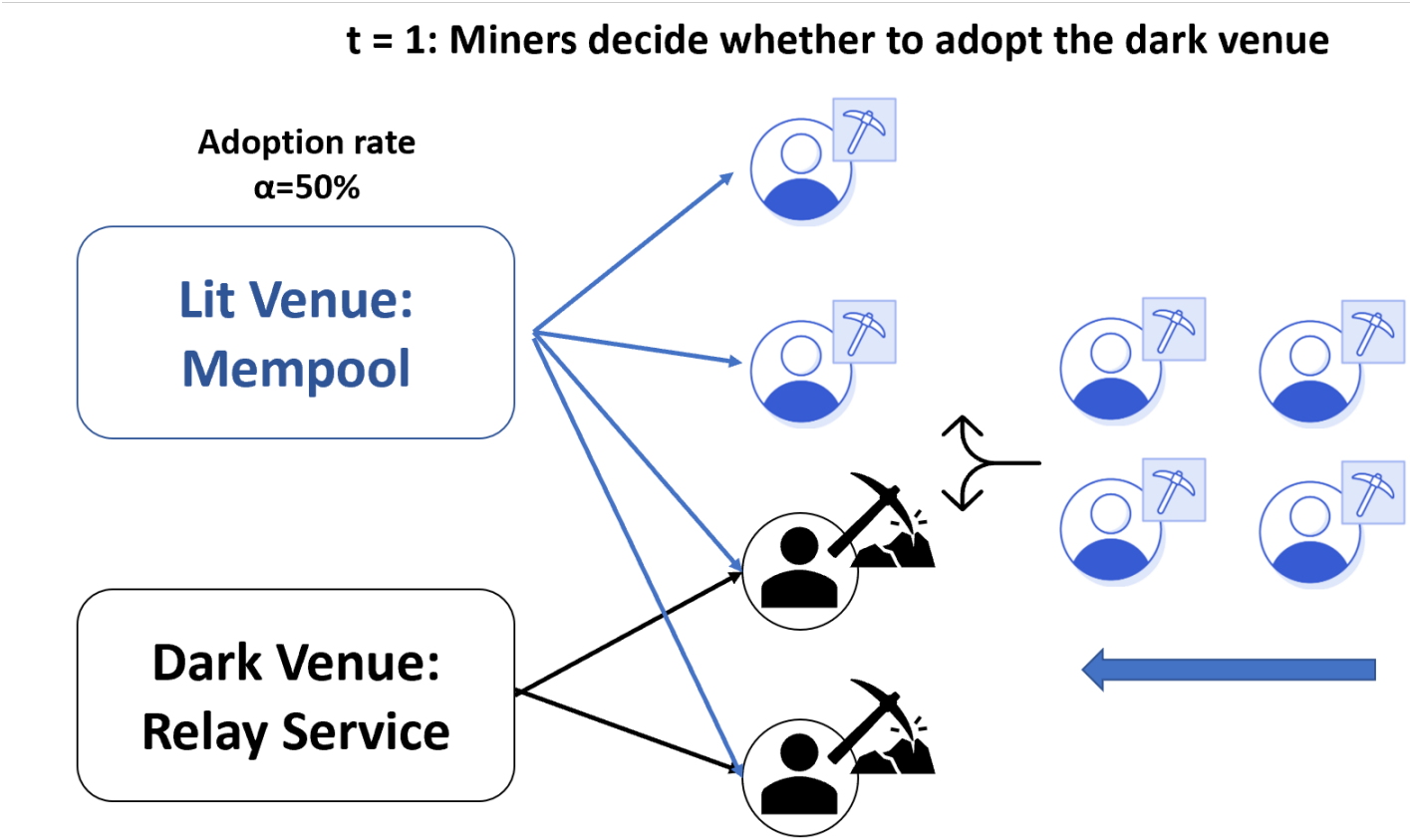
- 3 periods indexed by t, $t = 1, 2, 3$.
- 3 types of agents:
  - A continuum of homogeneous and rational miners
  - A frontrunnable user and a discrete set of non-frontrunnable users
  - Two arbitrageurs
- Two Transaction Submission Venues: Dark Venue and Lit Venue

Model Timeline



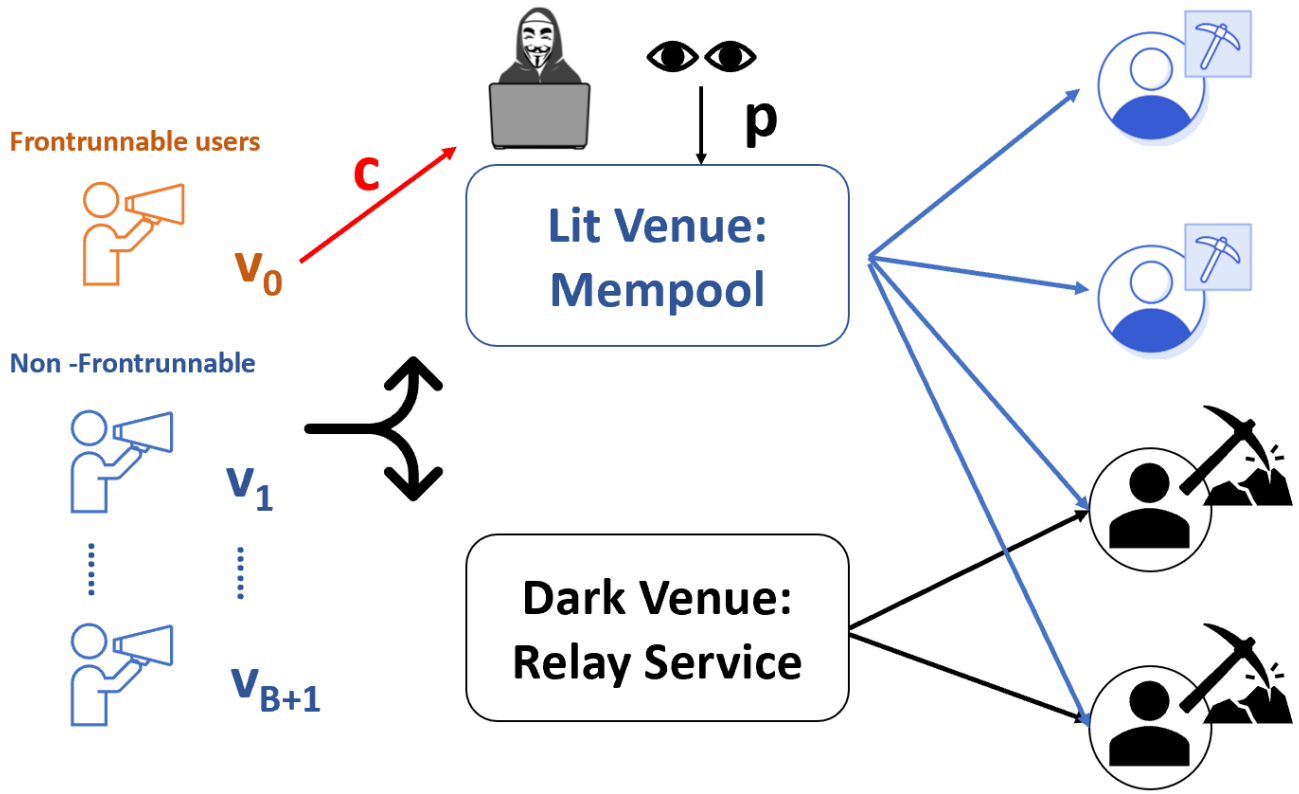
Period $t = 1$

- All miners observe transactions submitted through the lit venue
- Transactions submitted through the dark venue are observed only by miners who join the dark venue

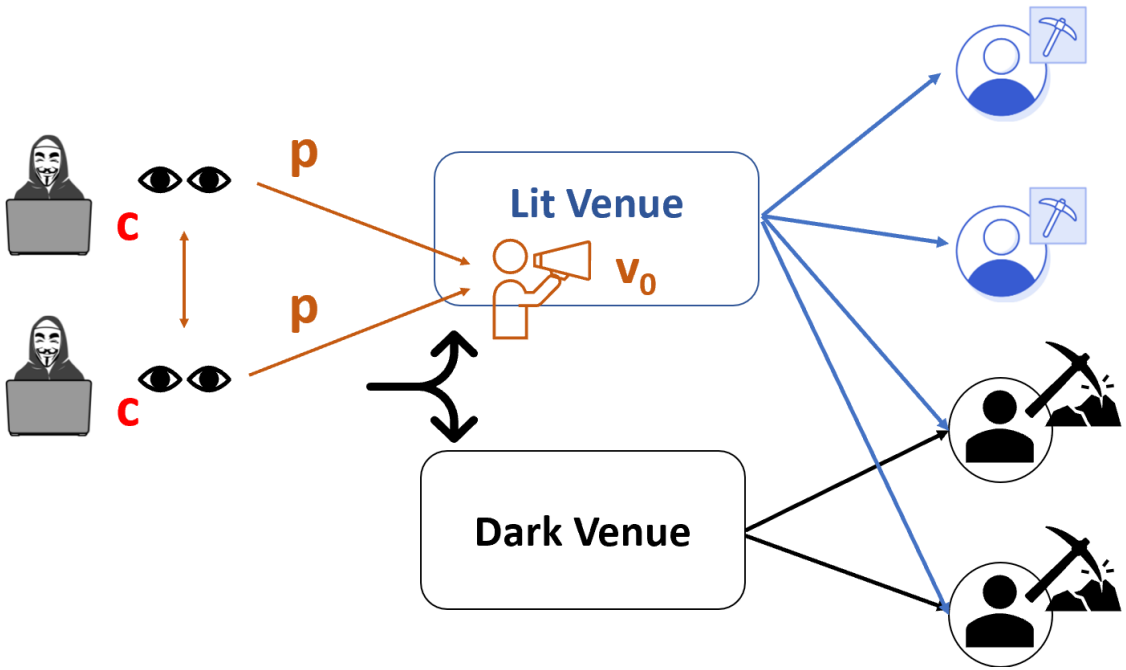


Period $t = 2$

- Frontrunnable user: loses $c > 0$ if his transaction is frontrun by an arbitrageur.
- Users simultaneously decide which venue to send their transactions and attached fees.



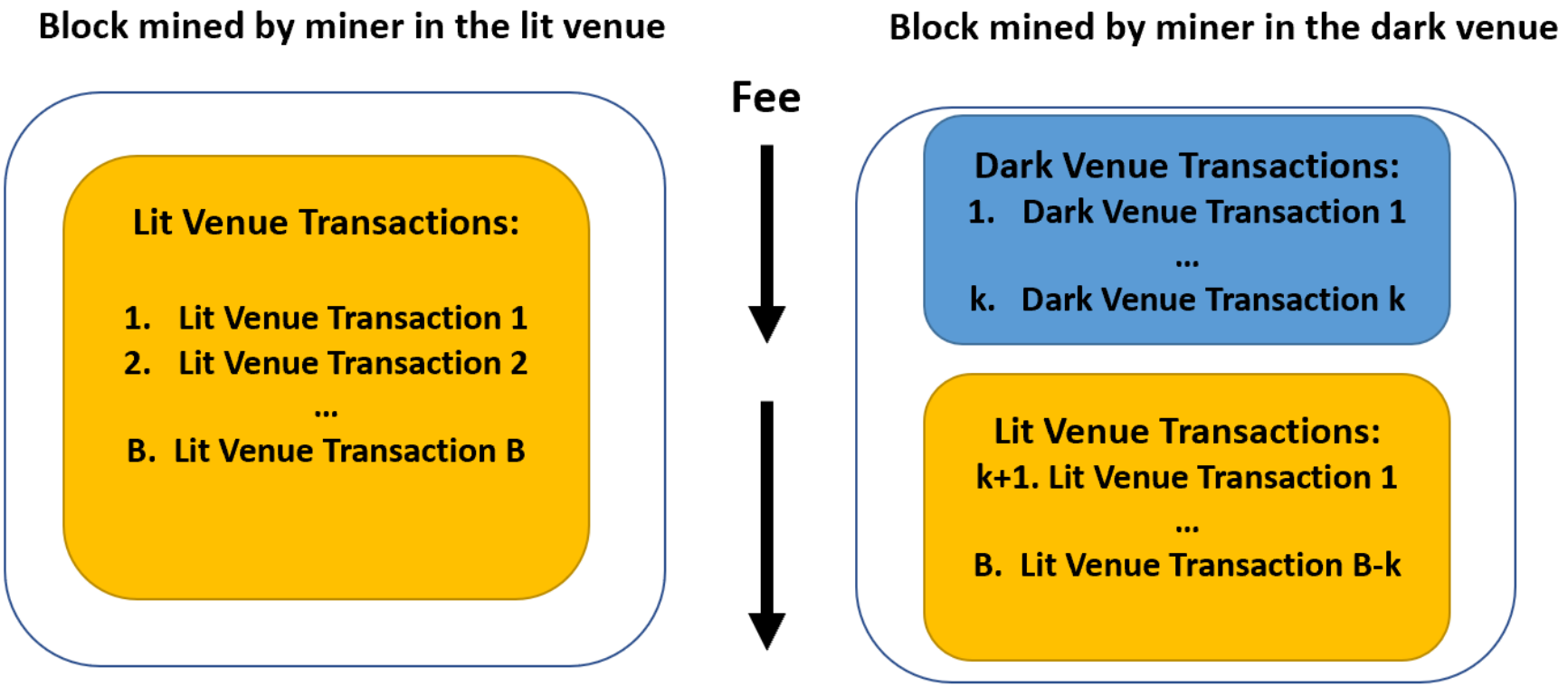
Period $t = 3$: Arbitragers' choice



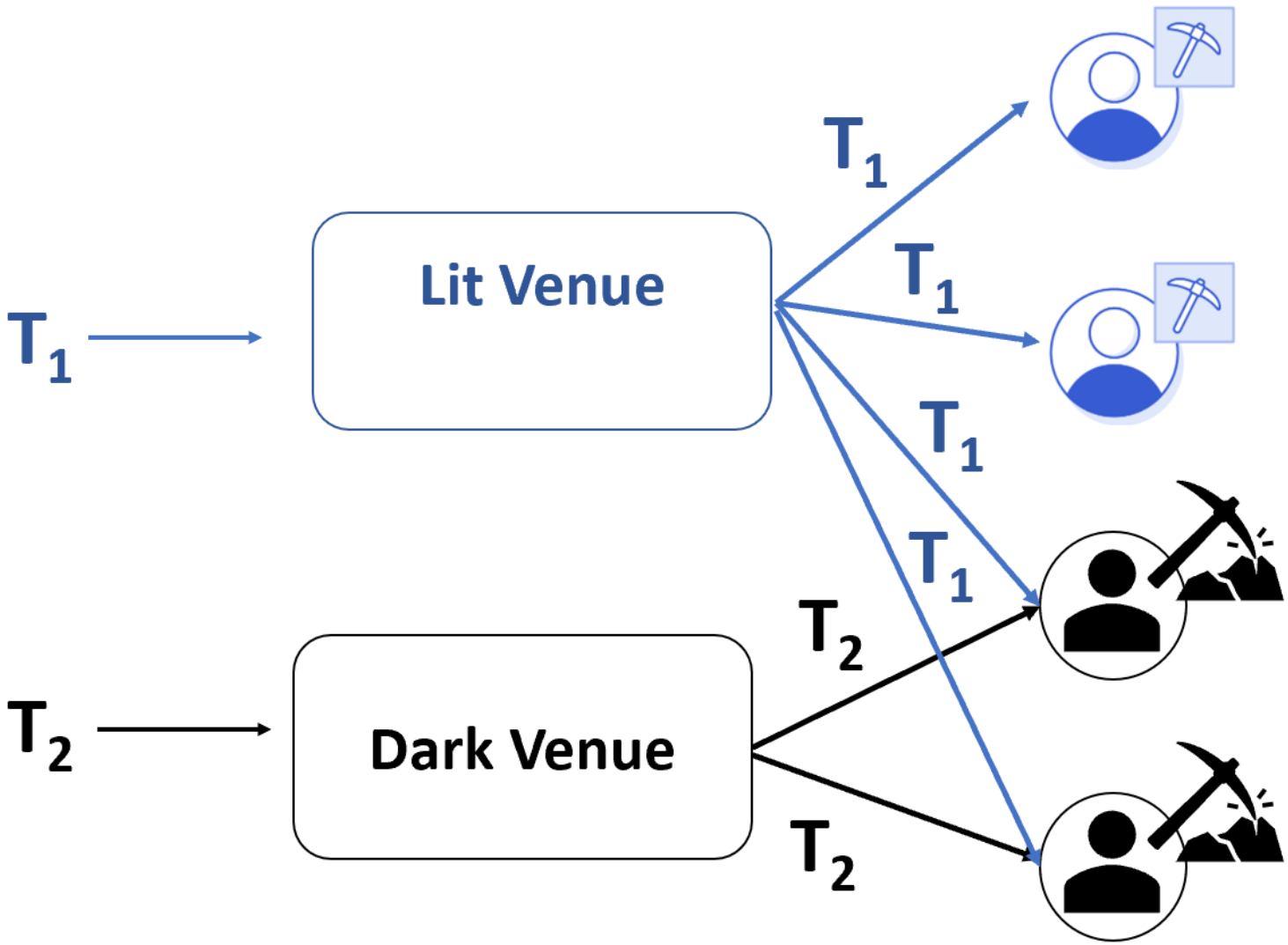
- An arbitrageur who exploits the opportunity earns a profit $c \geq 0$.
- For any opportunity, the arbitrageur creates an order, attaches a fee and decides which venue to use: lit venue, dark venue, or both.
- If the order is broadcast through the lit venue, the other arbitrageur will observe it

Period $t = 3$: Transaction Execution Order

- Block capacity is B.
- The winning miner can only select from the transactions he observes.
- Miner who mines the block selects B transactions whose attached fees are the highest.



Execution risk in the dark venue



Execution risk in the dark venue: arbitrageur

- **Execution risk:** a fraction $(1-\alpha)$ of miners may never observe transactions submitted to the dark venue.
- Trade-off faced by arbitrageurs
  - Pros of dark venue: priority execution and avoid information leakage
  - Cons of dark venue: execution risk
- If α is large, execution risk is low, choose dark venue only; if α is small, choose both venues together.
- If p is small, information is valuable, choose dark venue only; if p is large, no need to hide information, so choose both venues together.

Execution risk in the dark venue: frontrunnable users

- **Execution risk:** a fraction $(1-\alpha)$ of miners may never observe transactions submitted to the dark venue.
- Trade-off faced by users
  - Pros of dark venue: avoid frontrunning
  - Cons of dark venue: execution risk
- If α is large, execution risk is low, choose dark venue; if α is small, choose the lit venue.
- If p or c is large, frontrunning risk is high, choose dark venue; if p and c are small, choose the lit venue.

Miners' Adoption of Dark Venue

- Miners who join the dark venue can observe more transactions and earn the fees from arbitrageurs and users on the dark venue.
- If sufficiently many miners join the dark venue, that is, if α is large enough, miner's payoff may be lower than in the case $\alpha = 0$
  - Frontrunnable user may reroute her transaction from lit to dark venue if execution risk is small enough.
  - Migration of this transaction eliminates frontrunning opportunities, and thus reduce fees from arbitrageurs.

Equilibrium

Proposition (Subgame Perfect Equilibrium (SPE))

1. *If $c > c_1$, there exists a unique full adoption equilibrium where the adoption rate $\alpha^* = 1$, the frontrunnable user selects the dark venue, and the arbitrageurs do not submit arbitrage orders.*
2. *If $c \leq c_1$, there exists a partial adoption equilibrium where the dark venue's adoption rate $\alpha^* < 1$, the frontrunnable user submits her transaction through the lit venue, and the arbitrageurs send their orders to the dark venue only or to both venues.*

High Frontrunning Risk

- **If c is large:**
  1. Without the dark venue, the frontrunnable user will not submit his transaction.
  2. To incentivize the frontrunnable user to submit and earn the transaction fee, miners adopt the dark venue.
  3. In equilibrium, all miners decide to join the dark venue so that they are able to observe the transaction submitted by the frontrunnable user.

Low Frontrunning risk

- **If c is small:**
  1. Without a dark venue, the frontrunnable user would still submit his transaction to the blockchain
  2. Frontrunning arbitrage generates fees (arbitrageurs bid high fees to outbid each other) for miners.
  3. To maintain their revenue, only a small fraction of miners choose to adopt the dark venue, which creates high execution risk.
  4. The frontrunnable user prefers to submit through the lit venue and face frontrunning risk.
  5. **A dark venue does not prevent frontrunning arbitrage.**

Transaction Fees

- The introduction of a dark venue **increases the minimum fee** which guarantees the execution of a transaction!
- Since a dark venue weakly reduces the block space used by arbitrageurs, shouldn't we expect a decline in transaction costs? Not quite
  1. Miners adopt the dark venue only if they earn higher transaction fees, and thus the equilibrium transaction fees increase.
  2. The introduction of the dark venue may attract the frontrunnable transaction which would not have been submitted otherwise.

Testable Implications

- The blockchain dark venue will be at least partially adopted by miners
- Miners who adopt dark venue have a higher expected payoff than miners who stay in the lit venue.
- Users submit transaction through the dark venue when the frontrunning risk is high
- Arbitrageurs' transaction fees increase after the introduction of the dark venue.

Adoption rate of the dark venue (Flashbots).

Estimated Adoption Rate = Blocks mined with Flashbots Relay/ Total Blocks mined

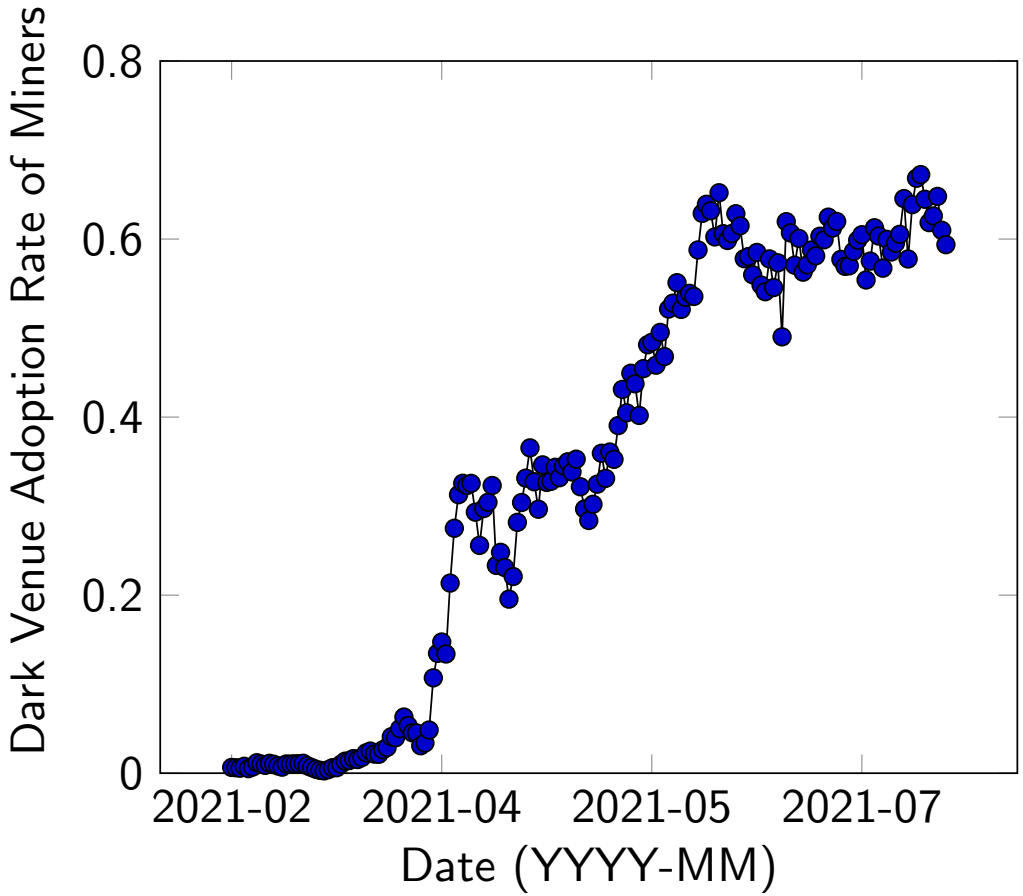
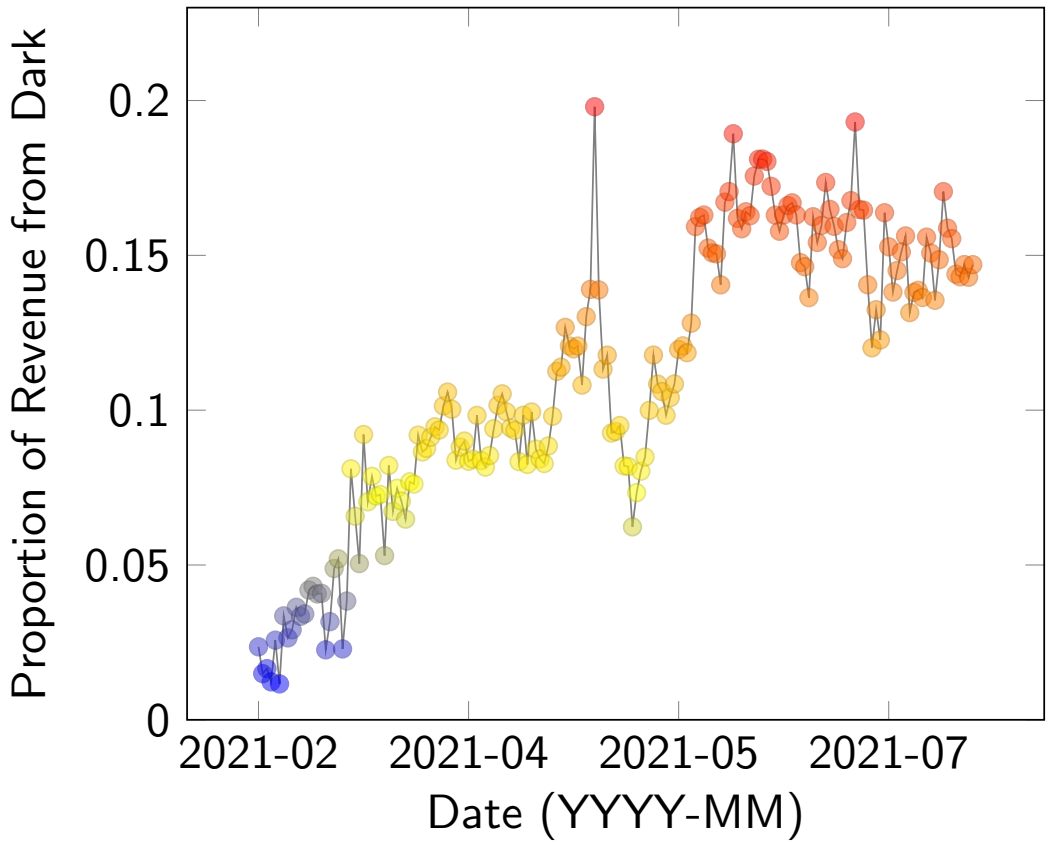


Figure: Adoption rate of Flashbots.

Proportion of Flashbots miners' revenue from dark venue.



Miners' Revenue in Dark and Lit Venues.

Expected payoff of miner who joins the dark venue higher (around 0.16 ETH per block) than the expected payoff of miners who stay in the lit venue.

	Dependent variables: Miner's Revenue per Block
Intercept	1.21^{***}
	(0.06)
Dark	0.16^{***}
	(0.032)
Day fixed effects?	yes
Observations	1,762,017
R^2	0.02
Note:	*p<0.1; **p<0.05; ***p<0.01

Users' Migration

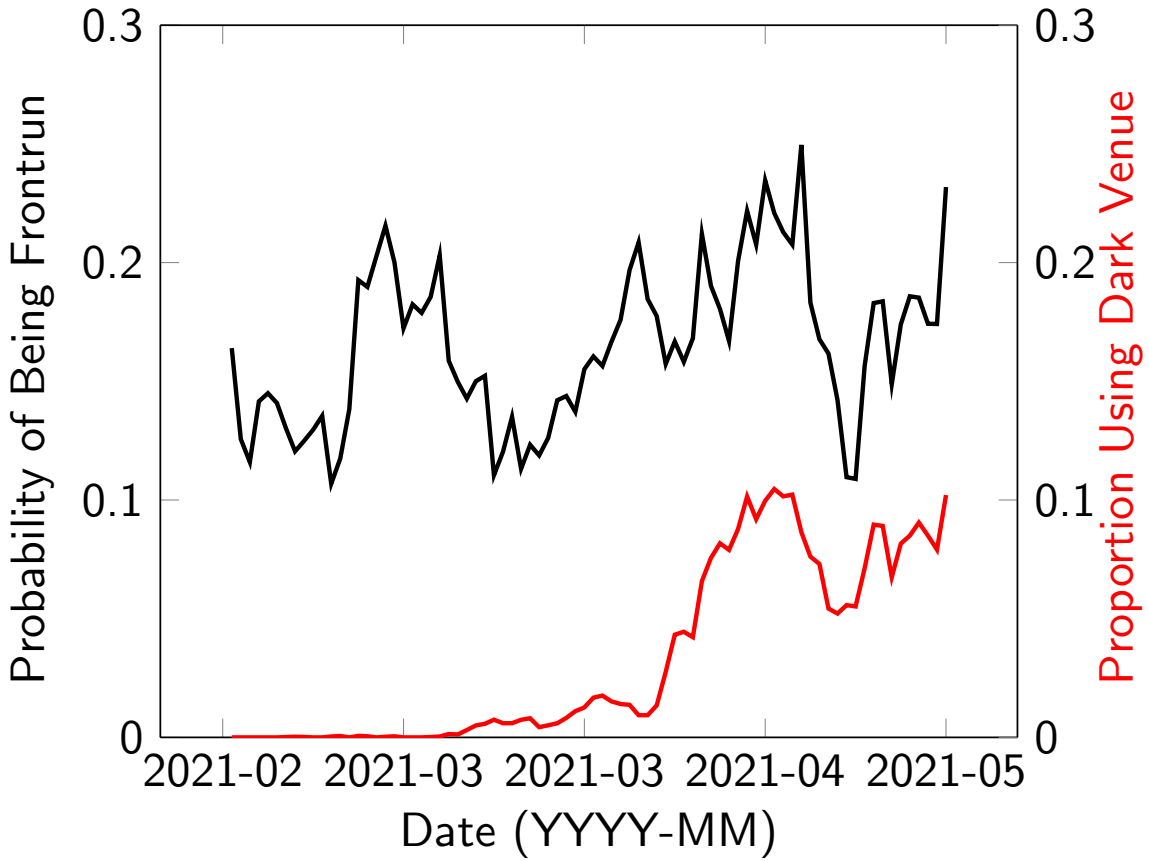


Figure: The black line represents the daily average probability of being attacked for frontrunnable users. The red line represents the daily proportion of frontrunnable transactions sent to dark venue.

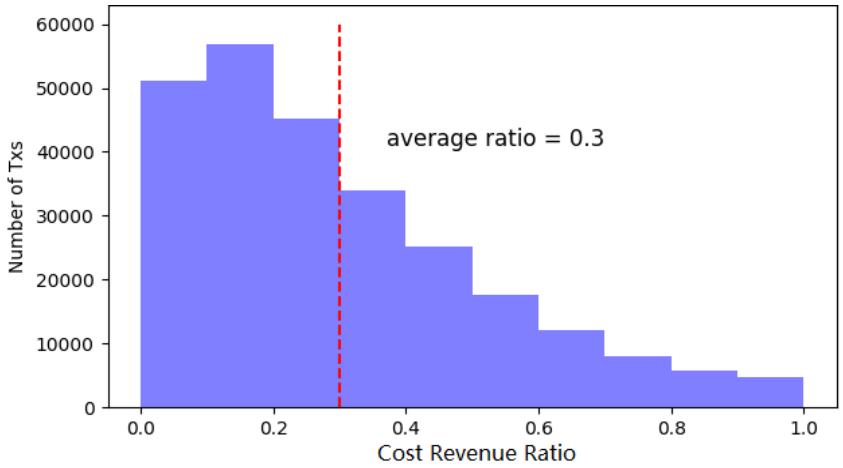
Users' Migration

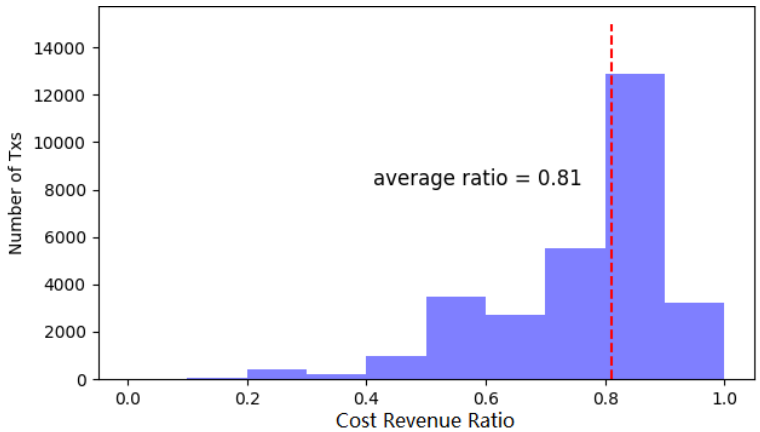
A 1% increase in probability of being frontrun is associated with a 0.6% increase in the proportion of frontrunnable transactions submitted through the dark venue.

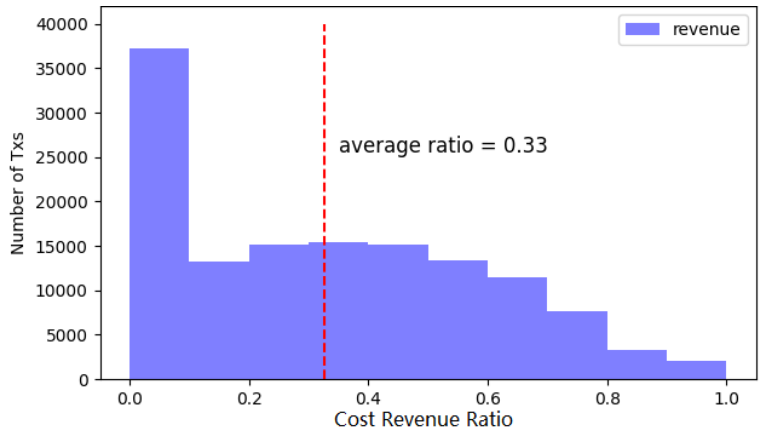
	Dependent variables: *Proportion of Transactions Through Dark*
Intercept	-0.066
	(0.18)
Probability of Being Frontrun	0.605***
	(0.010)
Observations	80
R^2	0.3
Note:	*p<0.1; **p<0.05; ***p<0.01

Arbitrageurs' Welfare

Cost-to-Revenue Ratio = Gas fees paid/ Total Revenue from frontrunning







Arbitrageurs' Welfare

After the introduction of the dark venue, arbitrageurs' cost increases by a third, mainly due to arbitrage transactions sent through dark venue.

	Dependent variables: Cost-to-revenue Ratio	
	(a)	(b)
Intercept	0.300^{***}	0.300^{***}
	(0.001)	(0.001)
After	0.091^{***}	0.013^{***}
	(0.001)	(0.001)
Dark		0.441^{***}
		(0.002)
Observations	428,685	428,685
R^2	0.03	0.19
Note:		*p<0.1; **p<0.05; ***p<0.01

Conclusion

- The increased use of blockchain for financial services leads to rethinking the transaction submission channels.
- Relay channels which create dark venues will be at least partially adopted by miners and utilized by arbitrageurs.
- But transaction costs on blockchain will not be lower.
- Miners who join the dark venue will have higher payoff, whereas miners who stay in the lit venue will have lower payoff.
- Users have higher pay-offs while arbitrageurs have lower pay-offs.

Thank You!

Yannis Bakos and Hanna Halaburda. 2021. *Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance*. Working Paper.

Bruno Biais, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta. 2019. The Blockchain Folk Theorem. *The Review of Financial Studies* 32, 5 (04 2019), 1662–1715.

Sabrina Buti, Barbara Rindi, and Ingrid M. Werner. 2017. Dark pool trading strategies, market quality and welfare. *Journal of Financial Economics* 124, 2 (2017), 244–265. `https://EconPapers.repec.org/RePEc:eee:jfinec:v:124:y:2017:i:2:p:244-265`

Agostino Capponi, Sveinn Olafsson, and Humoud Alsabah. 2019. *Proof-of-Work Cryptocurrencies: Does Mining Technology Undermine Decentralization?* Working Paper.

Hao Chung and Elaine Shi. 2021. Foundations of Transaction Fee Mechanism Design. *arXiv preprint arXiv:2111.03151* (2021).

Lin William Cong, Zhiguo He, and Jiasun Li. 2020. Decentralized Mining in Centralized Pools. *The Review of Financial Studies* 34, 3 (04 2020), 1191–1235.

Hans Degryse, Mark Van Achter, and Gunther Wuyts. 2009. Dynamic order submission strategies with competition between a dealer market and a crossing network. *Journal of Financial Economics* 91, 3 (2009), 319–338. https://EconPapers.repec.org/RePEc:eee:jfinec:v:91:y:2009:i:3:p:319-338

David Easley, Maureen O'Hara, and Soumya Basu. 2019. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics* 134, 1 (2019), 91–109.

Gur Huberman, Jacob D Leshno, and Ciamac Moallemi. 2021. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies* 88, 6 (03 2021), 3011–3040.

Kose John, Thomas J Rivera, and Fahad Saleh. 2020. *Economic Implications of Scaling Blockchains: Why the Consensus Protocol Matters*. Working Paper.

Andreas Park. 2021. *The Conceptual Flaws of Constant Product Automated Market Making*. Working Paper.

Julien Prat and Benjamin Walter. 2021. An Equilibrium Model of the

Market for Bitcoin Mining. *Journal of Political Economy* 129, 8 (2021), 2415–2452.

Tim Roughgarden. 2021. Transaction fee mechanism design. *ACM SIGecom Exchanges* 19, 1 (2021), 52–55.

Ioanid Roşu and Fahad Saleh. 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science* 67, 2 (2021), 661–672.

Fahad Saleh. 2020. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies* 34, 3 (07 2020), 1156–1190.

Haoxiang Zhu. 2014. Do Dark Pools Harm Price Discovery? *The Review of Financial Studies* 27, 3 (2014), 747–789. `http://www.jstor.org/stable/24465693`