

---

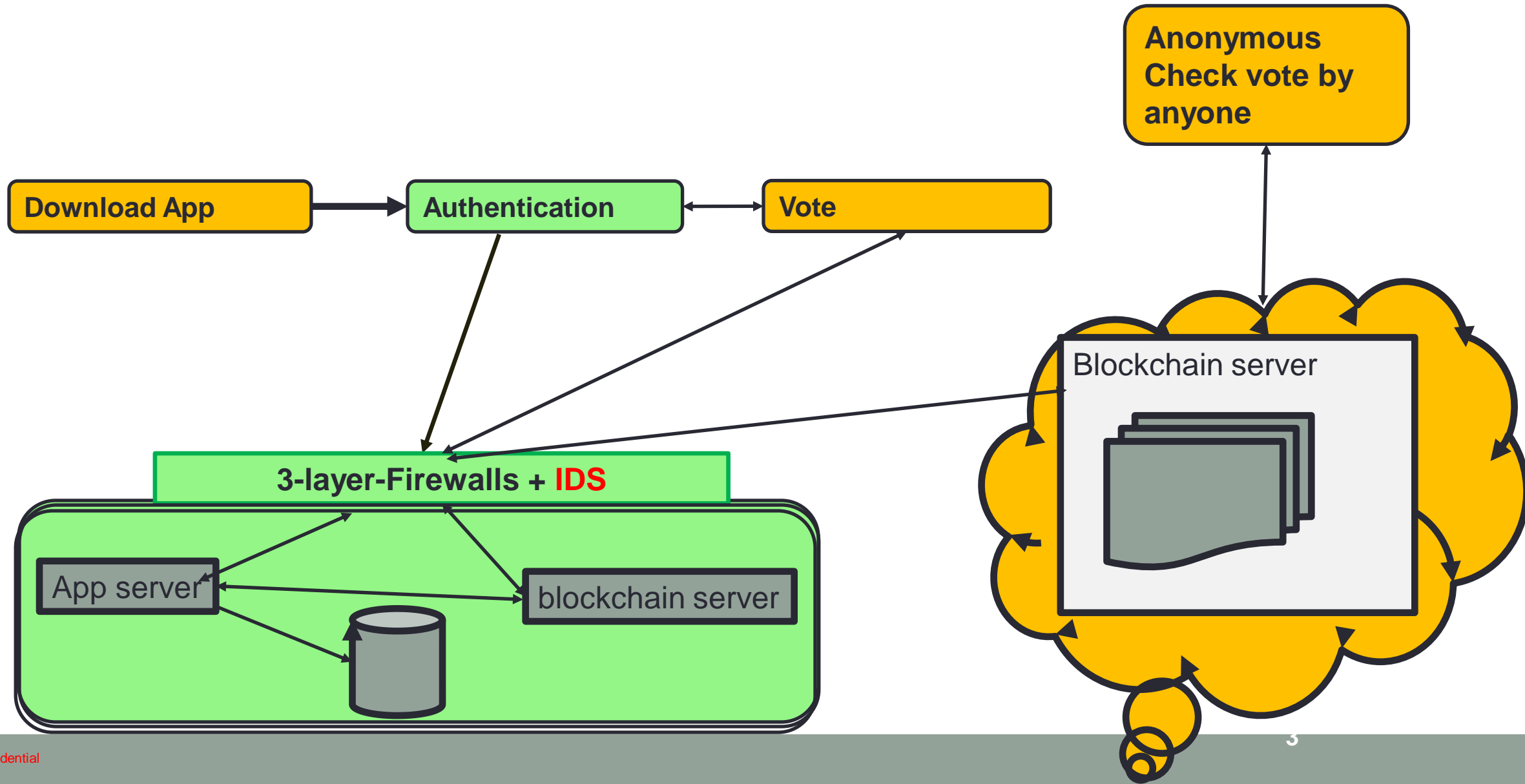
# Verifiable & Resilient Voting

Contact: [dliu@macrosql.com](mailto:dliu@macrosql.com)  
[Zoom](#)

# Comparison of Voting Systems:

	MacroSQL	Dominion	Paper
<b>Security Check</b>	ID & wallet verification	ID verification	ID verification
<b>Risks</b>	<ol style="list-style-type: none"> <li>1. Human ID check</li> <li>2. Online or Offline</li> </ol>	<ol style="list-style-type: none"> <li>1. Human ID check</li> <li>2. Right receipt, wrong barcode</li> <li>3. mass produce fake ballots;</li> <li>4. Interpret at will.</li> <li>5. Hard to detect cheating</li> <li>6. Human tamper machine</li> </ol>	<ol style="list-style-type: none"> <li>1. Human ID check</li> <li>2. Human check</li> <li>3. Scan machine</li> <li>4. Tabulation machine</li> </ol>
<b>Verification</b>	100%	Black box	Above 4 risks not easy to check
<b>3 party audit</b>	100% transparent	Very hard	Not easy: manual + permission
<b>Correctness &amp; Resilience</b>	100%, everything rebuildable	Difficult, black box	Human tamper not recoverable, voter can't verify his/her vote

# Architecture

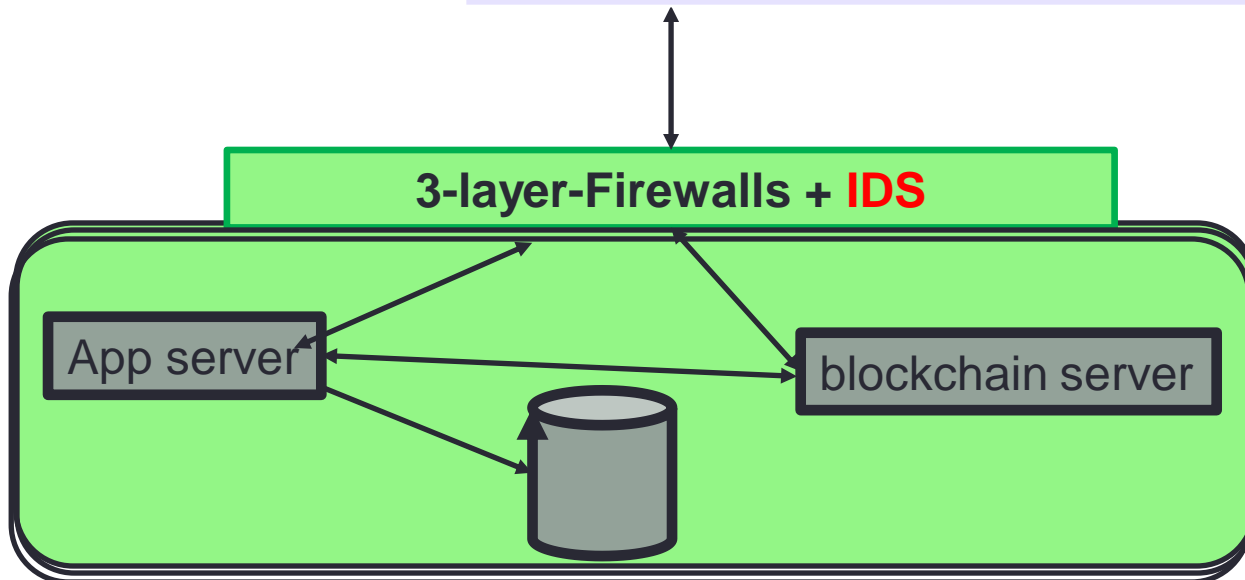


# Firewall + IDS (Intrusion Detection System):

3 layers firewall (IP + ports)

IDS support IP packet check up to 1000 keywords

IDS IP packet recording and alert



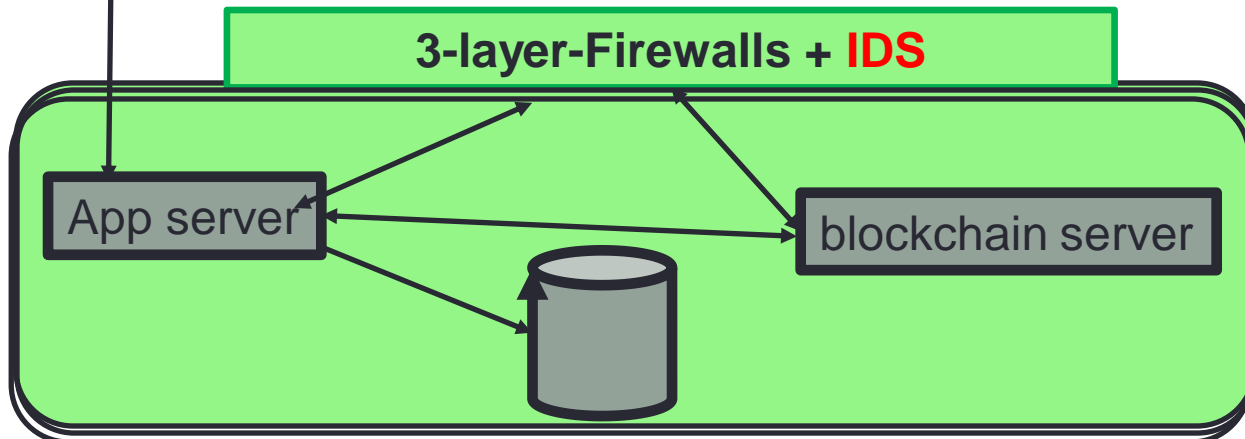
IDS = camera

# User Authentication:

4096 bit RSA key when register

2,3,4 factors login with strong password, fix IP modify

SSL, CSRF, session, DB check on every access; CSRF on every page access can be enabled



# Blockchain Security: Bullet-proof 3-tier

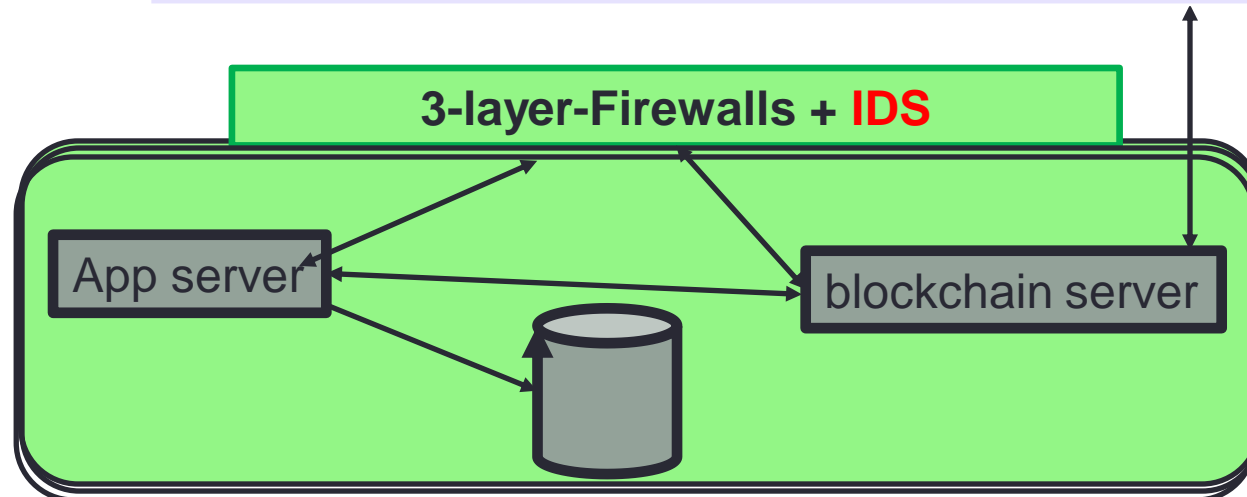
Our blockchain was designed for national stable currency, with 2 additional layers of security than normal Ethereum or Bitcoin blockchain

Our blockchain is resistant to attack of:

51% computing power attack (Bitcoin, Ethereum...)

Ethereum VM hack and smart contract hack

Virus or trojan horse

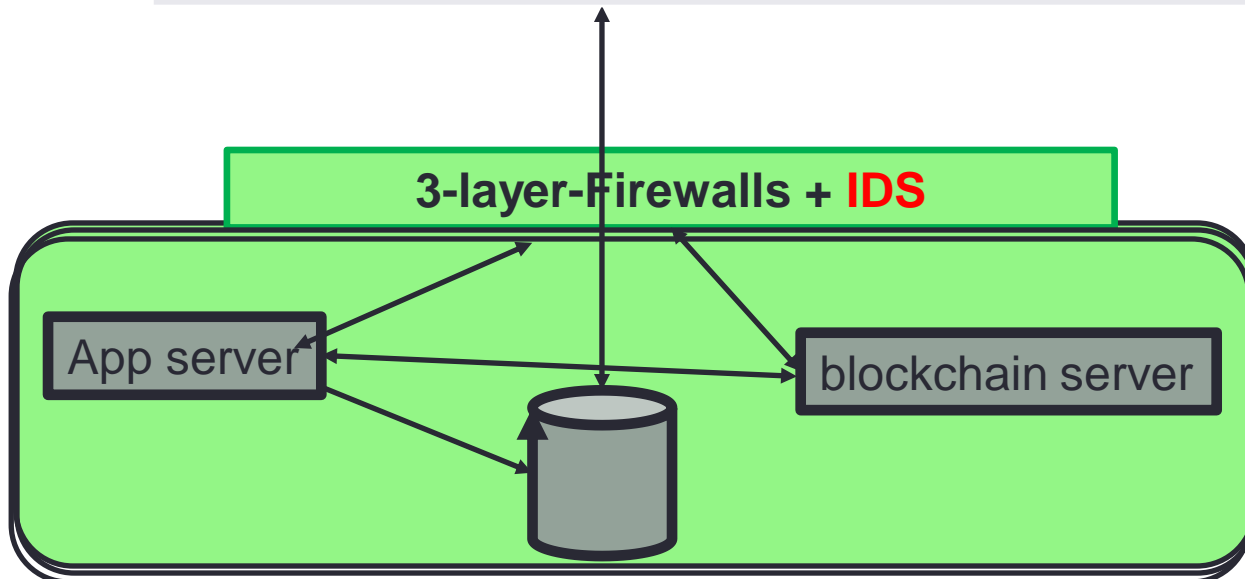


# DB security

All data is encrypted, optionally with symmetrical or RSA, user 4096bit RSA master public key

Checksum protection of each voted data, backup daily

Optionally DB access firewall



# Tamper-Proof, Openly Verifiable

---

- 1. Originally built as digital bank and stable currency, built for trustless environment**
- 2. 3-tier design: adding 2 layer of security check for 100% correctness**
- 3. 10000 times more secure than bank/exchange**
- 4. All data can be re-built from DB backup, or blockchain and DMV data**
- 5. Third party can have read-only access to blockchain; building their own node to do anonymous analysis and verification, they can't modify blockchain**
- 6. Only voter and official can see how voter's contribution to which candidate, neither can modify.**



# Built for Trustless environment:

---

- 1. Since each user can verify their votes using any browser & device, error is easily detectable**
- 2. Client security is not an issue**
- 3. Losing device don't affect security**
- 4. Hacking is detectable and don't affect correctness**
- 5. Probability of hacked is neglectable**
- 6. Can be configured fix IP domain access for extremely high security**

# Example of similar products we have built:

---

**1. Bpbtc.org:**

**It is a crypto exchange and bank + very secure 3-tier blockchain.**

**2. Bpbtc.net**

**Blockchain browser for Tier-1, Tier-2**

**All the technologies we discussed are already built.**

# Core Team:

Dave Liu, CTO, founder. performance tuning of database(18 Years Oracle, Intel, MarkLogic), MS in CS from [RPI](#), GPA4.0, [LinkedIn](#)



Dr. Symon Chang: CEO & Founder of [Tyan Computer](#), former General manager of Intel APAC R&D. PhD [Stanford University](#)



Fu Chen, driver, system, PhD of CS at Univ of NJ @Rutgers, Peking Univ BS of CS, [linked in](#)



Wenyun He, tech support, operation, sales &market Tsinghua BS, MS in EE from [RPI](#) [linked in](#)



Yang Zhang, Accounting and Financial Media, Master of Finance,Trinity College Dublin, [the University of Dublin, Ireland, linked in](#)



# Exchange using Cluster Database: 10~15 msec fin-tech tx

RtFinex 实时: 以微秒交易 白皮书 销售 加密货币 交易 账户 设置

CRYPTO

BTC	6600.0	1.54%
ETH	433.0	2.36%
DASH	222.0	4.72%
RTX	2.0	0%
SCC	22.0	0%

BTC 5m 对比 指标 模板

Bitcoin price in USDT, 5, RTFinex 开=65.00 高=65.00 低=65.00 收=65.00  
Volume (20) 66 n/a

Chart by TradingView

订单	价格	数量
卖 13	99.00000	9.00000
卖 12	92.00000	198.00000
卖 11	88.00000	156.00000
卖 10	86.00000	220.00000
卖 9	85.00000	154.00000
卖 8	82.00000	220.00000
卖 7	79.00000	22.00000
卖 6	77.00000	28.00000
卖 5	75.00000	242.00000
卖 4	72.00000	176.00000
卖 3	70.00000	22.00000
卖 2	68.00000	132.00000
卖 1	66.00000	66.00000
买 1	65.00000	44.00000
买 2	58.00000	176.00000
买 3	55.00000	247.00000
买 4	48.00000	88.00000
买 5	47.00000	88.00000
买 6	44.00000	180.00000
买 7	43.00000	176.00000
买 8	33.00000	231.00000
买 9	32.00000	88.00000
买 10	28.00000	66.00000
买 11	23.00000	110.00000
买 12	22.00000	110.00000
买 13	18.00000	242.00000

类型 限价 显示 100% 持续时间 7天 价格 82 数量 44

卖出

余额: 885300.83 BTC

类型 限价 显示 100% 持续时间 7天 价格 数量

买入

余额: "100000888.66 USD"

交易时间	卖方	价格	数量
9/16/2018, 1:02:47 PM	卖	77	16
9/16/2018, 1:02:54 PM	买	77	1

开放订单	价格	数量	取消
卖 LMT	82	0/44	×
买 LMT	82	0/44	×

公司 联系人 活动 白皮书 招聘 销售 团 中文