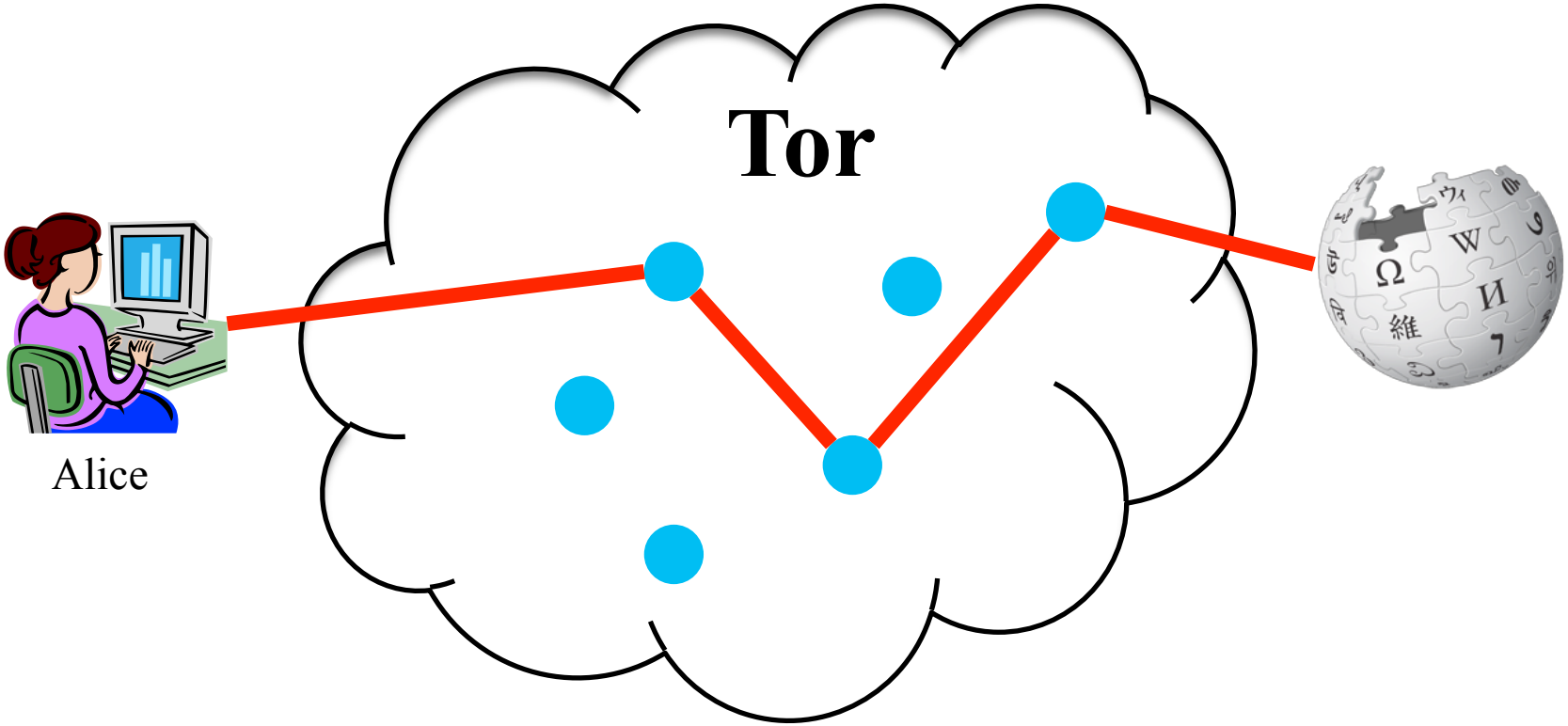
BLACR: TTP-Free Blacklistable Anonymous Credentials with Reputation

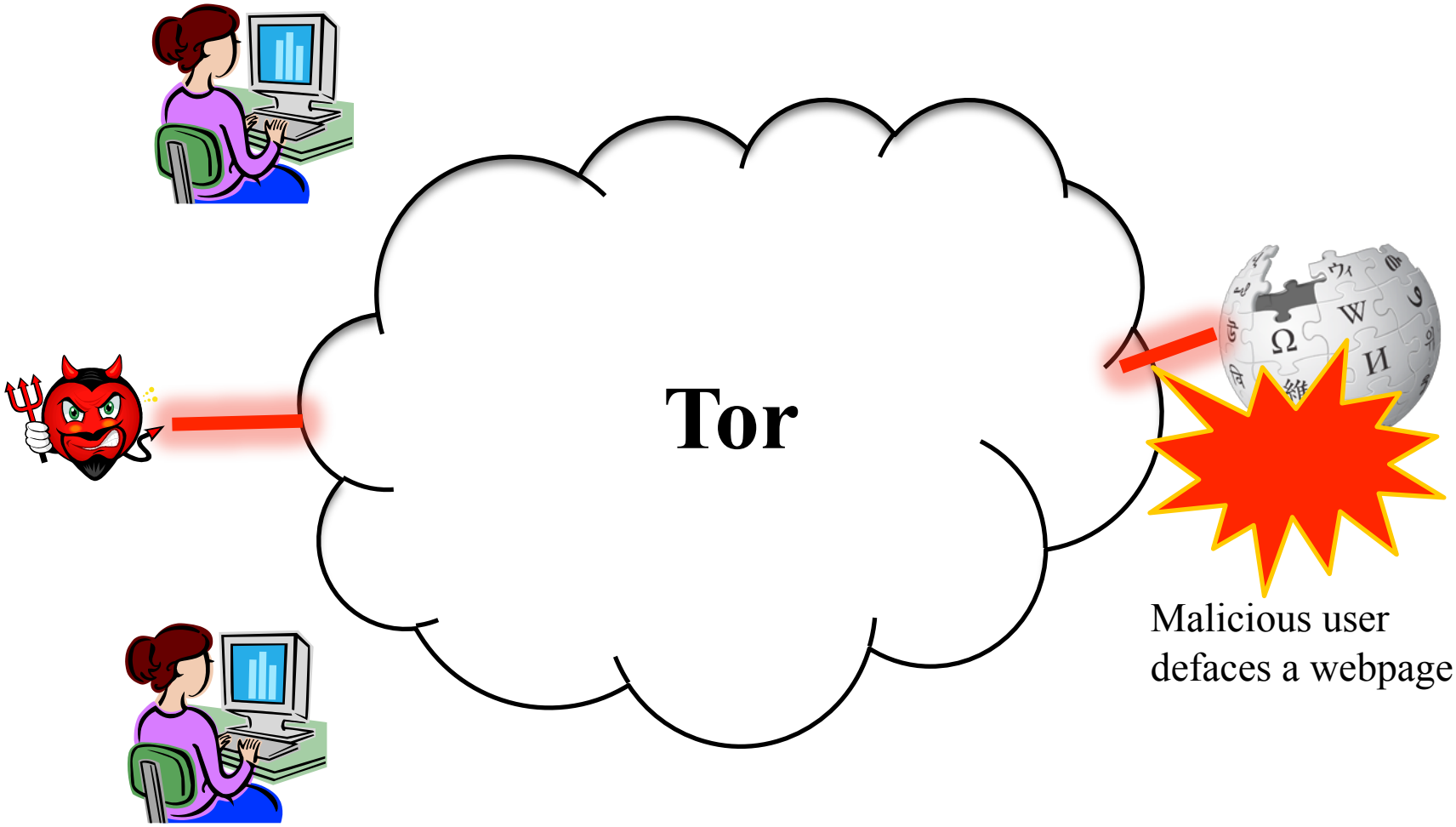
Man Ho Au, Apu Kapadia, Willy Susilo
University of Wollongong &
Indiana University Bloomington

Anonymous access to services protects users' privacy



Tor prevents Wikipedia from learning Alice's location or browsing habits

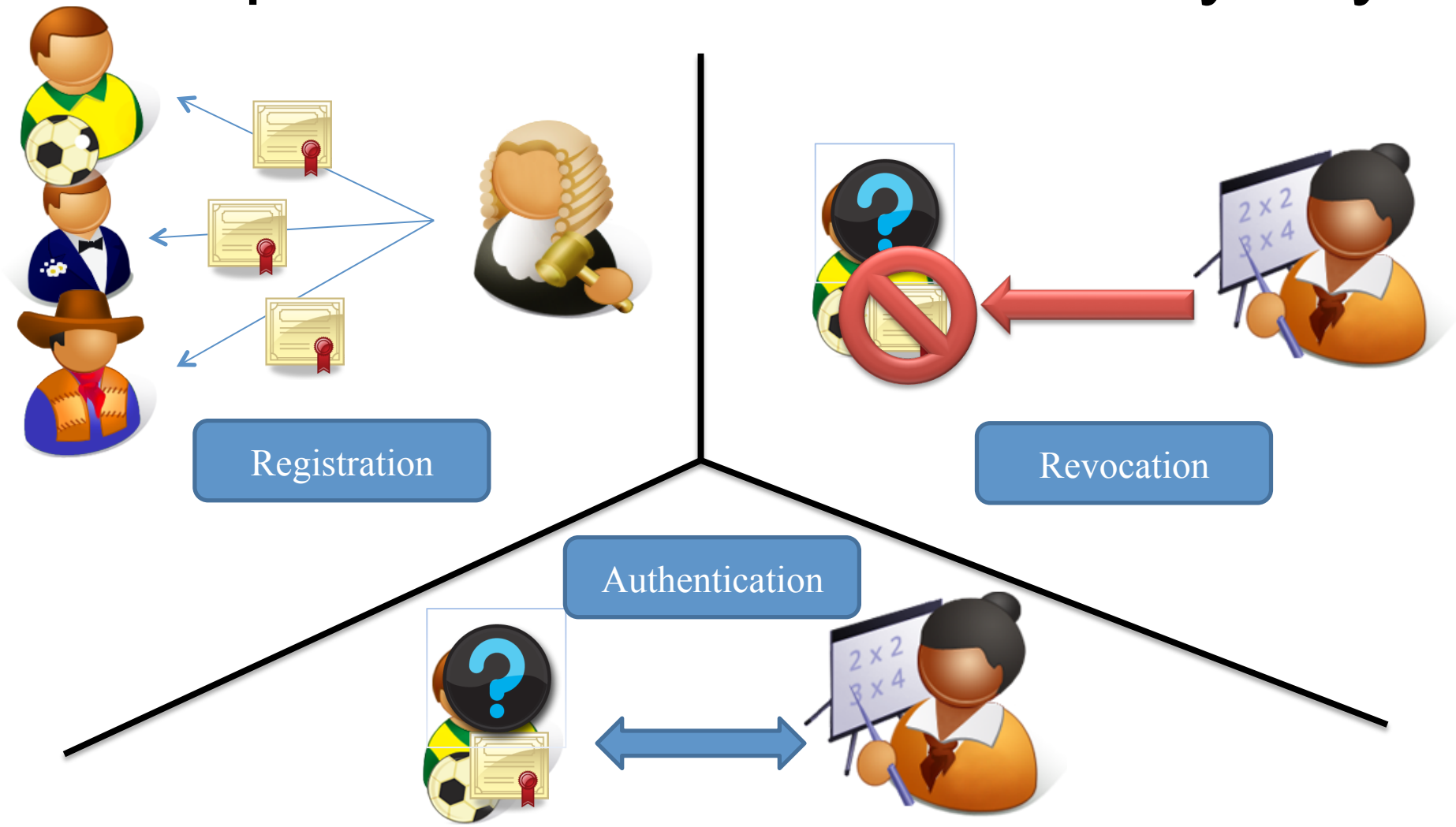
Unfortunately, users can abuse their anonymity



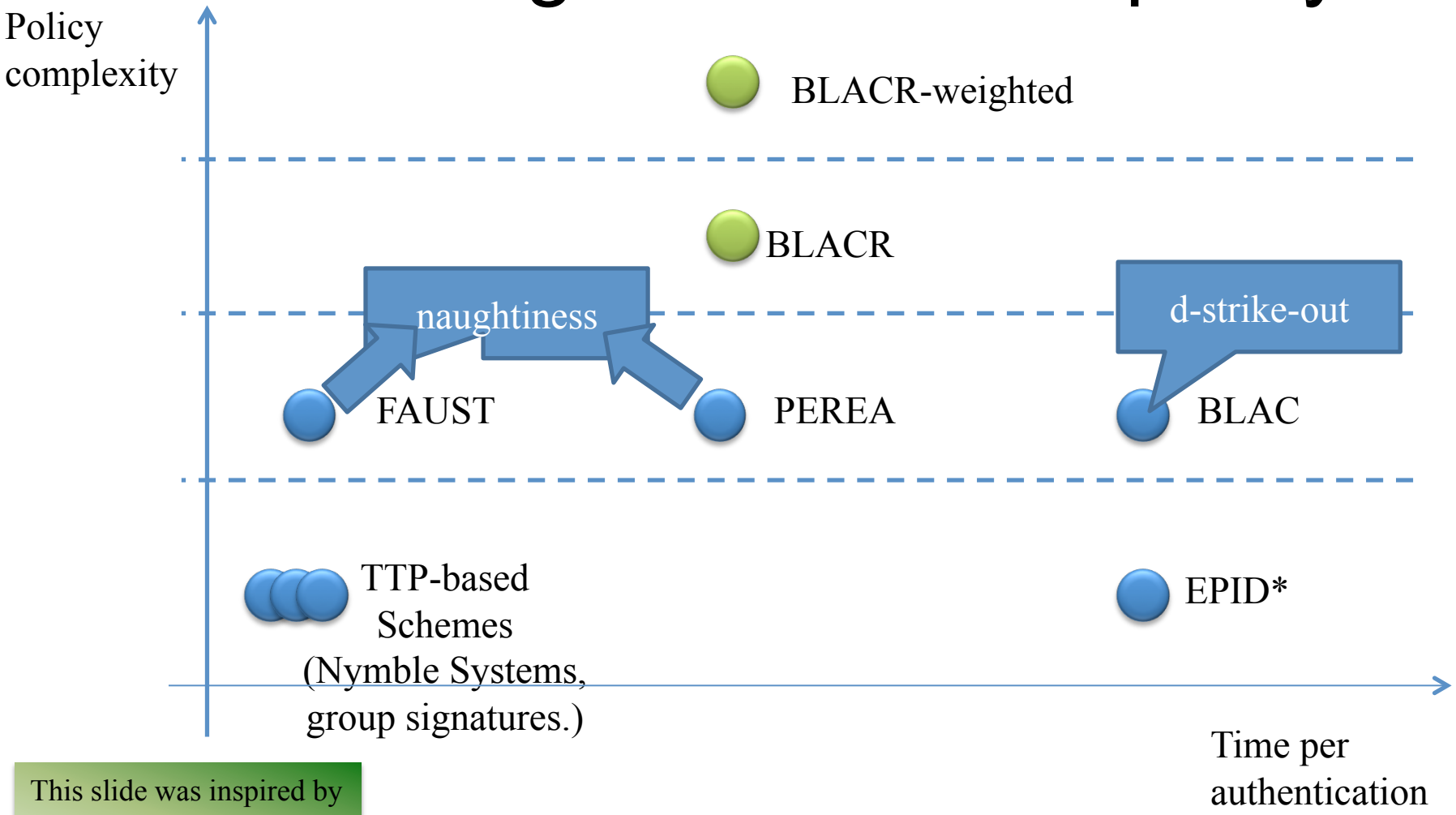
In response, some providers block anonymous access entirely

How can we strike a balance between accountability and anonymity?

Revocable anonymous credentials can provide accountable anonymity

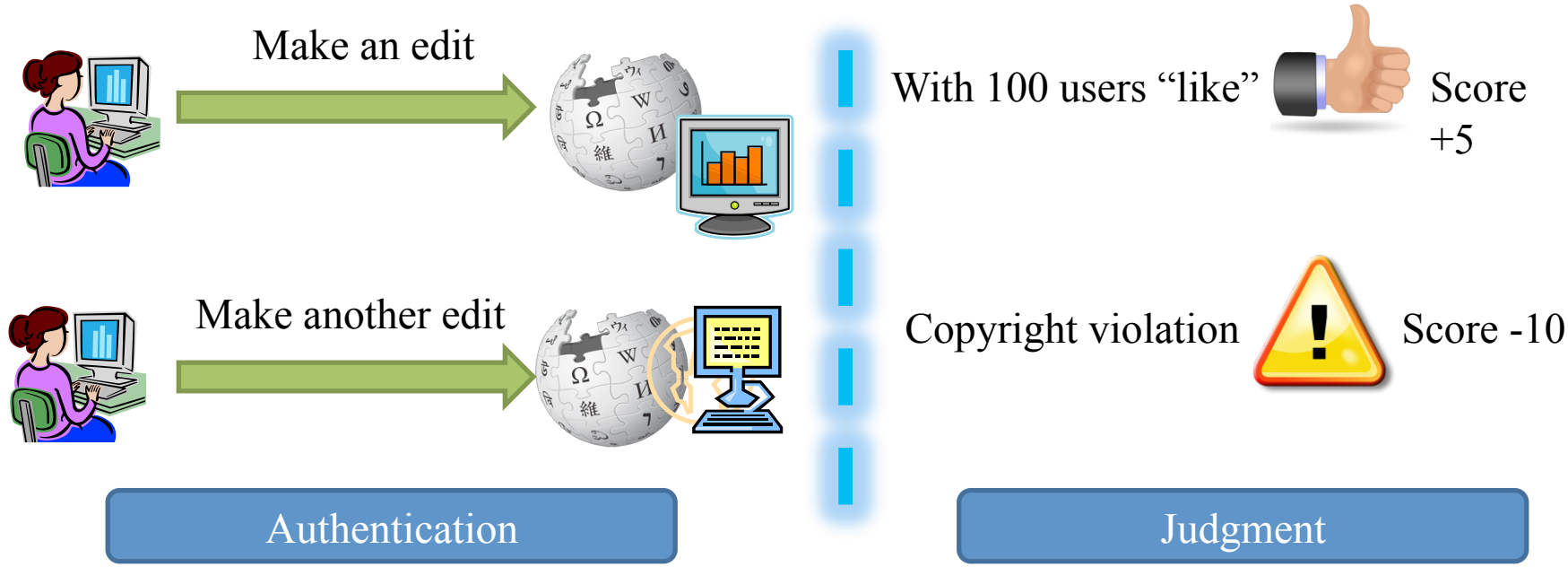


BLACR is TTP-free and provides the most general access policy



This slide was inspired by Nick Hopper's presentation on FAUST.

BLACR adds reputation to BLAC



Reputation = 5 – 10 = -5

Access Policy: User can authenticate if his/her reputation is above -10

Generalisation of naughtiness which supports positive score

BLACR scores reputation across different categories

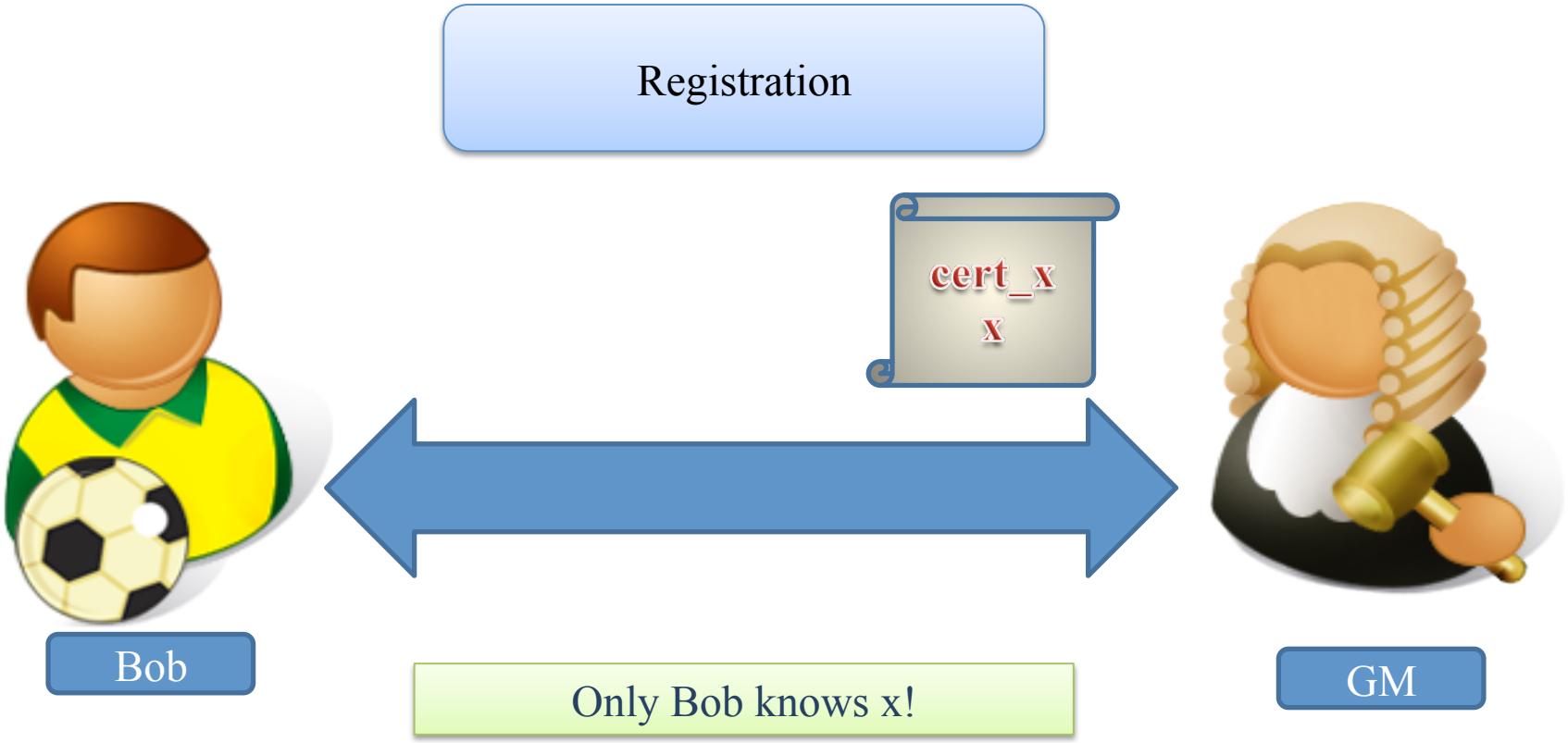
A sever may maintain categories for **video content** and **comments**

Video Content Rules:	
100 good karma	+ 5
Minor copyright violations	-2
Major copyright violations	-10

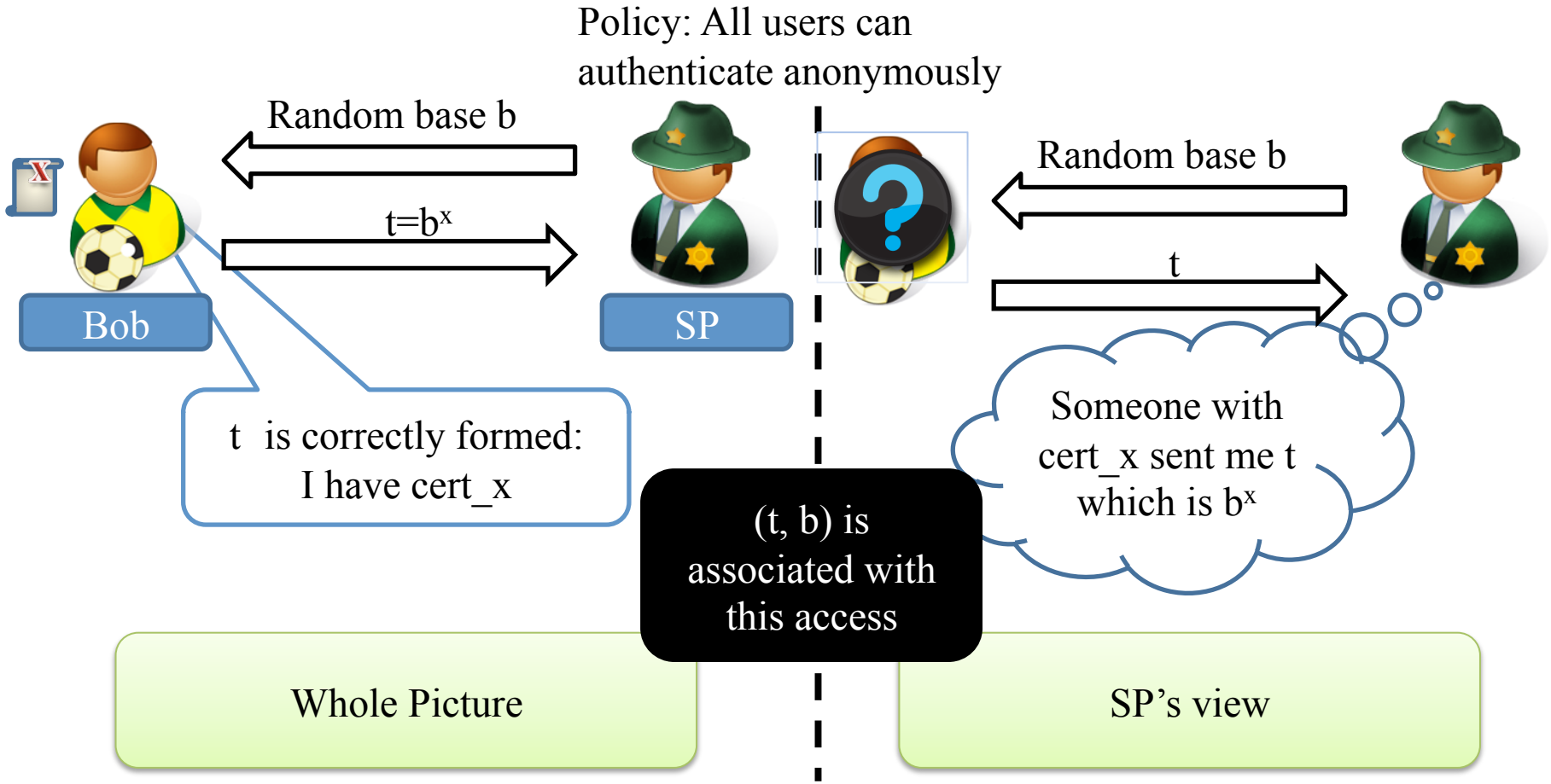
Comments Rules:	
Rated helpful by 100 users	+ 5
Use of offensive words	-2
Use of hate speech	-10

Access Policy: User can authenticate if his/her reputation in Video Content > -5 AND in Comments > -1

BLACR is similar to all anonymous credential systems in Registration



Anonymity is provided via a standard ZK Technique



BLACR supports reputation via a novel use of ZK techniques

Policy: reputation > -1

Random base b

List of Scores

t, CMT(R)

$R_1 = 0$ $t_1 \neq b_1^x$

$R_2 = 0$ $t_2 \neq b_2^x$

$R_3 = 4$ $t_3 = b_3^x$

$R_4 = -1$ $t_4 = b_4^x$

$R_5 = 0$ $t_5 \neq b_5^x$

$R_6 = -2$ $t_6 = b_6^x$

$\mathbf{R = \sum R_i = 1}$

List of Scores

t_1	b_1	3
t_2	b_2	-2
t_3	b_3	4
t_4	b_4	-1
t_5	b_5	6
t_6	b_6	-2

1. t is computed correctly.
2. CMT(R) is computed correctly.
3. R > -1

requires sending $CMT(R_i)$

Nothing about x is revealed

Nothing about R is revealed

Computation and transmission are of size O(n)

Only incremental work is needed in **express-lane authentication**

Policy: reputation > -1

Random base b

List of Scores

t, CMT(R), CMT(R)

1. t is computed correctly.
2. CMT(R) is computed correctly (with respect to t_k)
3. CMT(R) Is computed correctly (with respect to the additional entries)
4. R + R > -1

Computation and transmission are of size O(∂n)

List of Scores

t_1	b_1	3
t_2	b_2	-2
t_3	b_3	4
t_4	b_4	-1
t_5	b_5	6
t_6	b_6	-2

List of Scores

t_1	b_1	3
t_2	b_2	-2
t_3	b_3	4
t_4	b_4	-1
t_5	b_5	6
t_6	b_6	-2
t_7	b_7	1
t_8	b_8	2

Additional entries

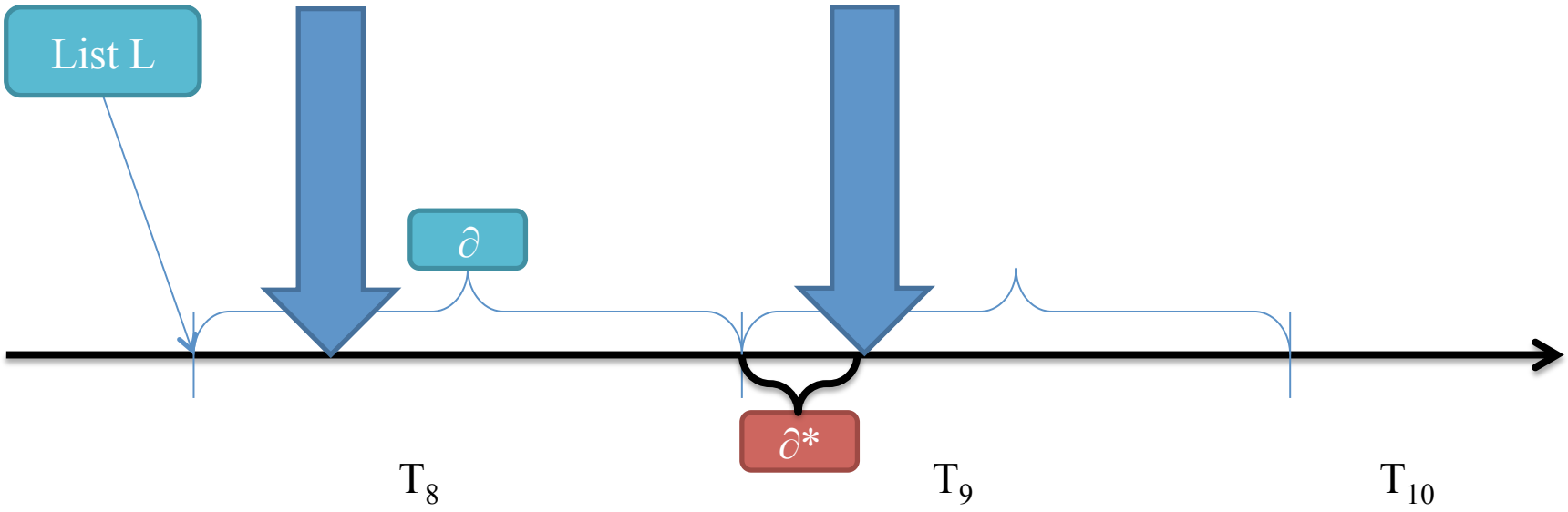
Express-lane tokens are tied to time periods to preserve anonymity

Authentication at T_8 results in a receipt t_k on list L

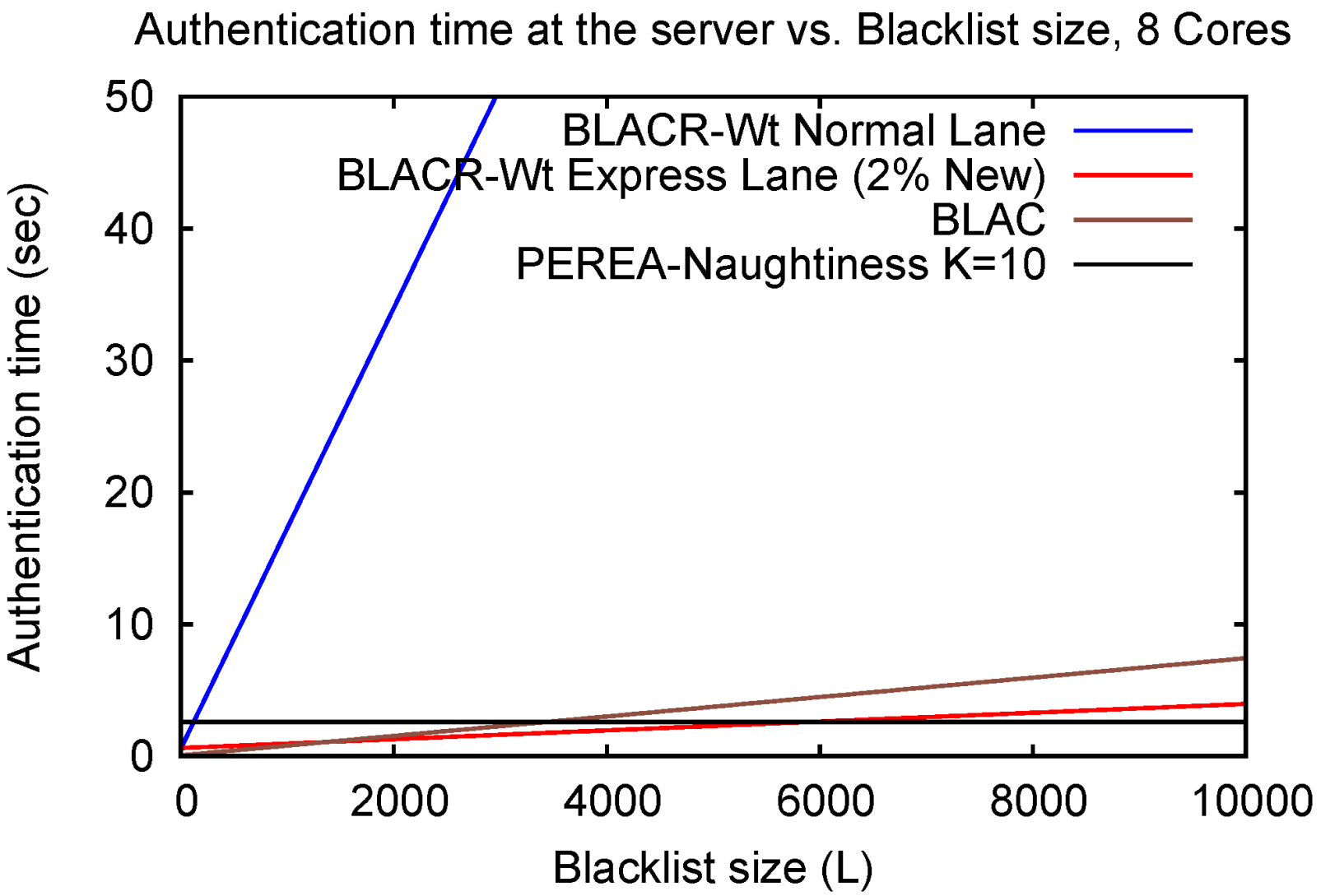
Authentication at T_9 involves:

1. List L
2. Additional entries ∂
3. Additional entries ∂^*

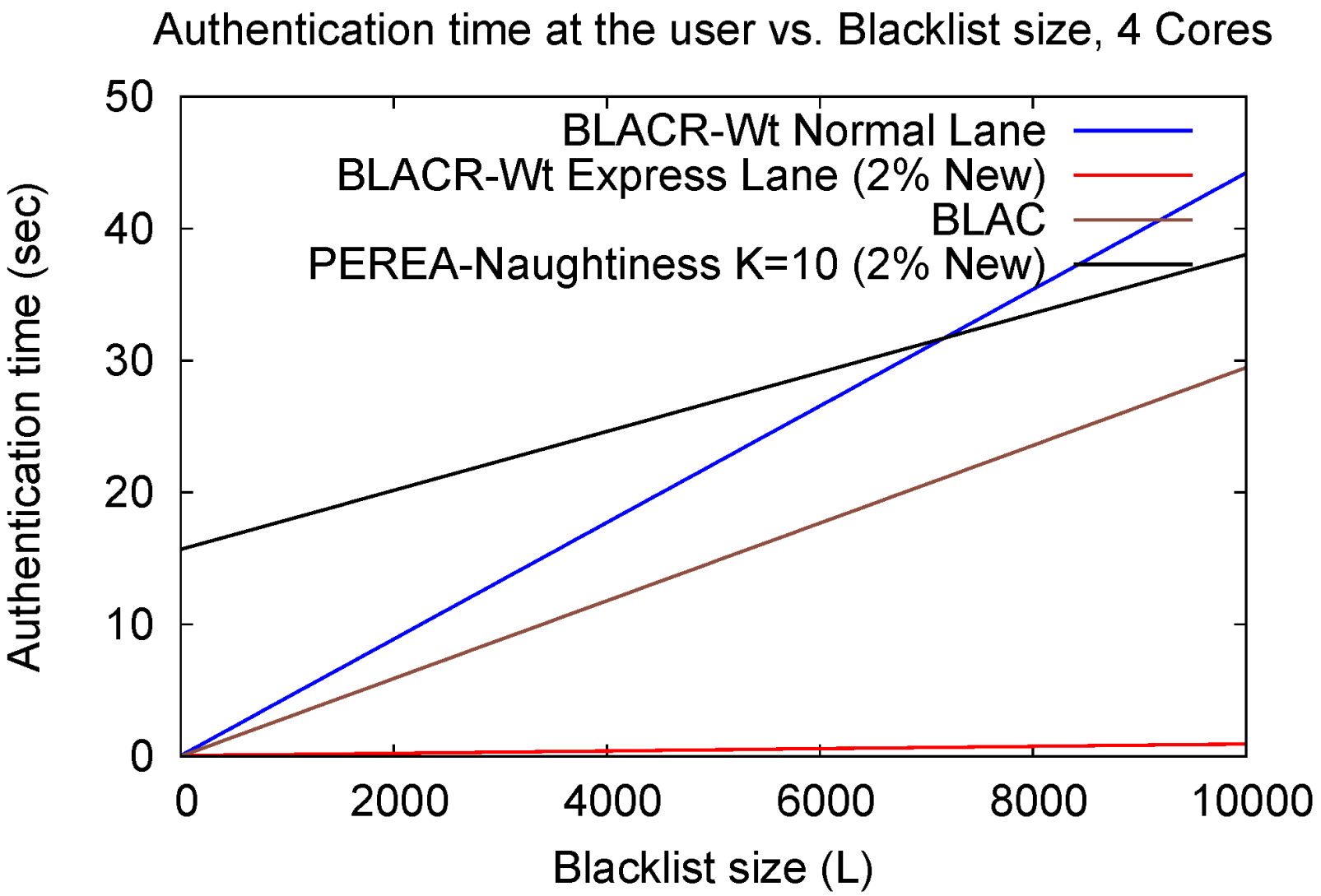
Obtain receipt t_k related to L + ∂



BLACR is fast at the server



BLACR is fast at the user too



Conclusion:
We make three contributions

We generalize the concept of **reputation based anonymous blacklisting**

We introduce **express-lane tokens** to greatly speed up authentication

We propose a **weighted extension** to penalize repeated misbehaviors

Punishing repeated misbehavior without affecting anonymity

List of Scores		
t_1	**b_1**	**-3**
t_2	b_2	-2
t_3	**b_3**	**-1**
t_4	b_4	-3
t_5	**b_5**	**-6**
t_6	b_6	-1

If t_1, t_3, t_5 belongs to Bob…

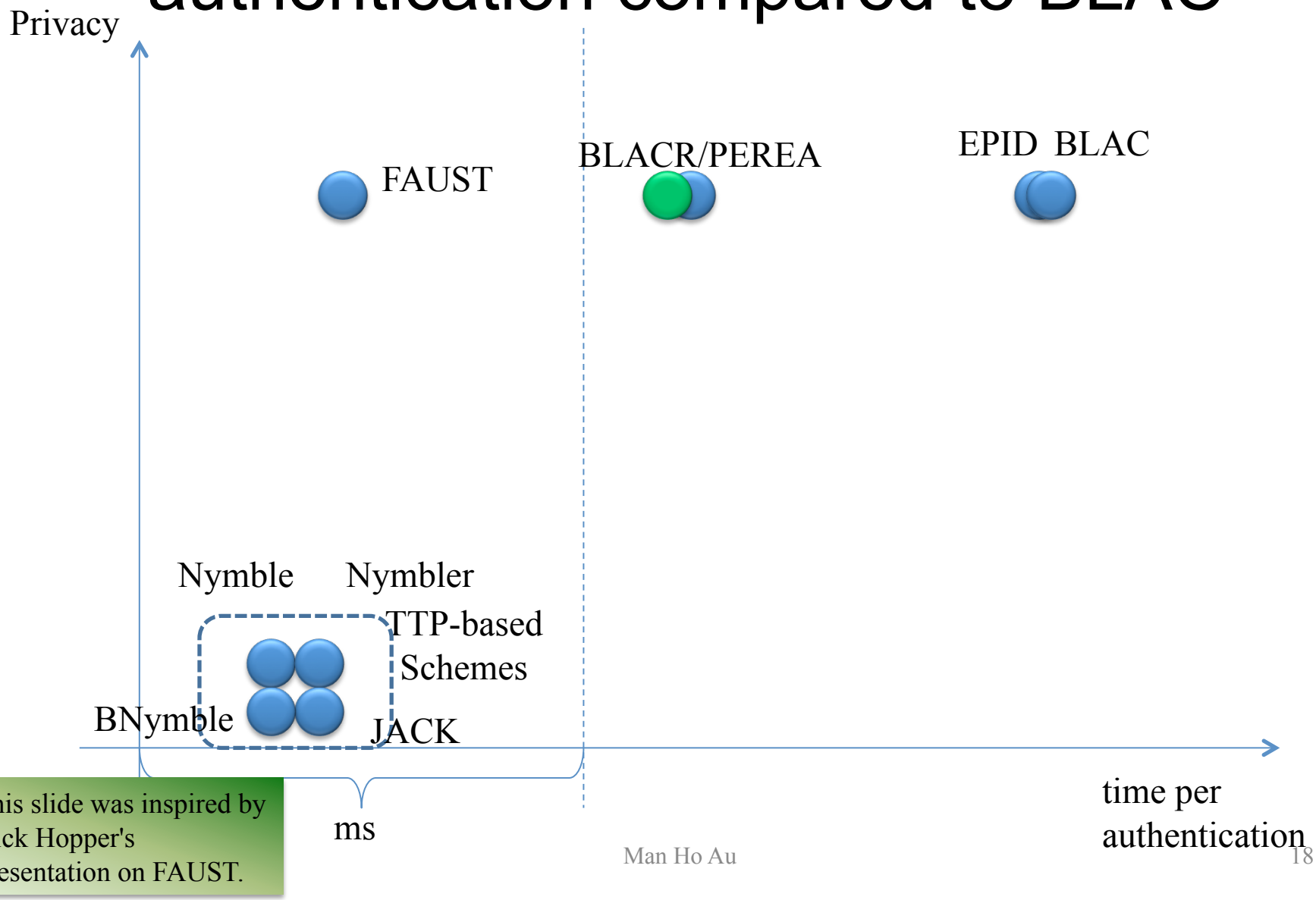
Reputation = -3 - 1 - 6 = -10

Weight	
1	1
2	2
3	4
4	10
5	20

In the weighted version:

Reputation = -3 + 2*(-1) + 4*(-6) = -29

BLACR improves the speed of authentication compared to BLAC



This slide was inspired by Nick Hopper's presentation on FAUST.