**Крипто-Выборы – защита от фальсификаций**

 **или выборы будущего**

Наступает эра электронных выборов, когда можно не выходя из дома голосовать по интернет. Однако вопрос о честности существующих систем электронных выборов остается открытым – в них возможны фальсификации, так как все они являются централизованными. Это вызвано тем, что сервер, производящий подтверждения голосов и их расчет, является централизованным и может управляться отдельными людьми с полным доступом к базе данных. В этом случае человек, имеющий полный доступ (администратор сети или сервера) может вручную или с помощью сторонних программ тайно изменять результаты выборов.

Поэтому необходимо обратить свой взор на появившуюся недавно (в 2009г) одноранговую децентрализованную систему обмена и учета зашифрованной информацией – **криптовалюту**. Полную информацию обо всех достоинствах криптовалюты вы можете найти в интернете. Если систему выборов сделать на основе криптовалюты (криптовыборы, криптоголосование), то мы получим:

1. Фальсифицировать голосования или выборы не возможно.
2. Голосование изначально тайное, но каждый избиратель может голосовать, по желанию, открыто.
3. Все транзакции с передачей своих голосов видны любому через интернет в обезличенном виде.
4. Подсчёт голосов происходит в реальном времени: автоматически и быстро.
5. Себестоимость таких выборов ничтожно мала, и криптовыборы (криптоголосования) можно проводить хоть каждый год. То есть перевыбирать депутатов каждый год – что положительно сказывается на ответственности депутатов перед своими избирателями.
6. Криптовыборы невозможно сломать, уничтожить - пока не уничтожен весь интернет. Данные о ходе голосования хранятся на каждом компьютере, который участвовал в криптовыборах. Поэтому весь ход голосования автоматически восстановится при появлении связи между компьютерами.
7. Продолжительность голосования может быть растянута на неделю или даже на месяц – чтобы все успели без суеты проголосовать.

**Способ реализации, основы.**

Каждый год создается новая криптовалюта для голосования.

Создаются и опубликовываются номера кошельков (счета), которые привязаны к вариантам данного голосования и на которые избиратели будут пересылать свои криптоголоса. Назовем их «выбираемые счета».

Каждому избирателю выдается программа-кошелек, которая создаёт криптосчет. Назовем их «голосующие счета». На этот голосующий счет перечисляется с криптосчета ЦИК (который всем известен) в качестве голоса криптомонета (криптоголос). Этот криптоголос избиратель может перевести на выбираемый счет.

Сам процесс голосования – это перевод криптовалюты (криптоголоса) избирателем со своего голосующего счета на выбираемый счет.

Таким образом, на том или ином «выбираемом счету» копятся криптоголоса, и результаты голосования можно смотреть сразу в реальном времени любому человеку через интернет.

**Способ реализации, частности.**

Сама система криптовалюты решает все задачи о выборах кроме одного вопроса – как каждому избирателю передать криптокошелек с голосующим счетом и зачислить ему криптоголос так чтобы:

1. была соблюдена тайна голосования. То есть голосующий счет был бы обезличенным при создании или передачи голосующего счета конкретному избирателю.
2. была защита от создания «мертвых душ». То есть когда выдающий или создающий криптокошельки или криптосчета орган был бы лишен возможности создать лишние криптокошельки, получить на них криптоголоса и проголосовать ими.
3. была защита от использования в ТИК и УИК невостребованных избирателями программ-кошельков. Например, избиратель не участвует в выборах и его кошелек остается в УИК при проведении криптовыборов, его вскрывают и пользуются противозаконно.

Все эти вопросы решают частности в реализации криптовыборов. Вот несколько из них (в данной инициативе они не принципиальны и могут быть обсуждены или приняты отдельно).

Программа-кошелек, которая создает криптосчет и обслуживает транзакции выдается избирателю в УИК по его паспорту и избиратель расписывается в ведомости о получении. Выдача происходит круглый год. Сама программа-кошелек у всех одинаковая. Избиратель на своем компьютере дома запускает программу-кошелек и она создает случайный адрес-счет (голосующий счет). Таким образом, тайность криптоголосования будет соблюдена, а так же будет создана защита от «мертвых душ» - каждый сможет просмотреть ведомость о выданных программах-кошельках и подсчитать общее число голосующих. Желательно эту информацию так же дублировать в электронной базе ЦИК.

Голосования назначаются на первую половину года – например на май – как раз там майские праздники и можно совместить демонстрации с предвыборной агитацией. По прошествии выборов (и даже во время их), каждый, кто не захотел голосовать, может свой криптоголос перевести на «возвратный счет» в ЦИК (или ТИК или УИК) и получить за него реальные деньги – например 500 рублей. Причем это можно сделать в течении 1-2 месяца после окончания голосования. Таким образом, все кто не захотел участвовать в выборах получат большую мотивацию все же прийти в УИК и забрать свой конверт с программой-кошельком, создать свой криптосчет, получить на него криптоголос и продать его обратно государству. «Возвратный счет» так же будет виден всем – а значит сразу будет ясно: какое количество избирателей вообще не проголосовало. Таким образом, будет создана защита от использования невостребованных программ-кошельков в ТИК или УИК.

**Способ внедрения криптовыборов в текущем законодательстве, без переделки законов.**

Уже сейчас можно внедрить криптовыборы как вариант голосования по аналогии с досрочным голосованием. То есть избиратель, желающий проголосовать досрочно, приходит в УИК в течении месяца до основных выборов ( но не позже чем за неделю) и уведомляет устно УИК. Те выдают ему программу-кошелек, а избиратель расписывается в книге избирателей что получил «электронную крипто-бюллетень» досрочно. Таким образом, на самих выборах уже он не получит бюллетень, так как в книге избирателей напротив него уже будет стоять запись что он голосовал заочно путем криптовыборов.

Дальше он голосует так, как предложено выше в системе криптоголосования. А в ЦИК будет собрана информация отдельно по тем, кто голосовал досрочно обычным образом и через криптовыборы.